Zweiter Teil: Die drei Strukturmerkmale des DSG

Beim eidgenössischen Datenschutzgesetz handelt es sich um einen der wenigen Erlasse, der Antworten ebenso auf die *digitale Transformation* zu geben sucht. Eine Herausforderung, mit der sich neben dem Privatrecht ebenso das Urheberrecht, z. B. wegen Streamingdiensten, konfrontiert sieht.[338] Gleichwohl beschränkt sich das DSG weder auf spezifische Technologien der Personendatenverarbeitung noch auf spezifizierte (z. B. automatisierte) Verarbeitungshandlungen oder Technologien.[339] 228

Die Totalrevision setzt zwar neue Akzente. Anstoss zu dieser Totalrevision gaben zum einen die Entwicklungen in der EU.[340] Die Schweiz ist auf einen Angemessenheitsbeschluss vonseiten der zuständigen EU-Behörden angewiesen, vgl. Art. 45 DSGVO.[341] Zudem wurde die Totalrevision mit dem Aktualisierungsbedarf wegen des rasanten technologischen wie gesellschaftlichen Wandels begründet. Hinzu trat ein Attest, das der Wirksamkeit des geltenden DSG ein bescheidenes Zeugnis ausstellte.[342] Die jüngsten datenschutzrechtlichen Neuerungswellen erfolgen nicht nur in Anerkennung von Bedeutung, Chancen und Risiken moderner Datenverarbeitungstechnologien.[343] 229

338 Aufschlussreich z. B. die Beiträge in AcP 218 (2018), Heft 2–4, 151 ff.

339 Zum weit definierten Begriff des Verarbeitens (von Personendaten) vgl. Art. 5 lit. d (ff.) nDSG; Art. 3 lit. e und lit. f DSG.

340 Verordnung der EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, in Kraft seit dem 25. Mai 2016 mit einer Umsetzungsfrist bis zum 25. Mai 2018; abrufbar unter: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (zuletzt besucht am 30. April 2021); zur «Globalisierungswirkung» Birnhack, CLSR 2008, 508 ff.; zur Notwendigkeit der datenschutzrechtlichen Harmonisierung Cottier, SRIEL 2016, 255 ff.

341 Ausserdem hat die DSGVO extraterritoriale Wirkung, vgl. Art. 3 Abs. 2 lit. a und lit. b DSGVO. Dass die Vorgaben der DSGVO für manch ein Schweizer Unternehmen direkt gelten, wurde trotz des Ablaufes der Umsetzungsfrist am 25. Mai 2018 nur ungenügend zur Kenntnis genommen, vgl. NZZ, Was das neue EU-Datenschutzgesetz für die Schweiz bedeutet, Mai 2018, <https://www.nzz.ch/wirtschaft/strengerer-datenschutz-auch-in-der-schweiz-ld.1388558> (zuletzt besucht am 30. April 2021); zur Totalrevision auch mit Blick auf einen Angemessenheitsbeschluss Frei, Jusletter vom 17. September 2018, N 17 f.

342 Vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017 (17.059), 6941 ff.; Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011 (BBl 2012 335); vgl. weiter Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, 5 ff.; zum Vorentwurf: <https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vorentw-d.pdf> (zuletzt besucht am 30. April 2021); zum Entwurf: <https://www.admin.ch/opc/de/federal-gazette/2017/7193.pdf> (zuletzt besucht am 30. April 2021); grundlegend zum sog. Vollzugsdefizit Buchner, 1; zum Vollzugsdefizit auch Spiecker genannt Döhmann, in: Epiney/Sangsue (Hrsg.), 1 ff., 7 ff.; vertiefend zum Vollzugsdefizit dritter Teil, VII. Kapitel.

343 Den Bedeutungswandel, den das Datenschutzrecht allerdings gerade auch mit der DSGVO vollzieht, auf diese starke Hand der Behörden zu reduzieren, greift indes zu kurz. Vertiefend zu den Entwicklungstrends der DSGVO vgl. dritter Teil, XIII. Kapitel, A.

230 Gleichwohl soll an dieser Stelle – wie bereits im historischen Teil, allerdings chronologisch nicht ganz so weit zurück – eine Rückblende insb. auf den Gesetzgebungsprozess im Rahmen der *Verabschiedung des ersten DSG* erfolgen. Die ebenda geführten Debatten und getroffenen Entscheidungen sind auch nach der Totalrevision relevant: Denn mit dieser wird von der *Grundstruktur, dem Basiskonzept sowie den prägenden Leitprinzipien des ersten DSG* nicht abgegangen.[344] Ebendiesen widmet sich dieser zweite Teil. In ihm werden *drei Strukturelemente* des eidgenössischen Datenschutzgesetzes genauer analysiert. Eine solche vertiefte Beschäftigung mit der *Wirkungsstruktur des DSG* ist nicht zuletzt der Tatsache geschuldet, dass das DSG in seiner Gesamtheit sowie für seinen privaten Bereich von wissenschaftlicher Seite bislang eher wenig Aufmerksamkeit erfahren hat.[345]

231 Seit jeher wird vertreten, dass das eidgenössische Datenschutzgesetz eine sog. *Querschnittsmaterie* regelt.[346] Gleichwohl werden zahlreiche der datenschutzrechtlichen Konzepte und Begriffe – nicht zuletzt dasjenige des Schutzobjektes resp. Schutzzweckes sowie damit zusammenhängend die Regelungsmechanik und die Ansätze des DSG – mit einem bemerkenswerten Facettenreichtum umschrieben.[347] Die Interpretationsvielfalt und damit eine gewisse Orientierungslosigkeit zeigt sich z. B. im Evaluationsschlussbericht, der im Zuge des zwanzigjährigen Bestehens des Datenschutzgesetzes veröffentlicht wurde und Anstösse für die Totalrevision lieferte:

> «Das Datenschutzgesetz konkretisiert den grundrechtlichen *Schutz der Privatsphäre*, wie er in Art. 8 Abs. 1 EMRK sowie in der Bundesverfassung verankert ist. Art. 13 Abs. 2 BV legt fest: „Jede Person hat Anspruch auf *Schutz vor Missbrauch ihrer persönlichen Daten*." Obwohl es aus dem Wortlaut der Norm nicht klar hervorgeht, wird mit dieser Bestimmung das *Grundrecht auf informationelle Selbstbestimmung* definiert. Damit wird ein Schutzniveau hinsichtlich der persönlichen Daten statuiert, das nur unter den Voraussetzungen von Art. 36 BV eingeschränkt werden kann, d. h. die Einschränkung muss auf einer gesetzlichen Grundlage beruhen, ein öffentliches Interesse oder den Schutz von Grundrechten Dritter bezwecken sowie den Grundsatz der Verhältnismässigkeit und den Kerngehalt des Grundrechts auf informationelle Selbstbestimmung wahren. Dem Recht auf informationelle Selbstbestimmung kommt horizontale Drittwirkung zu, d. h. eine Schutzpflicht besteht auch gegenüber Datenbearbeitungen durch Privatpersonen. Konkretisiert wird dieser Schutzbereich durch Art. 4 ff. und Art. 12 ff. DSG (Schweizer 2008: 326 (N 43) zu Art. 13). Das DSG bezweckt gemäss Art. 1 „den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden". Der *Schutz der Persönlichkeit* zielt dabei primär auf die Bearbeitungen durch Private, der Schutz der

344 Die Begleitgruppe schlug in ihrem Bericht vor, sich am geltenden Aufbau des DSG zu orientieren, vgl. Bericht der Begleitgruppe Revision DSG, Normkonzept zur Revision des DSG vom 29. Oktober 2014, 7.

345 Zur Unkenntnis des Rechtsgebietes und verwirrenden Interpretationen auch zum Schutzbereich vgl. Gamper, Jusletter IT vom 22. Februar 2011, N 2 f.

346 Vgl. den Hinweis des EDÖB: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html> (zuletzt besucht am 30. April 2021); Bolliger/Féraud/Epiney/Hänni, 11.

347 Vertiefend hierzu insb. dritter Teil, VII. Kapitel, A.2.

> Grundrechte auf die Bearbeitungen durch staatliche Behörden. Zur Motivation des Datenschutzes führte der Bundesrat in seiner Botschaft an, der Umgang mit Daten könne sich in verschiedener Weise nachteilig oder verletzend auf die betroffene Person auswirken: Verunsicherung, wenn man nicht mehr überblickt, wer Daten über einen bearbeitet; Anmassung durch indiskretes Auskundschaften; Benachteiligung oder unbillige Behandlung aufgrund unrichtiger, unvollständiger oder nicht mehr aktueller Informationen; lebenslänglicher Makel aufgrund dauerhafter Aufbewahrung und Verwendung negativer Angaben; Verletzung der Persönlichkeit durch übermässiges Bearbeiten, z. B. durch Anprangern in der Öffentlichkeit oder Erheben unnötiger Angaben bei einem Vertrag; Verletzung durch Zweckentfremdung der Daten (Bundesrat 1988: BBl 1988 II 416). Das DSG will somit verhindern, dass Personen durch *nicht konformes Bearbeiten ihrer Daten einen Schaden erleiden*; sie sollen also zum Beispiel nicht aufgrund bestimmter Informationen, die ein Arbeitgeber nicht ohne Wissen der Person beschaffen dürfte, ihre Stelle verlieren. Das DSG setzt aber bereits vor dem Schaden an, indem es – anknüpfend an den grundrechtlichen Schutz der Privatsphäre – die Personen generell vor einer informationellen Entblössung schützen will. Dabei ist es nicht die Absicht des Gesetzgebers, mit dem DSG Datenbearbeitungen generell zu unterbinden; vielmehr sollten diese so ausgestaltet werden, dass der informationellen Selbstbestimmung Genüge getan wird: „Ein Datenschutzgesetz hat nicht den Zweck, die Entwicklungsmöglichkeiten im Bereich der Informationstechnologien zu verhindern oder einzuschränken." Vielmehr seien *„gewisse Leitplanken* für die Datenbearbeitung zu setzen, die garantieren, dass die *Entfaltung der Persönlichkeit nicht durch unnötige und unerwünschte Informationstätigkeiten beeinträchtigt wird"* (BBl 1988 II 417–418)».[348] [Hervorhebungen durch die Autorin]

232 «Informationelle Selbstbestimmung», «Missbrauchsverhinderung», «Schutz der Privatsphäre», «gewisse Leitplanken zum Schutz der Persönlichkeitsentfaltung vor unnötiger Informationstätigkeit», «Verhinderung eines Schadens» – zumindest teilweise scheint der Beitrag Begriffe «untechnisch» zu verwenden und nicht darauf abzuzielen, ebendiese fundiert zu durchdringen. Die kurze Passage führt in exemplarischer Weise das Vielerlei an Konzepten und Begriffen, die im Rahmen der Auseinandersetzung mit dem DSG oft differenzlos kursieren, vor Augen.[349] Sie bestätigt den Befund, der bereits für das Private gefunden wurde, mit welchem der Datenschutz untrennbar zusammenhängt, dass dieses ein schwer zu fassendes Konzept ist. Entsprechend vage bleiben für das Datenschutzrecht

348 Bolliger/Féraud/Epiney/Hänni, 7 f., Hervorhebung durch die Autorin; vertiefend und umfassend zu den in diversen Rechtstexten verankerten staatlichen Schutzpflichten mit Blick auf die Verbürgung der Privatsphäre im digitalen Zeitalter vgl. Kaufmann/Ghielmini/Medici/Pulver, 4 ff., mit einer Zusammenfassung bei 1 ff.; vgl. sodann Baeriswyl, digma 2008, 4 ff., 5, wonach das Recht auf Anonymität ein Aspekt des Grundrechts auf informationelle Selbstbestimmung und deshalb grundsätzlich gewährleistet sei, wobei seine Einschränkung, die Offenlegung der Identität, einer Rechtfertigung bedürfe; zur Drittwirkung der Grundrechte vgl. z. B. Bucher, SJZ 1987, 37 ff.

349 Zudem wird auf ein Missverständnis mit Blick auf den Datenschutz in der Allgemeinheit hingewiesen. Dieses artikuliert Gamper, Jusletter IT vom 22. Februar 2011, Einleitung, mit den Worten: «Datenschutz als Regelung des Rechts auf Privatsphäre in der (elektronischen) Datenverarbeitung wird in allgemeiner Unkenntnis der Materie überwiegend auf einen Geheimhaltungsanspruch reduziert, der rechtlich jedoch nur sehr eingeschränkt existiert»; nach Schmid, in: Schmid/Girsberger (Hrsg.), 151 ff., 154 gehören zu den gesetzlich geschützten Persönlichkeitsrechten das Recht auf Privatsphäre, Ehre und informationelle Selbstbestimmung.

wesentliche Konzepte und Begriffe, was nicht nur der faktischen Verwirklichung, sondern auch der theoretischen Fortentwicklung im Wege steht. Immerhin – einige der über die Totalrevision eingeführten neuen Instrumente, wie beispielsweise das Verarbeitungsverzeichnis oder die Risiko-Folgenabschätzung, haben das Potential, eine gewisse strukturierende und damit kompensierende Wirkung zu erzielen.

233 Bei einer Auseinandersetzung mit dem DSG *gerade auch vor seiner Totalrevision* (die zu einer besseren Durchdringung der Materie auch in der Schweiz führte), präsentiert sich die Situation fast so, als ob die «Black Box» der Technik auch in das Recht transportiert würde. Das Recht des Privaten zeigt sich in einer für das Recht irritierenden Weise diffus. Als symptomatisch bezeichnet es denn auch Simitis, dass bis heute an der missverständlichen Begrifflichkeit des Datenschutzrechts festgehalten wird.[350]

234 Drei Strukturmerkmale prägen die Funktionsweise des DSG in beiden seiner Fassungen. *Erstens:* Der *Dualismus* im Sinne einer differenzierenden Regelung für den öffentlichen Bereich des Bundes und den privaten Bereich.[351] *Zweitens:* Ein generalklauselartiges Regime, in dessen Zentrum die allgemeinen Verarbeitungsgrundsätze stehen. *Drittens:* Die Anknüpfung des Datenschutzes für den privaten Sektor am Subjektschutz, genauer am *zivilrechtlichen Persönlichkeitsschutz*. Die Regelung des DSG für den privaten Bereich orientiert sich folglich an der Struktur von Art. 28 ZGB.[352]

235 Der zweite Teil will einen Beitrag zur besseren dogmatischen und konzeptionellen Durchdringung des DSG – in seiner Fassung vor, aber auch nach seiner Totalrevision – leisten. Die *Charakterisierung* des DSG anhand seiner *Strukturmerkmale* macht seine *Funktionsweise* («Wie funktioniert das Gesetz?») sichtbar. Alsdann wird es möglich, die Angemessenheit der Regelungsstruktur angesichts der Herausforderungen des Datenschutzes zu diskutieren («Funktioniert das Gesetz?»).[353] Eine solche mittel-, zweck- und zielorientierte Betrachtungsweise

350 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 2 f. und N 26; ebenso zur falschen Beschreibung des Rechtsgebietes Rossnagel, digma 2011, 160 ff., 160; vgl. Forstmoser, digma 2003, 50 ff., 51; als unglücklicher Begriff bezeichnet von Bull, Computer, 3; Drechsler sprach in seinem Beitrag anlässlich der Konferenz zum Titel «Neue EU-Datenschutzgrundverordnung: Herausforderungen für Schweizer Unternehmen bei der Umsetzung», Europa Institut an der Universität Zürich, Donnerstag, 24. Mai 2018, Zürich, von weit verbreiteten «fake news», also Missverständnissen resp. Fehlinformationen, was die Beschreibung und Interpretation des Datenschutzgesetzes und weiter des schweizerischen Datenschutzrechts anbelangt; eine ähnliche Einschätzung findet sich bei Bull, Vision, Vorwort und 1 ff., der die publizistische Darstellung der Rechtsmaterie und unbegründete Behauptungen beklagt; zur Fehlbezeichnung auch Gächter/Werder, in: Epiney/Fasnacht/Blaser (Hrsg.), 87 ff., 88 f.; zum Ganzen vgl. dritter Teil, VII. Kapitel.

351 Den Begriff einer dualen Rechtsnatur des DSG verwendet in seinem Beitrag zur Rechtsanwendung bei internationaler Datenbearbeitung durch Private zutreffend Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.8.

352 Vgl. Art. 12 f. i. V. m. Art. 4 ff. DSG; Art. 1 i. V. m. Art. 30 ff. nDSG.

353 Hierzu dritter Teil, VII. Kapitel.

scheint geeignet, zumindest teilweise Definitionsdefizite bezüglich des Terminus des Privaten abzumildern. Eine solche Analyse wird zu Tage fördern, dass es nicht nur der rasante technische Fortschritt und die Kommerzialisierung von Personendaten als quasi-exogenen Faktoren sind, die das Datenschutzrecht auf den Prüfstand stellen.[354] Vielmehr sind die Ursachen für das Vollzugsdefizit sowie die Schwächen der heutigen Datenschutzgesetzgebung teilweise *endogen und rechtskonzeptioneller Natur*. Die Wirksamkeitsdefizite des DSG liegen teilweise in seinen Anknüpfungspunkten und den Strukturmerkmalen selbst. Dass dieser Teil sich eher am Rande mit der Totalrevision befasst, ist keineswegs bloss den Faktizitäten der Zeit geschuldet. Vielmehr finden sich hierfür starke inhaltliche Argumente, zumal die Strukturmerkmale auch in Zukunft dem DSG seine Charakteristika vermitteln. Gleichwohl werden diese – auch wenn sie beibehalten werden – teilweise in einem neuen Licht erscheinen durch die Einführung neuer Instrumente qua Totalrevision.

Der Entscheid, den *Dualismus als primäres Strukturmerkmal* des DSG in seiner Entstehungsgeschichte zu präsentieren, vermag als erneuter Anachronismus erscheinen und etwas Selbstverständliches zu adressieren: Die Zweiteilung des Rechts in einen «öffentlichen» und einen «privaten» Bereich prägt bis heute die Vorstellungen des kontinental-europäischen Rechts.[355] Allerdings: Die markanteste konzeptionelle Differenz zwischen dem DSG auch nach Totalrevision und der DSGVO ist diesem thematischen Aspekt zuzuordnen. Die DSGVO geht zu einem Monismus über; das DSG hält allerdings weitgehend diskussionslos an seinem Dualismus fest. Mit diesen Entwicklungen wird sichtbar, dass den Fragen rund um die *bereichsspezifischen Differenzierungen im Datenschutzrecht* herausragende Bedeutung zukommt.[356] Die Relevanz *systemischer Bezüge* für das Datenschutzrecht rückt allerdings in einem subjektivrechtlich geprägten Ansatz in den Hintergrund. Die Auseinandersetzung mit kontextuellen Herausforderungen des Datenschutzrechts ist bereits in der Debatte im Rahmen der Verabschiedung des ersten DSG ausgeprägt. Ihr widmen sich die nächsten Seiten. 236

354 Vgl. zu den Herausforderungen auch Bischof/Schweizer, digma 2011, 152 ff.
355 So auch sichtbar anhand der universitären rechtswissenschaftlichen Curricula.
356 Grundlegend hierzu m. w. H. bereits Buchner, 7 ff.

IV. Kapitel: Erstes Strukturmerkmal – Dualismus

«L'élaboration longue et chaotique d'une loi fédérale sur la protection des données est à plus d'un titre exemplaire de ce qui se passe au niveau du processus législatif, lorsque des intérêts privés et économiques sont en jeu.»[357]

A. Die Gretchenfrage nach dem Ausgangspunkt

237 Die (gesetzgeberische) Geschichte wiederholt sich – in die Länge zogen sich ebenso die Arbeiten im Zuge der Totalrevision des DSG, nicht nur diejenigen im Zusammenhang mit der Verabschiedung eines ersten eidgenössischen Datenschutzgesetzes. Im historischen Teil wurde die Etablierung der Idee eines Zweikammersystems bezüglich der Kategorie des Privaten beschrieben.[358] Sie geht von einem Dualismus von öffentlich und privat aus. Dass dieses Zweikammersystem nicht schwarz-weiss und absolut etabliert ist, wird an verschiedenen Stellen, insb. anhand einer Auseinandersetzung mit dem Verhältnismässigkeitsprinzips sichtbar werden.[359] Gleichwohl lässt sich für das DSG – selbst nach seiner Totalrevision – die dualistische Struktur als ein Charakteristikum beschreiben.

238 Wie aber wurde und wird dieses Verhältnis aus datenschutzrechtlicher Perspektive insb. in der Schweiz thematisiert? Für eine Annäherung an den Datenschutz und damit auch das Verhältnis der Normgestaltung im Datenschutzrecht für Verarbeitungshandlungen durch Private einerseits und durch öffentlich-rechtliche Stellen andererseits war eine literarische Metapher prägend: «big brother is watching you».[360] In Orwells Worten klingt ein übermächtiger Staat als grosser Bruder an, der den kleinen, zerbrechlichen, machtunterlegenen Bürger durchleuchtet, überwacht und zum gläsernen Bürger degeneriert.[361] Ihm galt in den Anfängen die volle Aufmerksamkeit, ging man doch in der Zeit des Erlasses der ersten Datenschutzgesetze nicht davon aus, dass Private in gleichem Masse Personendatenbestände generieren und verarbeiten würden können.[362] Es

357 Jeanprêtre, AB 88.032, 5. Juni 1991, 944.
358 Erster Teil, III. Kapitel, A.
359 Zweiter Teil, V. Kapitel, 3.; zur Neueinbettung und Verblendung des Dualismus durch den Ausbau von Vorgaben, welche gemeinsam für beide Bereiche gelten, mit der Totalrevision vgl. dritter Teil, VIII. Kapitel, A.
360 Für die Schweiz seit der Veröffentlichung des PUK-Berichts schon Rüesch, AB 88.023, 13. März 1990, 132; Bründler, SJZ 1993, 129 ff., 129; vgl. Buchner, 26.
361 Vgl. beispielsweise Vesting, in: Ladeur (Hrsg.), 155 ff., 164; zum gläsernen Steuerpflichtigen vgl. Broger, zsis Monatsflash 7, 1 ff.
362 Hierzu der Hinweis von Simitis im Interview, abrufbar unter: <https://www.datenschutzzentrum.de/interviews/simitis/interview-simitis.mp3> (zuletzt besucht am 30. April 2021); Hoffmann-Riem, AöR 1998, 513 ff., 524 ff.; Vesting, in: Ladeur (Hrsg.), 155 ff., 165.

waren staatliche Stellen, die erste Grossrechenanlagen zum Einsatz brachten.[363] Die Diffundierung des Computers in die Gesellschaft hatte noch nicht stattgefunden.[364] Immerhin: Mit der Referenz auf den grossen Bruder Staat und der damit erfolgenden Anknüpfung an Verwandtschaftsbeziehungen wird bereits «ein (kleineres) Geschwister» impliziert. In der datenschutzrechtlichen Debatte sind damit Private, die Personendaten verarbeiten, gemeint.[365]

Die stark bildhafte Rhetorik unter diesem Aspekt – die für den rechtlichen Diskurs, der sich gerne fachlich-neutral präsentiert, so gar nicht passen will und gleichwohl in kaum einem juristischen Beitrag fehlt – lädt zu einigen Gedanken ein: 239

Chronologisch betrachtet ist es vorab der grosse Bruder als staatliche resp. amtliche resp. obrigkeitliche Stelle, dessen Personendatenverarbeitungen Widerstand und im Ergebnis auch die Forderung nach rechtlichen Beschränkungen auslösen. Wie im ersten Teil gezeigt, widmeten sich die Datenschutzgesetze der ersten Generation einzig der Regulierung von Datenbearbeitungen durch den Staat. Das erste Schweizer Datenschutzgesetz von 1993 dagegen reiht sich – nach einem langen Ringen um die Verabschiedung eines Normkomplexes auch für den privaten Bereich – in die zweite Generation ein:[366] Es formuliert Vorgaben für die Personendatenverarbeitung durch öffentliche Stellen des Bundes wie durch Private, vgl. Art. 2 Abs. 1 lit. a und lit. b DSG und Art. 2 Abs. 1 lit. a und lit. b nDSG. 240

Die *kognitive Annahme*, wie sie in der *Orwellschen Metapher* mitschwingt, hat im DSG Niederschlag gefunden: Das Hauptaugenmerk gilt der staatlichen Datenbearbeitung, die als grössere Bedrohung beurteilt und somit einer strengeren Regelung zugeführt wird als Personendatenverarbeitungen durch Private. Hierzu vertiefend was folgt: 241

Das DSG bleibt auch nach seiner Totalrevision ein *duales Gesetz* – ein Gesetz, das die Vorgaben für den öffentlichen Bereich des Bundes gegenüber dem privaten Bereich unterschiedlich gestaltet. Die besagte Differenzierung erfolgt sowohl in materiellrechtlicher wie auch verfahrensrechtlicher Hinsicht. Entsprechend war und bleibt die *bereichsspezifische Differenzierung ein charakteristisches Element* des schweizerischen Datenschutzgesetzes. Angelegt wurde sie im Zuge der Verabschiedung des ersten DSG. Eine komplette Vereinheitlichung i. S. der Identität der Normen für die Verarbeitung von Personendaten durch Private und 242

363 Simitis im Interview, abrufbar unter: <https://www.datenschutzzentrum.de/interviews/simitis/interview-simitis.mp3> (zuletzt besucht am 30. April 2021); Hoffmann-Riem, a. a. O.; Vesting, in: Ladeur (Hrsg.), a. a. O.

364 Von einer «Demokratisierung der Informationstechnologien» spricht Nissenbaum, 24, 1.

365 Ähnlich Buchner, 5.

366 Zur Generationeneinteilung Mayer-Schönberger, Information und Recht, 113 ff.; vgl. auch Weichert, in: Bäumler (Hrsg.), 158 ff., 160.

öffentliche Stellen des Bundes wurde – soweit ersichtlich – in der Schweiz bislang nicht dezidiert gefordert, auch nicht im Zuge der Totalrevision.[367]

243 Ein Bericht zur Totalrevision hält denn auch fest, dass das «einheitliche» Gesetz für den privaten und öffentlichen Bereich beibehalten, allerdings die Bestimmungen *soweit wie möglich* vereinheitlicht werden sollten.[368] Umgesetzt wird diese Annäherung über mehrere neue Instrumente, die *für beide Bereiche* gelten sollen: Exemplarisch zu nennen sind insofern die Vorgaben für den Datenschutz durch Technik und Voreinstellungen, Art. 7 nDSG; die Pflicht zur Erstellung eines Verarbeitungsverzeichnisses nach Art. 12 nDSG, die (annähernden) Vereinheitlichungen bezüglich der Informationspflichten nach Art. 19 nDSG oder die Datenschutz-Folgenabschätzung, Art. 22 nDSG.

244 Anders wurde die Vereinheitlichung der beiden Bereiche namentlich in Deutschland bereits im letzten Jahrhundert als richtungsweisend für die *Modernisierung des Datenschutzrechts* beschrieben.[369] Denn die sog. kleine Schwester – die Datenbearbeitung durch Private –, so wurde attestiert, sei längst ihren Kinderschuhen entwachsen: Im 21. Jahrhundert, für welches von der «elektronischen Eigenaufrüstung der Gesellschaft mit Datenverarbeitungstechnologien»[370] resp. der «Demokratisierung der Informationstechnologien»[371] gesprochen wird, werde das Individuum nicht nur von Datenbearbeitungen durch den grossen Bruder Staat bedroht, sondern auch und gerade durch Private wie Google, Facebook usf.[372] Die Forderung auf eine Vereinheitlichung wird nicht zuletzt mit der *Vergleichbarkeit der Bedrohungslage* begründet, die von Personendatenverarbeitungen durch staatliche Behörden und Private, insb. den Internetgiganten, ausgeht.[373] Zudem wurde der *Zugriff der Behörden auf die infolge eines Regimes mit niedrigerem Schutzniveau erlangten Personendaten der privaten Akteure pro-*

367 Vgl. immerhin Baeriswyl in: Baeriswyl/Rudin (Hrsg.), 47 ff., 59, demgemäss sich die ursprüngliche Unterscheidung zwischen Datenbearbeitungen im öffentlichen gegenüber dem privaten Bereich kaum mehr durchführen lasse.

368 Bericht der Begleitgruppe Revision DSG vom 29. Oktober 2014, Normkonzept zur Revision des Datenschutzgesetzes, 8.

369 M. w. H. Buchner, 36 f.

370 So Vesting, in: Ladeur (Hrsg.), 155 ff., 157 ff., insb. 161 f.

371 So Nissenbaum, 24, 1; vgl. auch zur Digitalisierung des Alltags Richter, in: Mehde/Ramsauer/Seckelmann (Hrsg.), 1041 ff.

372 Vgl. Hassemer, in: Simon/Weiss (Hrsg.), 121 ff., 126 f.; Buchner, 1 und 26 ff.; heute sind es nicht mehr nur Informations- und Kommunikationstechnologien, die in die Gesellschaft diffundiert sind. Vielmehr sind unzählige Alltagsgegenstände wie Autos, Kühlschränke usf. mit Informationsverarbeitungstechnologien ausgerüstet – vgl. zum Phänomen des Internet of Things mit einem Fokus auf vertragsrechtliche Fragestellungen z. B. Eggen, AJP 2016, 1131 ff.; zum weiteren Phänomen der Informatisierung des Alltags, insb. durch ubiquitous computing, die Beiträge gesammelt von Friedemann (Hrsg.), *passim*; zum Paradigmenwechsel mit seiner Abkehr von Grossrechnern in staatlicher Hand hin zu Kleinstrechnern Rudin, digma 2001, 126 ff., 127 f.; zur Durchdringung des Alltages der Informations- und Kommunikationstechnologien Mattern, in: Mattern (Hrsg.), 11 ff.

373 M. w. H. und kritisch zu dieser kognitiven Annahme Vesting, in: Ladeur (Hrsg.), 155 ff., 156 ff., insb. 160 ff.; ebenso kritisch Buchner, 44 ff.

blematisiert.[374] Eine mögliche regulatorische Schlussfolgerung könnte sein, die Personendatenverarbeitung durch Behörden wie Private identischen Vorgaben zu unterwerfen.[375]

245 Ebendiesen Schritt hat die Europäische Datenschutz-Grundverordnung, in Kraft seit dem 25. Mai 2016, vollzogen. Ihre Vorgaben sind gleichermassen auf öffentliche wie private Verantwortliche anwendbar. Ungeachtet dessen, dass die Totalrevision von diesen Entwicklungen in der EU mitangestossen war – die Implementierung eines Monismus stand nicht zur Debatte.[376]

246 In der Schweiz sind die datenschutzrechtlichen Auseinandersetzungen bis heute von einer starken Position zugunsten privatwirtschaftlicher Erwägungen geprägt. Ihr gemäss sollen Personendatenverarbeitungen durch Private resp. der private Bereich datenschutzrechtlich so weit wie möglich als freier Bereich gestaltet werden.[377] Illustrativ hierfür ist das im Zuge der Schaffung des ersten eidgenössischen Datenschutzgesetzes erfolgte Ringen, *überhaupt* einen Normkomplex für den privaten Bereich verabschieden zu können. Die Schaffung eines Normenkomplexes, auch für Personendatenverarbeitung durch Private, war während des gesamten Prozesses strittig; die Debatte prägte den gesamten Gesetzgebungsprozess.

247 Es lohnt sich, *Relevanz und Argumente dieser bereichsspezifischen Debatte im Rahmen der Verabschiedung eines ersten eidgenössischen Datenschutzgesetzes* genauer nachzuvollziehen. In der Schweiz bezog namentlich Tercier zur Notwendigkeit einer Datenschutzgesetzgebung, die sich auch auf den privaten Bereich erstrecken sollte, unmissverständlich Stellung:

> «Est-ce que les articles 28 ss ne suffisent pas? Ma réponse, et c'est ma conviction, est clairement non […]. Les articles 28 ss du Code civil ne donnent pas un arsenal suffisant. Pourquoi? Au moins pour deux raisons principales. La première, c'est que les articles 28 ss fonde sur des formulations à caractère très général. Or, nous sommes dans un domaine où les généralités ne suffisent pas. Il faut des notions claires, garantissant une sécurité juridique suffisante. Deuxièmement avec l'article 28, pour les ordinateurs en tout cas, on est dans un domaine où les armes du droit civil ne suffisent plus […].»[378]

248 Das Zitat dokumentiert, dass in der Schweiz von Anfang an Überzeugungsarbeit geleistet werden musste, um für den privaten Sektor *überhaupt* eine spezifische Datenschutzgesetzgebung erlassen zu können. Die Richtung, aus welcher sich der Schweizer Gesetzgeber der Datenschutzgesetzgebung annäherte, war damit vorgegeben.

374 Vesting, 72.
375 Grundlegend Ders., *passim*.
376 Hierzu dritter Teil, VIII. Kapitel.
377 BBl 1988 II 414 ff., 418 ff., insb. auch 428 ff.
378 Vgl. Danioth, AB 88.032, 13. März 1990, 125 ff., 126.

249 Eine Entscheidung, *dass* der private Sektor ebenso einer datenschutzrechtlichen Regelung zuzuführen sei, sagt noch nichts darüber aus, wie weit Schutzinstrumente und Schutzniveau für den privaten und den öffentlichen Bereich des Bundes einander angenähert werden sollen oder inwieweit die Normen für den öffentlichen gegenüber dem privaten Bereich im Datenschutzrecht differenziert oder (punktuell) einheitlich geregelt werden sollen.[379]

250 Das zumindest theoretisch markanteste und wirkungsmächtigste Instrument zur Gestaltung eines datenschutzrechtlichen Regimes ist die Fixierung des *Ausgangspunktes hinsichtlich der Personendatenverarbeitung: Freiheit der Datenbearbeitung als Grundsatz mit Schranken* einerseits oder *Verarbeitungsverbot als Grundsatz mit Erlaubnistatbeständen* andererseits.[380] Dass der Entscheid für den Ausgangspunkt ein leitendes Ordnungsprinzip des Datenschutzrechts ist, wurde in der Schweiz bislang ungenügend zur Kenntnis genommen. Erst im Zuge der Totalrevision wurde dieser Aspekt vermehrt thematisiert.[381]

251 Der gesetzgeberisch gewählte Ausgangspunkt stellt ein strukturelles Kernelement für die datenschutzrechtliche Konzeptionierung und für das Schutzniveau dar. Entsprechend dient er auch als Instrument zur bereichsspezifischen Differenzierung oder Angleichung.[382] Der Entscheid für einen bestimmten Ausgangspunkt ist anders gewendet ein *Kerninstrumentarium* zur Erreichung eines bestimmten Schutzniveaus, auch wenn sich die beiden Mechanismen annähern lassen: je grosszügiger die Erlaubnistatbestände im Grundsatz des Verarbeitungsverbotes, je schärfer die Verarbeitungsverbote resp. -schranken im Grundsatz der Verarbeitungsfreiheit, desto deutlicher die Annäherungen zwischen den beiden «Extrempolen». Umgekehrt liegt die Extremlösung für ein maximal divergierendes Schutzniveau für den öffentlichen und den privaten Sektor theoretisch gesprochen darin, für einen Sektor ein Verarbeitungsverbot mit eng formulierten Ausnahmetatbeständen zu definieren und für den anderen Sektor die Freiheit der Datenbearbeitung mit rudimentären Verarbeitungsverboten festzulegen.[383]

252 Dem Entscheid dürfte *präjudizierende* Wirkung zugemessen werden in dem Sinne, dass sich nicht nur die weiteren Gesetzesnormen, sondern auch die Rechtsauslegung daran zu orientieren haben: Ein Bereich, der als prinzipiell freier resp. nicht durchregulierter Bereich konzipiert wird, sollte konsequent gestaltet

379 Grundlegend hierzu Buchner, 5 ff.
380 Vgl. hierzu ebenso Ders., 80 ff.; für die USA und den Beginn dieser Vision in den 1930er Jahren Regan, xii.
381 Rosenthal, Jusletter 16. November 2020, N 7 ff.; Glatthaar, 1.
382 Man könnte an dieser Stelle geneigt sein zu folgern, dass der Ausgangspunkt das Schutzniveau des Datenschutzrechts selbst ist. Dass dem nicht so ist, wird an späterer Stelle deutlich werden, wo auf weitere Instrumente, die das Schutzniveau mitgestalten, eingegangen wird.
383 Zum Ganzen Buchner, 80 ff.

werden. Zudem sind auslegungsbedürftige Bestimmungen systemkongruent zu interpretieren.[384]

Die nachfolgenden Ausführungen wollen vor diesem Hintergrund in Erinnerung 253
rufen, wie zentral das Ringen um ein Datenschutzgesetz für den privaten Bereich und in der Folge die Frage nach der differenzierten Gestaltung der Vorgaben für den öffentlichen und den privaten Bereich in der Schweiz war. Im schweizerischen Schrifttum vermochte sich die grundlegende Bedeutung der Differenzierung resp. der Nichtdifferenzierung zwischen Privatrecht und öffentlichem Recht im Datenschutz, basierend auf einer Analyse stichhaltiger und sachlicher Argumente, bislang nicht abzubilden. Im Zuge der Totalrevision wurde das Konzept nicht ernsthaft verhandelt; immerhin thematisiert die Lehre den Ausgangspunkt gemäss DSG. Anhand des politischen Prozesses im Rahmen der Verabschiedung des ersten Datenschutzgesetzes lässt sich die Relevanz der bereichsspezifischen Auseinandersetzung herausarbeiten. Insofern soll auch beleuchtet werden, welche strukturellen Entscheidungen die Differenzierung dazumals prägten. Es geht insofern zum einen um den gewählten Ausgangspunkt für die Personendatenverarbeitungen für den privaten resp. den öffentlichen Bereich. Zum anderen sind weitere Elemente zu beschreiben, die dazu Anlass geben, das DSG – namentlich wegen des entgegengesetzten Ausgangspunktes – als *duales Regime* zu qualifizieren. Eine Charakterisierung, die für ein Gesetz, das gemeinhin als Einheitsgesetz beschrieben wird, nicht offensichtlich ist.[385] Verschiedenes gilt es bereits an dieser Stelle anzufügen: Erstens finden sich auch im DSG gemeinsame Schnittmengen der Normierung für den öffentlichen gegenüber dem privaten Bereich, insb. anhand der gemeinsamen Verarbeitungsgrundsätze. Das Verhältnismässigkeitsprinzip, das in seiner öffentlichen Natur auch für den privaten Bereich gilt, führt zu einer teilweisen Annäherung der beiden Regime: Ein öffentlich-rechtliches Prinzip annektiert quasi den privaten Bereich. Zudem bringt die Totalrevision gewisse Modifikationen durch Einführung neuer Instrumente, die für beide Bereiche gelten. Mit ihnen geht zwar keine Anpassung des materiellrechtlichen Grundsatzentscheides in Bezug auf den Ausgangspunkt einher. Gleichwohl stellen diese für beide Bereiche vorgeschriebenen Instrumente zur Umsetzung einer Datenschutz-Compliance den Dualismus in ein etwas anderes Licht.

384 Der Befund hat namentlich auch für ein Regelungsregime hohe Bedeutung, das generalklauselartig normiert; vgl. hierzu zweiter Teil, V. Kapitel.

385 Vgl. zur Titulierung als Einheitsgesetz durch Bundesrat Koller, AB 88.032, 5. Juni 1991, 948; Danioth, AB 88.032, 13. März 1990, 127; Ders., in: Schweizer (Hrsg.), 9 ff., 9.

B. Duales Einheitsgesetz

1. Von Titulierung und Inhalt

> «Die Notwendigkeit von datenschutzrechtlichen Regeln sowohl für den privaten wie den öffentlichen Bereich zu bejahen, warf die Frage – ich möchte sogar sagen: die Kontroverse – auf, ob es sinnvoll und angezeigt sei, die Bestimmungen der beiden Rechtsgebiete in je einem separaten Erlass zu behandeln oder in einem einzigen Erlass zusammenzufassen, wie es der Bundesrat vorschlägt. Die Kommission hat die Vorteile eines Einheitsgesetzes höher gewichtet als unbestreitbare Nachteile.»[386]

254 1992 trat auf eidgenössischer Ebene ein Datenschutzgesetz in Kraft, das die Verarbeitung personenbezogener Daten für den öffentlichen Bereich des Bundes wie auch im privaten Sektor normierte. Unter dem sog. *persönlichen Geltungsbereich* definiert das DSG seinen Adressatenkreis und verankert mit Art. 2 Abs. 1 lit. a DSG, dass das DSG für die Bearbeitung von Daten durch *Private* – gemäss lit. b auch für diejenige durch die *Bundesbehörden* – einschlägig ist.[387]

255 Diese Regelung in Bezug auf die Adressaten steht im Einklang mit der verfassungsrechtlichen Kompetenzausscheidung.[388] Aus der privatrechtlichen Regelungskompetenz ergibt sich ebenso die Kompetenz, im Bereich des privatrechtlichen Datenschutzes zu normieren.[389] Sodann ist der Bund zuständig, das öffentliche Recht des Bundes zu erlassen, worauf auch die Regulierung der Datenbearbeitung durch Bundesorgane basiert. Nicht anwendbar ist das DSG grundsätzlich auf Personendatenverarbeitungen durch kantonale und kommunale Behörden;

386 Danioth mit Verweis auf eine ähnliche, vereinte Regelung im UWG oder Kartellrecht, AB 88.032, 13. März 1990, 127.

387 Identisch nach Totalrevision Art. 2 Abs. 1 nDSG; Abgrenzungsschwierigkeiten können sich insb. im Rahmen der Wahrnehmung öffentlicher Aufgaben durch privatrechtlich angeknüpfte Unternehmen ergeben. Auf eine Vertiefung dieses Themas wird verzichtet.

388 Art. 3 BV sieht als Grundregel für die bundesstaatliche Kompetenzverteilung das Prinzip der Einzelermächtigung vor, wonach der Bund nur über jene Zuständigkeiten verfügt, die ihm die Bundesverfassung zuweist. Hierbei lautete Art. 3 BV 1848 und 1874: «Die Kantone sind souverän, soweit ihre Souveränität nicht durch die Bundesverfassung beschränkt ist, und üben als solche alle Rechte aus, welche nicht der Bundesgewalt übertragen sind.» Die aktuelle Version ist seit der Revision 1999 in Kraft, vgl. insb. auch Art. 42 BV: «Der Bund erfüllt die Aufgaben, die ihm die Bundesverfassung zuweist.» Art. 42 f. wurden mit der Revision 1999 eingeführt, die Subsidiaritätsklausel später gestrichen bzw. in Art. 5a und Art. 43a BV verschoben. Die einzelermächtigenden Kompetenzen des Bundes auf dem Gebiet des Privatrechts waren Art. 64 aBV sowie die Verfassungsnorm zur Erhaltung der Lauterkeit im Geschäftsverkehr, Art. 31 bis Abs. 2 aBV. Die Zivilrechtskompetenz des Bundes geht teils auf das Jahr 1874 zurück (BV 1874 Art. 64 Abs. 1: insb. wirtschaftsrelevante Bereiche; vgl. auch BV 1874 Art. 53 Abs. 1), teils auf das Jahr 1898 (BV 1874 Art. 64 Abs. 2: übrige Gebiete des Zivilrechts), teils auf das Jahr 1905 (BV 1874 Art. 64 Abs. 1: Patente, Muster und Modelle) zurück, vereinzelt sogar auf das Jahr 1848 (BV 1848 Art. 49: Vollstreckung rechtskräftiger Zivilurteile). Heute obliegt dem Bund die Regelung des Privatrechts aufgrund von Art. 122 Abs. 1 BV.

389 Zu diesem Anwendungsbereich Art. 2 Abs. 1 lit. a DSG; nach Totalrevision Art. 2 Abs. 1 lit. a nDSG.

insofern greifen die kantonalen Datenschutzgesetze. Deren Einhaltung wird von kantonalen Datenschutzbeauftragten überwacht.[390]

256 Das eidgenössische Datenschutzgesetz formuliert in den Art. 4 ff. DSG resp. nach Totalrevision gemäss Art. 6 nDSG unter den «allgemeinen Bestimmungen» *gemeinsame Verarbeitungsgrundsätze für beide Bereiche*. Diese allgemeinen Grundsätze, die Leitplanken für beide Bereiche setzen, weisen Parallelen zum Einleitungstitel des ZGB auf, und zwar in *zweifacher Hinsicht*: Es handelt sich zum einen um die grundlegenden Prinzipien des Datenschutzrechts, die für beide Bereiche Wirksamkeit entfalten sollen. Vergleichbare Grundsätze formuliert die Europäische Datenschutz-Grundverordnung in Art. 5 DSGVO. Die allgemeinen Verarbeitungsgrundsätze erfüllen anders gewendet eine Art Leitsternfunktion für beide Bereiche, ähnlich wie der Einleitungstitel des ZGB mit seinen fundamentalen Prinzipien für das gesamte Privatrecht (und keineswegs bloss für das ZGB) wirksam werden soll (oder gar darüber hinaus wirkt).[391] Zum anderen werden im Datenschutzgesetz zentrale Prinzipien des Einleitungstitels wie Treu und Glauben zu allgemeinen Verarbeitungsgrundsätzen gemacht.[392] *Materiellrechtlich* sind sie das Herzstück des Datenschutzgesetzes. Allerdings, so wird zu zeigen sein, sind die allgemeinen Verarbeitungsgrundsätze im DSG – anders als in der DSGVO – für den öffentlichen und privaten Bereich *in zwei unterschiedliche Systeme* eingebettet. Ebendies führt zu einer signifikanten Unterschiedlichkeit der datenschutzrechtlichen Regime.

257 Für das DSG hat sich, weil es die Personendatenverarbeitung durch Bundesbehörden wie Private normiert, die Beschreibung *Einheitsgesetz* etabliert.[393] Allerdings vermag diese Titulierung den strukturellen Gehalt des DSG nicht abzubilden – im Gegenteil wird mit dem Titel ein Rechtskonzept assoziiert und suggeriert, das sich im Gesetz gerade nicht findet. Dass nach DSG für den privaten und den öffentlichen Sektor beträchtliche Divergenzen gelten, rückt mit der Benennung und Qualifizierung des DSG als Einheitsgesetz aus dem Blickfeld. Die Titulierung überdeckt die eigentliche *materiellrechtliche Kernfrage* jeder datenschutzrechtlichen Regulierung und die hierzu getroffenen Entscheidungen:[394] diejenige nach der bereichsspezifischen Differenzierung oder auf deren Verzicht.

390 Vgl. zum föderalistischen System der Schweiz, das sich auch im Datenschutzrecht niederschlägt, Rudin, SJZ 2009, 1 ff.; zum datenschutzrechtlichen Regelungsgefecht, dem DSG, den kantonalen Datenschutzgesetzen sowie den Spezialgesetzen vgl. Epiney/Hofstötter/Meier/Theuerkauf, 221 ff.

391 Honsell, BSK-ZGB I, Einleitung vor Art. 1 ff. N 1.

392 Allerdings: Während dem Einleitungstitel des ZGB konkretisierende und ausgereifte Normenkomplexe mit erheblicher Regelungsdichte zu den einzelnen Verhältnissen folgen, bleiben die hoch abstrakten Grundsätze von Art. 4 ff. DSG resp. Art. 6 nDSG weitgehend ohne nähere Konkretisierung für den datenschutzrechtlichen Kontext.

393 Vgl. Art. 2 DSG und Art. 2 nDSG; s. EJPD, Bericht Begleitgruppe, 3; vgl. z. B. Danioth, AB 88.032, 13. März 1990, 127; BBl 1988 II 414 ff., 431; Maurer-Lambrou/Kunz, BSK-DSG, Art. 1 N 6.

394 Dazu namentlich für Deutschland Vesting, in: Ladeur (Hrsg.), 155 ff., 156 ff.; Buchner, *passim*.

258 In der Entscheidung für eine vereinheitlichte resp. monistische Normierung schlägt sich die Überzeugung nieder, dass die Bedrohungen, die von Datenverarbeitungen durch den Staat und Private unter den Gegebenheiten moderner Verarbeitungstechnologien ausgehen, vergleichbar, ja identisch sind und folglich eine rechtliche Differenzierung nicht sachgemäss erscheint – so der Ansatz in der DSGVO. Im Entscheid für ein materiellrechtlich zweigeteiltes Datenschutzrecht manifestiert sich hingegen die Überzeugung, dass grundsätzliche Unterschiede zwischen den Bearbeitungskontexten bestehen.[395] In der Schweiz hat sich letztere durchgesetzt und gehalten. Die Differenzierung zwischen den beiden Bereichen im schweizerischen Datenschutzgesetz wurde zwar von fachlichen und sachlichen Argumenten mitgetragen, war allerdings bei Lichte betrachtet stark von *politischen Kräften* getrieben; namentlich die Interessen vonseiten der Privatwirtschaft nahmen massgeblichen Einfluss.[396]

259 Wer das eidgenössische Datenschutzgesetz als *Einheitsgesetz* in der Hand hält, realisiert wenig von der Brisanz, Virulenz und Spannungshaftigkeit, aus der es damals hervorging. Lässt man die Stellungnahmen vonseiten der Expertengremien sowie die Voten in den Räten Revue passieren, kommt schnell ans Licht, wie kontrovers über Schutzniveau und Regelungsinstrumente für den privaten und den öffentlichen Sektor sowie über das Verhältnis der Datenschutzgesetzgebung für die beiden Bereiche debattiert wurde. Die Gesetzgebungsmaterialien dokumentieren die *politischen Kräfte und Dimensionen*, die hinter dem eidgenössischen Datenschutzgesetz als Einheitsgesetz wirk(t)en.

260 Illustrativ insofern der strategische Entscheid, beide Sektoren formell in einem Gesetz zur Abstimmung zu bringen: Er erfolgte aus *politischem Kalkül*.[397] Denn während die Normierung für den öffentlichen Sektor Rückenwind genoss, sah sich diejenige für den privaten Sektor starkem Gegenwind ausgesetzt. Nur indem *ein* Gesetz für beide Bereiche vorgelegt wurde, konnte Schiffbruch und eine (partielle) Ablehnung einer Gesetzgebung für den privaten Sektor verhindert werden. Zwar wurde hinterfragt, ob dieses Vorgehen mit den politischen Rechten und namentlich dem Grundsatz der Einheit der Materie im Rahmen der Gesetzgebung im Einklang stand.[398] Das fusionierende Vorgehen schien – nicht zuletzt, weil es sich beim Datenschutz um eine sog. Querschnittsmaterie handle – gleichwohl als opportun und legitim.[399] Im Ansatz wurde eine Überzeugung dokumentiert, wonach es für das Individuum, dessen Schutz im Zentrum stünde, nicht relevant sei, ob Datenbearbeitung durch den Staat oder Private erfolge.[400] Wie aber gestaltete

395 Buchner, 5.
396 Hierzu sogleich 2., wo der Weg zum Zweikammersystem abgeschritten wird.
397 Forstmoser, digma 2003, 50 ff., 50 f.
398 Müller, LeGes 2013, 507 ff., 507.
399 Danioth, AB 88.032, 13. März 1990, 127; Nabholz, AB 88.032, 5. Juni 1991, 940.
400 Vgl. Küchler, AB 88.032, 13. März 1990, 128 f.

sich der Prozess des Austarierens datenschutzrechtlicher Normierung(en) für den privaten und den öffentlichen Sektor im Folgenden und Einzelnen?

2. Der Weg zum datenschutzgesetzlichen Zweikammersystem

261 Den langwierigen Gesetzgebungsprozess im Rahmen der Verabschiedung des ersten eidgenössischen Datenschutzgesetzes retrospektiv nachzuzeichnen, ist kein einfaches Unterfangen.[401] Eine solche Rückblende über das erst gerade abgeschlossene Gesetzgebungsprojekt der Totalrevision ist für diese Studie und ihre Forschungsfragen allerdings unverzichtbar. Sichtbar wird damit, welcher Stellenwert der Frage der bereichsspezifischen Differenzierung zugewiesen wurde und welche Argumente insofern vorgetragen wurden. Im Ergebnis wurde ein Gesetz verabschiedet, dessen *erstes Charakteristikum in seiner dualistischen Struktur* liegt.

262 Der Gesetzgebungsprozess, der zur Verabschiedung des ersten eidgenössischen Datenschutzgesetzes führte, war vom Druck und Widerstand vonseiten der *Wirtschaftsakteure* auf die datenschutzrechtliche Normierung für den privaten Bereich geprägt.[402] Unbestritten war, dass nicht nur für die moderne Leistungsverwaltung Personendaten unverzichtbar seien, sondern auch für private Versicherungsunternehmen, Kreditinstitute oder Arbeitgeber.[403] Dies reflektierend sollte eine Normierung für den privaten Sektor der Bedeutung von Informationsbeschaffungen und dem wirtschaftlichen Wettbewerb Rechnung tragen.[404] Die konkrete Ausgestaltung des Datenschutzgesetzes für den privaten Sektor gegenüber dem öffentlichen Sektor beschäftigte die involvierten Akteure während des gesamten Gesetzgebungsprozesses. Die Verhandlungen insofern waren mit hoher Ambivalenz belegt und sind als eigentlicher Brennpunkt der schweizerischen Datenschutzgesetzgebung zu bezeichnen.

263 In Bezug auf den Aspekt des *Dualismus* ist vorab relevant, dass der dazumal amtierende Vorsteher des EJPD, Altbundesrat Furgler, *im Vorfeld* richtungsweisende Entscheidungen traf: Einerseits sollte bundesgesetzlich sowohl die Personenbearbeitung durch Private wie durch Bundesbehörden geregelt werden, wohingegen die Bearbeitung durch kantonale und kommunale Behörden mangels einer allgemeinen Kompetenznorm im Bereich des Datenschutzes der kantona-

401 Von einer wechselvollen Geschichte, die ihren Anfang mit der Motion Bussey im Jahr 1971 nahm, spricht Kleiner, in: Brem/Druey/Kramer/Schwander (Hrsg.), 397.

402 Jaggi, AB 88.032, 13. März 1990, 161 f. mit Hinweis auf die Konzessionen in den Domänen Direktmarketing, Kreditauskunfteien und die Kompetenzen des EDÖB; der politische Druck vonseiten der wirtschaftlichen Kreise nahm seinen Anfang bei den Arbeiten der Kommissionen.

403 Forstmoser, SJZ 1974, 217 ff., 218.

404 BBl 1988 II 414 ff., 430 und 434; grundlegend zu Ansprüchen auf Informationsbeschaffungen vor der Verabschiedung des DSG vgl. Hauser, 19 ff.

len Normierung oblag. Andererseits wurde die Einsetzung zweier verschiedener Expertengruppen beschlossen: Die erste wurde 1977 mit der Ausarbeitung von Datenschutzvorschriften für die Bundesverwaltung beauftragt, die zweite 1979 mit derjenigen für den privaten Bereich. Beide Arbeitsgruppen standen unter der Leitung von Pedrazzini.[405] Vonseiten der mit der Ausarbeitung betrauten Stellen und Personen hielt man es von Anfang an für *sachgerecht*, eine differenzierende Regelung für beide Sektoren zu veranlassen. Man orientierte sich entsprechend an einem fest etablierten Konzept eines «Zweikammersystems», dessen eine Kammer der Privatrechtsbereich und dessen andere Kammer der öffentlich-rechtliche Bereich darstellt.[406]

264 Die erste Expertengruppe legte Ende 1981 einen Vorentwurf für ein Bundesgesetz über den Datenschutz im Bereich der Bundesverwaltung vor.[407] Die zweite Expertenkommission präsentierte ihren Gesetzesentwurf für den privatrechtlichen Sektor im Sommer 1982. Als die beiden Vorentwürfe vorlagen, erteilte der Vorsteher des EJPD den bemerkenswerten Auftrag, diese *in einem einzigen Gesetz zusammenzulegen*. In diese Fusion des Vorentwurfs für ein Bundesgesetz über den Datenschutz im Bereich der Bundesverwaltung von 1981 und des Vorentwurfs für den privatrechtlichen Bereich von 1982 wurden zudem die Ergebnisse des Berichts und die Empfehlungen für den Medizinalbereich integriert, deren Erarbeitung unter der Leitung von Jaggi stand. Das Ergebnis war der *Vernehmlassungsentwurf von 1983*.[408]

265 Mehrere Gründe standen hinter dem Entscheid, die verschiedenen Regelungsbereiche – obschon man von Anfang an einem differenzierten System zuneigte – in *einem* Gesetz zu fusionieren: Vorab sprach als *sachlogisches Argument* für die Zusammenlegung der beiden Bereiche der Befund, dass Datenschutz eine *Querschnittsmaterie* sei und entsprechend gesetzlich ein gemeinsames Fundament für beide Bereiche vorgesehen werden sollte.[409] So sollten Leitprinzipien der Datenverarbeitung, wie sie sich in Gestalt allgemeiner Bearbeitungsgrundsätze in ausländischen Rechtsordnungen Anerkennung verschafft hatten, auch im Schweizer Datenschutzgesetz gelten, und zwar für beide Bereiche. Dazu sollte ein prozedurales Instrumentarium gleichermassen in beiden Feldern zum Einsatz kommen, namentlich Auskunftsrechte, aber auch die Funktion eines Datenschutzbeauftragten. Gleichzeitig sollte mit der Zusammenlegung einer Kritik an der Gesetzesflut entgegengetreten werden: Der Verabschiedung eines einzigen

405 Seethaler, BK-DSG, Entstehungsgeschichte DSG, N 27 f.
406 Die in dieser Schrift als «pointierter Dualismus» beschriebene Rechtsgestaltung ist ein Element insofern.
407 BBl 1988 II 414 ff., 426 f.; zum Ganzen vertiefend Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 18.
408 BBl 1988 II 414 ff., 426.
409 Danioth, AB 88.032, 13. März 1990, 126.

Gesetzes wurden vor dem Hintergrund dieses Einwandes bessere Erfolgschancen zugemessen.[410]

Das Hauptargument für die Zusammenlegung lag allerdings – wie gezeigt – an anderer Stelle: Früh zeichnete sich ab, dass einer allgemeinen Datenschutzgesetzgebung für den privaten Sektor heftiger Widerstand erwachsen würde. Dass ein Gesetz für die Datenbearbeitung im öffentlichen Sektor Schiffbruch erleiden könnte, fürchtete angesichts der Vorkommnisse im EJPD und namentlich der Informationstätigkeiten der Bundesanwaltschaft kaum jemand. Der sog. Fichenskandal, der zur Einsetzung einer PUK geführt hatte, und der Bericht derselben, die dem Parlament zeitlich noch vor der Beratung des Datenschutzgesetzes vorgelegt worden war, hatte die Schweiz zutiefst erschüttert.[411] Ein Staat, der sich als Schnüffelstaat entpuppt hatte, gab einer Grenzen setzenden Gesetzgebung selbst den finalen Impetus. In der Folge galt als der neuralgischste Bereich der Datenbearbeitung derjenige durch Bundesorgane.[412] Die Zugkraft, die der politische Prozess zur Verabschiedung eines Datenschutzgesetzes für Datenbearbeitungen durch Bundesbehörden infolge des Fichenskandals entfaltete, konnte nun als starkes Vehikel für eine Normierung des privaten Sektors genutzt werden. Die Fusionierung war *primär politisches Kalkül.* 266

Mit der Zusammenlegung erfolgte sodann nicht nur eine *Reduzierung des Umfangs* auf rund die Hälfte der ursprünglich entworfenen Bestimmungen. Gleichzeitig wurden bereits erste Konzessionen bezüglich der Vorgaben für den privaten Bereich gemacht.[413] So sollte etwa das Auskunftsrecht nicht voraussetzungslos gelten – vielmehr sollte die Auskunft infolge eines überwiegenden Interesses verweigert werden können. 267

Zu diesem ersten Vernehmlassungsentwurf von 1983 hielt der von 2001–2015 amtierende Datenschutz- (und später Öffentlichkeits-)beauftragte Thür fest: 268

> «[A]ls das erste Vernehmlassungsverfahren durchgeführt wurde und der erste Expertenentwurf vorlag, war das Resultat vernichtend. Vor allem von wirtschaftlichen Interessengruppen wurde ein eigentliches Sperrfeuer entfacht.»[414]

Während die Bestimmungen zum öffentlichen Sektor in der Vernehmlassung grundsätzlich gut aufgenommen wurden, stiessen die Normen zum Privatbereich bei den Arbeitgeber- und Wirtschaftsorganisationen – vorbehältlich der Konsu- 269

410 M. w. H. Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 17 ff., N 28 ff. und N 34 ff.; Forstmoser, digma 2003, 50 ff., 52.
411 Vgl. hierzu Kreis, digma 2009, 56.
412 Hilty, NZZ 1994, 22.
413 Zu diesen Abschwächungen im Zuge der Vereinigung Jaggi, AB 88.032, 13. März 1990, 131.
414 Thür, AB 88.032, 5. Juni 1991, 945.

mentenverbände – auf gänzliche Ablehnung.[415] Eine privatrechtliche Normierung wurde nicht nur per se kritisiert. Bemängelt wurde die geplante gemeinschaftliche Regelung für die beiden Sektoren, womit den grundlegenden konzeptionellen Unterschieden, so hiess es, nicht gebührend Rechnung getragen würde. Darüber hinaus mache ein Einheitsgesetz den Erlass zu kompliziert.[416] Die Vorgaben für den privaten Sektor seien zu umfangreich, engmaschig und komplex.[417] In diesem Sinne wurden vonseiten der Privatwirtschaft zwei getrennte Gesetze sowie eine Abschwächung der rechtlichen Vorgaben für gewisse wirtschaftliche Tätigkeiten, beispielsweise diejenigen, welche Kreditauskunfteien vornähmen, gefordert.[418] Dieser Vorstoss war seinerseits strategisch motiviert: Die Vertreterinnen und Vertreter der Privatwirtschaft versuchten, den Normenkomplex für den privatrechtlichen Sektor wieder zu isolieren, um ihn später verhindern zu können. Nicht nur der Bundesrat sah sich damit in seiner ursprünglichen Einschätzung bestätigt, wonach es ein prioritäres Ziel bleiben musste, *überhaupt* eine Regulierung für den privatrechtlichen Bereich zur Verabschiedung zu bringen.

270 Nach Kenntnisnahme der Ergebnisse der Vernehmlassung setzte der Bundesrat erneut eine Arbeitsgruppe unter der Leitung von Pedrazzini ein. Trotz der Einwände zum Vernehmlassungsentwurf und namentlich zum Vorwurf vonseiten der Privatwirtschaft, die den Vernehmlassungsentwurf für den privaten Bereich als einen zu hohen Vollzugsaufwand auslösend beurteilte, hielt man an der Überzeugung fest, dass die Persönlichkeit auch vor Datenbearbeitungen im privaten Sektor geschützt werden müsse. Der Auftrag an die Arbeitsgruppe war, eine entsprechende Überarbeitung an die Hand zu nehmen. Es resultierte ein gestraffter Entwurf, der sich weiterhin sowohl auf den öffentlichen wie den privaten Sektor erstreckte, die Bereiche aber gleichwohl stärker trennte. Allerdings erschien auch diese gestraffte Version der damaligen Departementsvorsteherin Kopp als zu komplex. Eine verwaltungsinterne Arbeitsgruppe unter der Leitung von Steinlin wurde mit einer weiteren Überarbeitung betraut. 1988 – also elf Jahre nach der Einsetzung einer Expertengruppe zur Erarbeitung eines Datenschutzgesetzes – wurde der Gesetzesentwurf mit Botschaft vom 23. März 1988 vorgelegt.[419] Ergänzend erfolgten Gesetzgebungsaktivitäten für bereichsspezifische Regulierungen, namentlich für den Medizinal- und Sozialversicherungsbereich.[420]

415 BBl 1988 II 414 ff., 429; vgl. Forstmoser, digma 2003, 50 ff., 53; dies geschah ungeachtet der bereits im Jahr 1985 zu findenden wissenschaftlichen Einschätzung, wonach die private Informationsverarbeitung intransparenter und unberechenbarer sei als die staatliche.
416 BBl 1988 II 414 ff., 428 ff.
417 M. w. H. Nabholz, in: Schweizer (Hrsg.), 1 ff., 2.
418 Hinweise bei Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 26 ff.; vertiefend zur Praxis der Kreditauskunfteien dritter Teil, VII. Kapitel, B.2.2.
419 Vgl. Ders., a. a. O.
420 Ders., a. a. O.

Die *Botschaft* äussert sich prioritär – einleitend und eindringlich – zur Notwendigkeit, den öffentlichen *und* den privaten Sektor einer Regulierung zuzuführen. Gefahren würden sowohl in Informationstätigkeiten von Bundesbehörden wie in denjenigen von Privaten lauern.[421] Mehrere Argumente leisteten alsdann die notwendige Überzeugungsarbeit für die Verabschiedung des Regelungskorpus für den privaten Bereich: Zunächst werden bedeutsame Gerichtsentscheide, die sich mit Persönlichkeitsverletzungen durch private Informationstätigkeiten befassten, aufgeführt.[422] Dabei gab man zu bedenken, dass Verletzungen der Geheim- resp. Privatsphäre nur selten publik würden, weil Private meist gar nicht wüssten, wer über sie Daten bearbeite. Dort, wo eine Verletzung vermutet werde und feststellbar sei, werde allerdings in der Regel eine Auskunft über die Datenbearbeitung verweigert. Eine gerichtliche Beurteilung von Persönlichkeitsverletzungen wegen Informationsverarbeitungen durch Private sei zudem mit erheblichen Prozessrisiken verbunden.[423] Als Beleg für den Bedarf einer privatrechtlichen Regelung werden sodann vorhandene Instrumente der Selbstregulierung privater Organisationen in Gestalt von berufsethischen Normen oder Standesregeln genannt.[424] 271

In den parlamentarischen Beratungen setzte sich die Kontroverse um das Verhältnis datenschutzrechtlicher Vorgaben für den privaten und den öffentlichen Sektor indes weiter fort. Erstberatend war der Ständerat; er verhandelte die Vorlage 1990. Es seien insofern die Worte des berichterstattenden Vertreters der vorberatenden Ständeratskommission Danioth aufgeführt: 272

> «Die Kommission […] bejahte einhellig die Notwendigkeit einer gesetzlichen Regelung des Datenschutzes auch im Privatrechtsbereich. Die unrühmlichen Vorkommnisse in der Bundesverwaltung dürfen nicht zur Annahme verleiten, in der Wirtschaft und anderen Bereichen seien keine Irrtümer und Missbräuche denkbar. Die Bejahung einer Gesetzgebung hat auch einen gleichsam rechtspraktischen Grund. Experten der Wissenschaft und der Praxis haben überzeugend dargetan, dass eine datenschutzrechtliche Konkretisierung des Persönlichkeitsschutzes durch den Gesetzgeber nicht zuletzt im Interesse der Wirtschaft und aller privaten Datenbearbeiter selber liegt […]. Im öffentlichen Bereich, das heisst bei der Bundesverwaltung, einen griffigen Datenschutz zu begründen, bedeutete wohl, Wasser in die Reuss oder in die Aare zu tragen. Die Aktualität lässt sich angesichts der sich jagenden Fichen-Enthüllungen kaum mehr überbieten. Unweigerlich muss man bedauern, dass der Gesetzgeber nicht schon lange gehandelt hat. Denn Letzterem wurde

421 BBl 1988 II 414 ff.; dazu, dass international wie national kein Datenschutzgesetzgeber zögerte, sich an die Adresse privater wie öffentlicher Stellen zu wenden, Simitis, NJW 1984, 394 ff., 401.

422 BBl 1988 II 414 ff., 418 f.

423 BBl 1988 II 414 ff., 420.

424 BBl 1988 II 414 ff., 419; der Selbstregulierungsansatz wird im revidierten Datenschutzgesetz aufgenommen, vgl. Botschaft DSG 2003, 2101 ff., 2138; zur Forderung auf eine Stärkung des Selbstregulierungsansatzes bereits um die Jahrtausendwende Rossnagel/Pfitzmann/Garstka, in: Bundesministerium des Inneren (Hrsg.), 43 ff.; vgl. zur Selbstregulierung sowie Zertifizierung unter Darstellung der hierzu vertretenen Ansichten betreffend die (Un-)Tauglichkeit der Selbstregulierung als Ausweg aus der Datenschutzkrise Pärli, digma 2011, 67 ff.; zur jüngsten Stärkung deskriptiv und ohne Evaluierung Hofmann/Meyer, Expert Focus 2017, 424.

> aus Wirtschaftskreisen starkes Misstrauen entgegengebracht. […] Die Notwendigkeit von datenschutzrechtlichen Regeln sowohl für den privaten wie den öffentlichen Bereich zu bejahen, warf die Frage – ich möchte sogar sagen: die Kontroverse – auf, ob es sinnvoll und angezeigt sei, die Bestimmungen der beiden Rechtsgebiete in je einem separaten Erlass zu behandeln oder in einem einzigen Erlass zusammenzufassen, wie es der Bundesrat vorschlägt. Die Kommission hat die Vorteile eines Einheitsgesetzes höher gewichtet als unbestreitbare Nachteile, was bei einer solchen Gesetzgebung übrigens nicht erstmalig ist (ich verweise auf das UWG, das Kartellrecht). Mit einem Einheitsgesetz wird dem Umstand Rechnung getragen, dass es sich um eine sogenannte Querschnittsmaterie handelt. Datenschutz ist nicht an Rechtskategorien gebunden.»[425]

273 Im *Ständerat* wurde von verschiedener Seite betont, dass das Gefahrenpotential im staatlichen Bereich deutlich höher sei als im privaten.[426] Folglich hatten nicht nur der Berichterstatter der ständerätlichen Kommission, sondern auch die Ständeräte selbst wiederum Überzeugungsarbeit für die privatrechtliche Normierung zu leisten. Es waren vorrangig Ständerätin Jaggi und Ständerat Onken, die sich in der kleinen Kammer für den privatrechtlichen Datenschutz engagierten. Rhinow – zu jenem Zeitpunkt nicht nur ordentlicher Professor für Staats- und Verwaltungsrecht an der Universität Basel, sondern auch Ständerat – nahm eine differenzierte Position ein:

> «Der moderne Sozialstaat zeichnet sich nicht nur durch einen Normenhunger, sondern auch durch einen hohen Bedarf an gespeicherten Personendaten aus […].»[427]

274 Zugleich plädierte er für eine Verbesserung des Datenschutzes ebenso für den privaten Sektor, weil Menschen in ihrer Persönlichkeit auch durch den Datenhunger privater Wirtschaftsunternehmer bedroht werden könnten. Entsprechend sei es richtig, beide Gebiete zu regeln, allerdings ebenso richtig, die beiden Gebiete unterschiedlichen Regelungsregimen zu unterstellen.[428]

275 Ebendieses Konzept – Regulierung für beide Gebiete *ja*, identische Regelung allerdings *nein* – setzte sich durch. Es war auch der Ständerat, der zugunsten der Verabschiedung eines DSG für beide Sektoren die Differenz zwischen öffentlichem und privatem Sektor nochmals akzentuierte. Im Ständerat erfolgten Zugeständnisse mit Blick auf die datenschutzrechtlichen Vorgaben für den privaten Sektor, namentlich die Erschwerung des Auskunftsrechts, die Ausklammerung und Abschwächung von Schutzmechanismen für spezifische Felder wie beispiels-

425 Danioth, AB 80.032, 13. März 1990, 126.
426 Vgl. Hefti, AB 80.032, 13. März 1990, 139.
427 Rhinow, AB 88.032, 13. März 1990, 130; vgl. etwas allgemeiner Pedrazzini zum staatlichen Informationsbedarf zur Erfüllung seiner Aufgaben, Wirtschaft und Recht 1982, 27 ff., 28, auch mit dem Hinweis, dass trotz des Fokus auf den öffentlichen Bereich der private Bereich nicht aus den Augen geraten dürfe.
428 Rhinow, a. a. O., 131.

weise Kreditauskunfteien, Adresshandel oder das Arbeitsverhältnis sowie die Beschneidung der Kompetenzen des ED(Ö)B.[429]

Als das Geschäft die *zweite Kammer,* den Nationalrat, im Dezember 1991 erreichte, hatte die Vorlage eine früh ein- und sich kontinuierlich fortsetzende Absenkung des Schutzniveaus für den privaten Sektor hinter sich. Längst hatte sich bestätigt, dass die Einschätzungen und Entscheidungen von Altbundesrat Furgler klug gewesen waren: Von Sacherwägungen motiviert, erfolgte eine je separate Erarbeitung eines Datenschutzkomplexes für den privaten und den öffentlichen Sektor; aus politischem Kalkül erfolgte die Zusammenlegung in einem Gesetz. Ein Gesetz, für dessen öffentlich-rechtlichen Teil die Entrüstung über die Fichenaffäre das Wort redete und das damit die notwendige Kraft hatte, die «kleine Schwester», die Normierung für den privatrechtlichen Bereich, mitzuziehen: 276

> «Wir sind immer wieder erstaunt darüber – nicht zuletzt angesichts der erhaltenen Lobbyistenpost aus Wirtschaftskreisen –, wie sehr der für uns zentrale Grundrechtsaspekt dieses Datenschutzes hinter wirtschaftlichen Interessenüberlegungen zurücktreten soll.»[430]

Auch Nationalrat Thür beklagte, dass eine immer offenkundigere Verschiebung weg von einem tragfähigen Expertenentwurf durch die herrschenden politischen Mehrheitsverhältnisse erfolgt war. Die Durchschlagskraft wirtschaftlicher Interessen habe das Gleichgewicht aus dem Lot gebracht, wie er nicht ohne Zynismus bemerkte: 277

> «Natürlich kann man darüber erleichtert und erbaut sein, dass es gelungen ist, wenigstens das Einheitsgesetz zu retten, dass also ein Auseinanderbrechen des Datenschutzgesetzes in einen öffentlich-rechtlichen Teil, der gesetzlich normiert wird, und einen privatrechtlichen, der auf den Weg des Zivilgesetzbuches verwiesen wird, verhindert werden konnte. Ich will diesen Teilerfolg, um den sich namentlich der Kommissionspräsident sehr bemüht hat, keineswegs geringschätzen. Doch welch ein Katalog von Zugeständnissen musste dafür gemacht werden? Welch hoher Preis musste bezahlt werden, um dieses Auseinanderbrechen zu verhindern?»[431]

Wie im Ständerat Rhinow wies im Nationalrat Nabholz darauf hin, dass sachlogische, genauer: verfassungsrechtliche Gründe – namentlich der Grundsatz der Privatautonomie – durchaus Anlass für die Differenzierung gäben. Entsprechend bedeute ein Entscheid für ein Gesetz, das sowohl Datenbearbeitungen durch Private als auch durch Bundesorgane erfasse, nicht zugleich, dass beide Bereiche identisch geregelt werden müssten. Ein weniger restriktives Regime für 278

429 Onken, AB 88.032, 13. März 1990, 129 f.; vgl. zur Beschneidung der Kompetenzen des EDÖB im Parlament und namentlich die Beschränkung auf eine Beratungsfunktion für den privaten Sektor Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 42.

430 Vollmer, AB 88.032, 5. Juni 1991, 943.

431 Onken, AB 88.032, 13. März 1990, 130.

den privaten Sektor sei im Interesse der Privatautonomie und zur Vermeidung einer überbordenden Datenschutzbürokratie durchaus denkbar. Allerdings wies Nabholz darauf hin, dass der Ständerat den Entwurf des Bundesrates im privatrechtlichen Teil zu stark entschlackt habe.[432] So waren die Konzessionen im Nationalrat und die Reduktion des Schutzniveaus im privaten Sektor zwar vorhanden, aber doch weniger einschneidend als im Ständerat.

279 Die parlamentarischen Beratungen dokumentieren, dass *die beiden Kammern unterschiedliche Kursrichtungen* verfolgten. Sie lassen sich in den Worten Danioths wie folgt wiedergeben:

> «[A]uf einen Nenner gebracht, kann man die Unterschiede so qualifizieren, dass der Nationalrat zu vermehrter Regelungsdichte neigte und insbesondere den Datenschutz im Privatrechtsbereich verstärkte beziehungsweise sich dem öffentlichen Normenstand in der Bundesverwaltung stark annäherte. Die Kommission des Ständerates hält daran fest, dass die unterschiedliche Interessenlage eine differenzierte Datenschutzgesetzgebung erfordert, was auch in einem Einheitsgesetz zum Ausdruck kommen muss: *Missbrauchsgesetzgebung* im Privatbereich, Verhaltensnormen im öffentlichen Bereich».[433] [Hervorhebung durch die Autorin]

280 Im Differenzbereinigungsverfahren allerdings wurden weitere Konzessionen vonseiten des Nationalrates erforderlich.[434] Bis die Differenzen – wiederum nach intensivem Ringen – bereinigt worden waren und für die Schweiz ein erstes DSG in Kraft trat, wurde das Jahr 1993 geschrieben. Kurz vor der Zielgeraden war es Bundesrat Koller, der im Differenzbereinigungsverfahren und in der zweiten Lesung im Ständerat für ein «zügiges Abschliessen» des langwierigen Prozesses plädierte und nun auch auf den Zeitdruck und die Relevanz des eidgenössischen Datenschutzgesetzes für die internationalen Beziehungen hinwies.[435]

281 *Zusammenfassend* ist für die Schweiz festzuhalten, dass es die Debatte um eine Datenschutzgesetzgebung auch für den privaten Bereich war, die den Gesetzgebungsprozess so langwierig machte. Den eigentlichen *Brennpunkt* im Rahmen der eidgenössischen Datenschutzgesetzgebung bildete entsprechend die Frage nach der Differenzierung des Datenschutzrechts für den öffentlichen und den privaten Bereich bis hin zu Standpunkten, die eine allgemeine Datenschutzgesetzgebung für den privaten Sektor verhindern wollten. Es gelang zwar, ein Gesetz für beide Bereiche zu verabschieden. Allerdings wurde das Schutzniveau für den privaten Sektor bei der Ausarbeitung des DSG *sukzessive* und in jedem Verfahrensstadium abgesenkt. Davon betroffen waren bestimmte Verarbeitungskontex-

---

432 Nabholz, AB 88.032, 5. Juni 1991, 940 f.
433 Danioth, AB 88.032, 5. Dezember 1991, 1018.
434 Vgl. Ders., AB 88.032, 13. März 1990, 228.
435 In seinen Worten anlässlich der Sitzung vom 10. März 1992: «Die Zeit drängt für dieses Datenschutzgesetz. Wir brauchen dieses Datenschutzgesetz unbedingt auch im internationalen Bereich […]. Schliesslich muss ich Ihnen sagen: Es wäre schön, wenn wir einmal ein Gesetz ohne Referendum erlassen könnten»; vgl. Koller, AB 88.032, 10. März 1992, 393.

te sowie die Betroffenenrechte. Aber auch die prozeduralen Instrumente, namentlich die Kompetenzen des EDÖB, wurden für den privaten Bereich zurückgebunden, eine Verbandklage verworfen. Ebendiese Konzessionen im privaten Bereich erfolgten unter dem Druck effizient eingebrachter *Wirtschaftsinteressen*. Im Ergebnis wurde ein *duales Datenschutzgesetz* verabschiedet, wobei die Vorgaben für den privaten Bereich an erster Stelle durch den Einfluss ökonomischer Interessenvertreter geschwächt wurden.[436]

282 Im Rahmen der Totalrevision liess sich eine ähnliche Dynamik verzeichnen: Bereits bei den Vorarbeiten wurde, wiederum von Wirtschaftsvertretern, angeführt, dass das aktuell geltende Instrumentarium genüge, um die Rechte und Pflichten der betroffenen Personen zu gewährleisten. Allerdings befinden sie sich mit dieser Ansicht heute in der Minderheit.[437] An der Differenzierung zwischen dem privaten und dem öffentlichen Bereich wurde im Zuge der Totalrevision festgehalten; indes werden mehrere neue Instrumente für beide Bereiche gleichermassen vorgesehen. Auch hinsichtlich einer Totalrevision stand die Schweiz infolge der internationalen, namentlich der europarechtlichen Entwicklungen, unter Zugzwang. Von der Basisstruktur und damit namentlich von den im Rahmen der Erarbeitung des ersten Datenschutzgesetzes getroffenen Anknüpfungspunkten wurde in der Totalrevision nicht abgegangen. Obschon die Totalrevision auch von den Entwicklungen im Europäischen Recht und hierbei insb. der DSGVO angestossen wurde, stand die Übernahme des in der DSGVO implementierten *Monismus*, der die datenschutzrechtlichen Vorgaben für behördliche wie private Verantwortliche identisch formuliert, nicht zur Debatte. Vielmehr wird am dualistischen System festgehalten, das sich durch verschiedene Elemente konstituiert.

283 Was die Darstellung des politischen Ringens um die Verabschiedung des ersten Datenschutzgesetzes sichtbar werden liess und was mit der Titulierung des DSG als Einheitsgesetz[438] in keiner Weise ausgedrückt wird, ist die *Relevanz und Brisanz, welche der Frage nach einer bereichsspezifischen Differenzierung* (oder des Verzichtes auf diese) für die Datenschutzgesetzgebung zukam – und zukommt.

284 An erster Stelle steht die Vor- und Grundsatzfrage, ob es das dualistische oder das monistische Regime ist, das datenschutzrechtlichen Anliegen effizienter zum Durchbruch zu verhelfen vermag. Offensichtlich stellen sich für ein monistisches Regelungsregime gegenüber einem dualen Regime, das für die beiden Bereiche unterschiedliche Normen vorsieht, unterschiedliche Rechtsfragen. So präsentieren sich Fragen der Anwendbarkeit sowie der Koordination und Auslegung der für die beiden Bereiche nuancierten Normen. Zudem ist die Abgrenzung der bei-

436 Jaggi, AB 88.032, 13. März 1990, 131; vgl. zur Regelung des Datenschutzes für den öffentlichen und nicht-öffentlichen Bereich auch Epiney/Hofstötter/Meier/Theuerkauf, 19 f.
437 EJPD, Bericht Begleitgruppe, 6 f.
438 Dazu exemplarisch M. w. H. Maurer-Lambrou/Kunz, BSK-DSG, Art. 1 N 6.

den Bereiche mit Blick auf Zugriffsbegehrlichkeiten des Sektors, der strengeren Vorgaben unterworfen wird, eine Herausforderung.

285 Dass die Bestimmung des einschlägigen Rechts schwierig sein kann, zeigte sich unlängst im Entscheid des Bundesverwaltungsgerichts A-3548/2018 i. S. Helsana+ vom 19. März 2019. Datenschutzrechtlich war das von der Zusatzversicherungs-AG betriebene, appbasierte Programm Helsana+ zu beurteilen. Nach diesem Programm sollten Nutzende über die App für bestimmte Aktivitäten, z. B. Sport, Pluspunkte sammeln können, wobei der Nachweis per Foto-Upload erfolgte. Später sollten die Pluspunkte in Barauszahlungen, Sachleistungen, Gutscheine von Partnerbetrieben umgewandelt werden können. Nutzungs- und Bonusberechtigt sollten Versicherungsnehmer einer Versicherungsgesellschaft der Helsana AG sein. Um die Teilnahmeberechtigung (i. e. die Eigenschaft, Versicherungsnehmerin resp. Versicherungsnehmer bei einer Helsana-Gesellschaft zu sein) sowie die Berechnung der Boni zu klären, holte die Helsana Zusatzversicherungs-AG bei den Antragstellenden die Einwilligung zu Personendatenverarbeitungsprozessen ein, um «Daten von der obligatorischen Krankenversicherung der Helsana-Gruppe zur Zusatzversicherung zu übertragen». Das Bundesverwaltungsgericht prüfte vorab, ob die Beklagte als Bundesorgan zu qualifizieren sei, da ein Zugriff auf Daten aus der obligatorischen Krankenpflegeversicherung im Rahmen des Registrierungsprozesses erfolge. Krankenkassen und private Versicherungsunternehmen, die dem BGG betreffend Aufsicht über Versicherungsunternehmen unterständen, gälten dann als Bundesorgane, wenn sie über eine Bewilligung zur Durchführung der sozialen Krankenversicherung nach Art. 4 VAG verfügen würden. Die Beklagte biete indes, so das Bundesverwaltungsgericht, unbestritten keine obligatorischen Krankenversicherungen an. Keine der Datenbearbeitungen, welche die Beklagte im Rahmen des Programms Helsana+ durchführe, beruhe auf solchen Personenangaben, die durch das Krankenversicherungsgesetz geregelt werden. Das Rechtsverhältnis zwischen den betroffenen Personen und der Beklagten sei entsprechend nicht öffentlicher Natur, die Beklagte handle nicht als Bundesorgan, womit es zur Anwendung der Bestimmungen des DSG für den privaten Bereich komme, Art. 12 ff. DSG.[439]

286 Weil die Schweiz, wie zu zeigen sein wird, einen pointierten Dualismus vorsieht, hat die Bestimmung des anwendbaren Rechts – des Normenkomplexes für den öffentlichen Bereich des Bundes resp. des Normenkomplexes für den privatrechtlichen Bereich – weitreichende Konsequenzen.

439 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 4.5.5.; zum Urteil s. auch Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f.; Vasella/Ziegler, digma 2019, 80 ff.; Pärli, SZS 2018, 107 ff. kritisch zur verordneten Selbstbestimmung; nach Totalrevision Art. 30 ff. nDSG.

3. Strukturierung des Dualismus

Nunmehr soll das dualistische Regime des DSG präziser erfasst werden. Von diesem wird auch mit der Totalrevision des DSG nicht abgegangen werden, ungeachtet der Tatsache, dass die DSGVO zu einem monistischen Modell übergegangen ist. 287

3.1. Gesetzessystematik – Überblick

Die duale Architektur des DSG wird nicht nur anhand des Schutzzweckartikels von Art. 1 DSG (das Gesetz soll die Grundrechte und die Persönlichkeit der Betroffenen schützen, vgl. Art. 1 nDSG) sowie des Anwendungsbereichs von Art. 2 DSG (Art. 2 nDSG), sondern auch anhand der Systematik des geltenden DSG deutlich. An den Anfang werden zwei Abschnitte gestellt, die für beide Bereiche gelten: Der 1. Abschnitt definiert *Zweck* sowie *Begrifflichkeiten* sowohl für den privaten als auch für den öffentlichen Bereich. Der 2. Abschnitt statuiert *allgemeine Datenbearbeitungsgrundsätze für beide Sektoren*. Anders noch hatte die Expertenkommission allgemeine Bestimmungen *je* für den privaten wie für den öffentlich-rechtlichen Datenschutz vorgesehen, was als die bessere, weil präzisere, Lösung galt.[440] Im Anschluss an den gewissermassen vor die Klammer gezogenen gemeinsamen Regelungskomplex des ersten und zweiten Abschnitts, der vereinzelte differenzierende Einzelnormen wie Art. 11a DSG beinhaltet, wird eine konsequente Zweiteilung vorgenommen: Im 3. Abschnitt folgt ein Korpus an Normen, der die Datenbearbeitung durch Private regelt. Der 4. Abschnitt sieht spezielle Regeln für die Datenbearbeitung durch öffentliche Stellen des Bundes vor. Die folgenden Abschnitte 5 ff. mit ihren Durchsetzungs- und Übergangsbestimmungen gelten dem Grundsatz nach für *beide Bereiche*. Sie enthalten gleichwohl bedeutsame Differenzierungen für den öffentlichen und den privaten Sektor. Exemplarisch ist der 5. Abschnitt, der den EDÖB für beide Bereiche als zuständige Behörde installiert. Allerdings kommen diesem unterschiedliche Kompetenzen für den jeweiligen Bereich zu. 288

Mit der *Totalrevision* finden sich die spezifischen Bestimmungen für den privaten resp. öffentlichen Bereich im 5. und 6. Kapitel. Unter dem Titel «Allgemeine Bestimmungen» steht das 2. Kapitel, dessen 1. Abschnitt sich den Begriffen und Grundsätzen, dessen 2. Abschnitt sich der Bekanntgabe von Personendaten ins Ausland, dessen 3. Abschnitt sich dem sog. postmortalen Datenschutz widmet. Dieser kennt in der DSGVO kein entsprechendes Pendant. Das 3. Kapitel regelt das Verhältnis von Verantwortlichem und Auftragsverarbeiter, das 4. Kapitel normiert die Betroffenenrechte, woraufhin das 5. und das 6. Kapitel mit den spe- 289

440 Pedrazzini, Grundlagen, 19 und 24.

zifischen Regeln für die Bearbeitung durch Private und Bundesbehörden folgen. Das 7. Kapitel befasst sich mit dem EDÖB.

290 Indem in den ersten vier Kapiteln Bestimmungen für beide Bereiche vorgesehen werden, wird der Normbestand, der für den öffentlichen wie den privaten Sektor gilt, ausgebaut. Das kommt durchaus einer Annäherung der beiden Systeme gleich. Immerhin: Es handelt sich um eine Angleichung, die in erster Linie *nicht* in der Überwindung der tradierten strukturellen und *materiellrechtlichen Differenzierung* besteht – namentlich nicht in Bezug auf den Ausgangs- sowie Anknüpfungspunkt. Im DSG gilt vor und nach Totalrevision das folgende Konzept: prinzipielles Verarbeitungsverbot und Legalitätsprinzip mit rechtlich definierten Erlaubnistatbeständen im öffentlichen Bereich, prinzipielle Verarbeitungsfreiheit mit Schranken im privaten Bereich.[441]

291 Die «Vereinheitlichung» wird mit der Totalrevision in erster Linie durch die Schaffung eines breiteren gemeinsamen Fundamentes von *prozeduralen und organisatorischen Datenschutzinstrumenten* vollzogen, die auf die faktische Verwirklichung und Implementierung des Datenschutzes abzielen (so namentlich das Verarbeitungsverzeichnis, das sowohl von privaten als auch von öffentlichen Verantwortlichen erstellt werden soll, vgl. Art. 12 nDSG). Die Totalrevision baut den Korpus an Vorgaben, die für beide Bereiche gelten, namentlich in diesem Aspekt aus.

292 Wie aber lässt sich die gesetzliche Differenzierung für den privaten und öffentlichen Bereich im geltenden DSG (und damit vor Totalrevision) strukturieren? Viele Umschreibungen finden sich, um das «zweigeteilte Einheitsgesetz» genauer zu charakterisieren, seine beiden Gesichter markanter und konkreter zu bezeichnen. Im Rahmen der Darstellung des historisch-politischen Prozesses fiel exemplarisch und trefflich eine Beschreibung des privaten Sektors als Missbrauchsgesetzgebung.[442] Später kursierten zusehends Charakterisierungen, die das Regime für den privaten Bereich als eines der *informationellen Selbstbestimmung* qualifizieren.[443] Zwar wurde seit 1993 erst die Bundesverfassung totalrevidiert, was auch

441 Hierzu bereits Forstmoser, digma 2003, 50 ff., 53; zum Legalitätsprinzip im Allgemeinen, aber auch spezifisch in Bezug auf die Verarbeitung von Personendaten Glass, 5 ff. und 91 ff.

442 Danioth, AB 88.302, 5. Dezember 1991, 1018; Belser, in: Epiney/Fasnacht/Blaser (Hrsg.), 19 ff., 34 ff.

443 Ob das DSG ein Recht auf informationelle Selbstbestimmung insb. auch für den privaten Bereich verbürgt resp. was die Elemente eines solchen Rechts sind, wird im Zuge dieser Arbeit vertieft analysiert; vgl. insb. zweiter Teil, VI. Kapitel sowie dritter Teil; die Auffassung, wonach das DSG ein Recht auf informationelle Selbstbestimmung verbürge, vertritt mit einem Fokus auf den privaten Bereich z. B. Aebi-Müller, N 267 und m. w. H. N 529; Dies., in: Girsberger/Schmid (Hrsg.), 13 ff., 20; Rosenthal, HK-DSG, Art. 4 N 66; Maurer-Lambrou/Kunz, BSK-DSG, Art. 1 N 5; Flückiger, PJA 2013, 837 ff.; aufschlussreich auch für die Schweiz die Ausführungen zur informationellen Selbstbestimmung mit der Einwilligungskonstruktion als zentrales Element Cavoukian, digma 2009, 20 ff.; hinterfragend dagegen zur Figur im Schweizer Rechtskorpus m. E. in zutreffender Weise, wenn auch mit einem Fokus auf den Grundrechtsschutz, Belser, in: Epiney/Fasnacht/Blaser (Hrsg.),

die Einführung eines neuen Art. 13 BV mit sich brachte. Zudem wurde das DSG seit seinem Inkrafttreten teilrevidiert.[444] Allerdings haben weder die bislang erfolgten Teilrevisionen noch die derzeit hängige Totalrevision einen Systemwechsel gebracht. Die Bedeutung der bis heute zugleich dezidiert wie nuanciert bereichsspezifischen Normierung, die das DSG für den öffentlichen gegenüber dem privaten Bereich vorsieht, wurde bislang nicht grundlegend thematisiert. Vielmehr wird man anhand zahlreicher Textstellen in eine andere Interpretationsrichtung verwiesen:

> «Das Datenschutzgesetz enthält *als gemeinsames Fundament* jeglicher Datenbearbeitung nebst den wichtigsten Begriffsumschreibungen die eigentlichen materiellen Grundsätze, ich möchte sie Spielregeln jeder Datenbearbeitung nennen […].»[445] [Hervorhebung durch die Autorin]

Die gemeinsamen Bestimmungen mit ihren generalklauselartigen, sehr allgemeinen Grundsätzen für die private wie die öffentliche Datenbearbeitung[446] wurden ebenso als das «ethische und rechtspolitische Fundament des Datenschutzgesetzes[447]» beschrieben. Allerdings verleitet die Referenz auf ein gemeinsames Fundament zu einer Fehlinterpretation in Bezug auf das Schutzniveau des Datenschutzgesetzes für den privaten gegenüber dem öffentlichen Bereich. Sie lässt die Assoziation mit einem *gemeinsamen und identischen Ausgangspunkt* entstehen. Doch das prägende Charakteristikum des DSG ist, wie bisher ansatzweise dargetan, dessen *Dualismus* mit *entgegengesetzten Ausgangspunkten* für den privaten und öffentlichen Bereich. Ebendies hat vorab bereits Rhinow mit folgenden Worten festgehalten: 293

> «Das Gesetz […] regelt zu Recht sowohl die Datenbearbeitung durch den Bund als auch durch private Personen. Trifft aber – ebenfalls zu Recht – unterschiedliche, differenzierte Normierungen, indem es bei den Bundesorganen das Legalitätsprinzip in den Vordergrund rückt, während es im privatrechtlichen Verhältnis die Mechanik des Persönlichkeitsschutzes von Art. 28 ZGB übernimmt.»[448]

---

19 ff.; auf Missverständlichkeiten hinweisend Meier, N 15 ff.; kritisch sodann Gächter/Egli, Jusletter vom 6. September 2010, N 19 ff.; Glass, 151 ff.; zutreffend mit dem Hinweis, dass ein Konzept der informationellen Selbstbestimmung bislang nicht ins Gesetz eingegangen ist, Ziegler/Vasella, digma 2019, 158.

444 Vgl. zur Teilrevision Wermelinger/Schweri, Jusletter vom 3. März 2008; zur Kritik an einer ersten Revision, wonach diese die Wirtschaft in ein zu enges Korsett schnüren würde, wobei die Autoren vertreten, dass ein starker Datenschutz auch der Wirtschaft diene, Baeriswyl/Rudin, Jusletter vom 28. Juni 2004; kritisch zur Revision, wie sie 2008 in Kraft trat, Brunner, in: Schaffhauser/Horschik (Hrsg.), 142 ff. und Ders., Jusletter vom 4. April 2011; Cottier, Jusletter vom 17. Dezember 2007, der die wichtigsten Neuerungen wie die Schärfung der Transparenzvorgaben darstellt und dafür plädiert, die Neuerungen nicht zu unterschätzen; Drechsler, AJP 2007, 1471 ff.; zur Teilrevision weiter Schmid, in: Schmid/Girsberger (Hrsg.), 151 ff., 156 ff.

445 So Danioth, AB 88.032, 13. März 1990, 127.

446 Zu einer Darstellung der Grundsätze auch Schmid, ZBJV 1995, 809 ff., 820; Peter, 125 ff.

447 BBl 1988 II 414 ff., 459.

448 Rhinow, AB 88.032, 13. März 1990, 130.

294 Ebenso prägnant Forstmoser:

> «Im Rahmen des Privatrechts gilt: erlaubt ist, was nicht verboten ist, das ist der Ausgangspunkt im privaten Bereich, während im öffentlichen Recht gilt: Verboten ist, was nicht erlaubt ist […].»[449]

295 Diese akkurate Qualifizierung wurde in der späteren Rezeption und Interpretation des DSG allzu oft übersehen. Nachfolgend werden die Elemente vertieft, die zur Beschreibung des DSG als *duales Gesetz* Anlass geben.[450] Am Anfang steht der richtungsweisende Entscheid für *entgegengesetzte Ausgangspunkte für den privaten und den öffentlichen Bereich*. Darin allerdings erschöpft sich die *bereichsspezifisch differenzierende Regelung* nicht. Vielmehr setzt das DSG besagte Grundsatzentscheidung mit «gegenüberliegendem Startpunkt» durch weitere Gestaltungselemente konsequent fort.

3.2. Entgegengesetzte Ausgangspunkte für die beiden Bereiche

3.2.1. Darstellung

296 In der Schweiz zeigt sich folglich die datenschutzgesetzliche Situation dergestalt, dass die quasi als allgemeiner Teil vorangestellten Prinzipien in ein *ganz unterschiedliches, ja gegenläufiges Konzept* für den privaten und den öffentlichen Sektor eingebettet sind. Für den privaten und den öffentlichen Sektor gelten entgegengesetzte Ausgangspunkte: grundsätzliches Verarbeitungsverbot mit Erlaubnisvorbehalten qua gesetzlicher Grundlagen für den öffentlichen Sektor, grundsätzliche Verarbeitungsfreiheit mit Schranken für den privaten Sektor. Es ist Art. 1 DSG, der Zweckartikel, der bei einer streng der privatrechtlichen und öffentlichrechtlichen Terminologie wie Dogmatik verpflichteten Lesart die verschiedenen Mechaniken resp. unterschiedlichen Regelungskonzepte über das Schutzobjekt in das DSG einführt.

297 Entsprechend drängt es sich für den *öffentlichen Bereich* auf, an die Theorie der Grundrechte und ihrer Beschränkungen anzuknüpfen, womit auch das *Legalitätsprinzip* für das Datenschutzrecht installiert wird, vgl. Art. 17 DSG und Art. 34 nDSG. Für den öffentlichen Bereich des Bundes gilt das grundsätzliche Verarbeitungsverbot, jeder Umgang mit Personendaten – das Erheben, Speichern, Auswerten usf. – braucht eine spezifische Legitimation, wobei eine gesetzliche

449 Forstmoser, digma 2003, 50 ff., 53, spricht davon, dass das Gesetz nicht verleugnen könne, ein Fusionsprodukt zu sein, dessen Anwendungsbereich von verschiedener Tiefe sei; die Botschaft spricht von einer «eingehenden Regelung» für den öffentlich-rechtlichen Bereich des Bundes, vgl. BBl 1988 II 414 ff., 414.

450 Zu dieser Terminologie Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.8.; als föderalistische Ordnung umschrieben von Schweizer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 1 N 13.

Grundlage den wichtigsten der Erlaubnistatbestände liefert. Entsprechend ist aus der Perspektive des Datenschutzes der Verarbeitungsraum im öffentlichen Bereich kein freiheitlicher. Vielmehr bedarf *jede* Personendatenbearbeitung durch *Bundesbehörden*, um rechtmässig zu sein, *einer spezifischen rechtlichen Grundlage ausserhalb des DSG*. Das DSG selbst liefert eine solche allgemeine Rechtsgrundlage für die Datenbearbeitung durch Bundesbehörden gerade nicht.[451] Der Inhalt datenschutzrechtlicher Regulierungen lässt sich folglich für den öffentlichen Sektor auf Bundesebene nie isoliert anhand des DSG erschliessen. Zu beachten ist vielmehr eine ganze Reihe bereichsspezifischer Erlasse, die sich vorrangig spezifischen hoheitlichen Aufgaben des Bundes in der Verwaltung (vgl. z. B. AsylG, ANAG, BGÖ, IVG, UVG usf.) sowie der Strafverfolgung und Verbrechensbekämpfung widmen und in diesem Kontext Personendatenverarbeitungen normieren.[452] Sodann datenschutzrechtlich von besonderer Relevanz und Brisanz ist der steuerrechtliche Bereich, wobei das Bundesgesetz über die direkte Bundessteuer datenschutzrechtliche Regeln vorsieht, vgl. Art. 112a DBG.[453]

Die genannten *bereichsspezifischen Spezialgesetze* weisen entsprechend eine doppelte Funktion auf: Sie bilden zunächst die Legitimationsgrundlage zur Durchbrechung des nach DSG implementierten Grundsatzes des Verarbeitungsverbotes und erfüllen damit das verfassungsrechtliche Legalitätsprinzip für den öffentlichen Bereich, vgl. Art. 17 DSG und Art. 36 Abs. 1 sowie Art. 5 Abs. 1 BV. Sodann finden sich in den Spezialgesetzgebungen differenzierende, ergänzende und derogierende Datenschutzbestimmungen. Hieraus wird deutlich, dass der *öffentliche Bereich* aus datenschutzrechtlicher Perspektive *kein einheitlicher, monolithischer ist*. Vielmehr handelt es sich um einen facettenreichen Bereich, dessen Teilbereich jeweils unterschiedliche Ziele verfolgen. Über die jeweiligen Spezialgesetze werden jeweils verschiedene Verarbeitungszusammenhänge in die datenschutzrechtlichen Erwägungen integriert. Folglich kann bereits an dieser Stelle festgestellt werden, dass sich die Relevanz systemspezifischer Erwägungen selbst in einem Regime mit datenschutzrechtlichem Querschnittsgesetz keineswegs auf eine Zweiteilung in einen öffentlichen und privaten Bereich beschränkt. Vielmehr 298

451 Der Mechanismus ist ähnlich zu demjenigen von Art. 3 ZGB für das Privatrecht: Die Bestimmung selbst sieht keinen allgemeinen Gutglaubensschutz vor; vielmehr muss dieser in jeweiligen spezifischen Gesetzesnormen wie z. B. Art. 930 ZGB speziell verbürgt werden. Art. 3 ZGB knüpft an solche Sondernormen an («Wo das Gesetz […]») und formuliert allgemeine Modalitäten namentlich aus der Beweisperspektive.

452 Illustrativ mit Bezug auf den Datenschutz bei intelligenten Mess- und Steuersystemen und Netzbetreibern die Beschreibung des anwendbaren Rechts als dreistufiger Rechtsrahmen von DSG, kantonalem Datenschutzrecht und Spezialgesetzgebung wie das Stromversorgungsgesetz vgl. Rechsteiner/Steiner, Jusletter vom 11. Juni 2018, N 8 ff.

453 Für eine Übersicht: Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 62 ff., insb. N 65 ff.; weitere einschlägige Spezialgesetze finden sich beispielsweise für den biomedizinischen Kontext, dessen Erlasse ebenso datenschutzrechtliche Bestimmungen aufweisen: Zu nennen ist namentlich das Humanforschungsgesetz, Art. 2 Abs. 2 lit. c *e contrario*, Art. 3 lit. f. und Art. 32 f. HFG (vgl. auch Art. 119 BV) sowie das GUMG.

wird der öffentliche Bereich aufgrund *pluraler Verarbeitungszusammenhänge weiter ausdifferenziert.*

299 Damit präsentiert sich auch die Bezeichnung des Datenschutzgesetzes als Querschnittsgesetz in einem anderen Licht: Personendatenverarbeitungen durch Bundesbehörden werden über das Gebot der gesetzlichen Grundlage bereichsspezifisch rückgekoppelt. Man könnte hierfür den *Terminus der Akzessorietät des Datenschutzes* für die jeweiligen Bereiche und Verarbeitungskontexte verwenden. Insofern zeigt sich das Datenschutzrecht gerade nicht als unabhängiges Rechtsgebiet, wie man aus der isolierten Betrachtung des Datenschutzgesetzes als Querschnittsgesetz zu schliessen geneigt ist. Vielmehr weist es *systemrelative Bezüge* auf.

300 Für den öffentlichen Sektor liefert unbestrittenermassen die *gesetzliche Spezialermächtigung* den wichtigsten Erlaubnistatbestand zur Durchbrechung des grundsätzlichen Verarbeitungsverbotes.[454] Zwar sieht das DSG die Einwilligung als Erlaubnistatbestand namentlich in den Art. 17 Abs. 2 lit. c sowie Art. 19 Abs. 1 lit. b DSG vor (vgl. Art. 34 Abs. 4 lit. b, Art. 36 Abs. 2 lit. c nDSG). Dennoch kann der Einwilligung – systemkongruent – im Bereich der Datenverarbeitung durch öffentliche Stellen nur eine zurückhaltende Rolle zukommen: Die Verletzung des Legalitätsprinzips als Verarbeitungsprinzip soll nur beschränkt möglich sein.[455] Die datenschutzrechtliche Einwilligung kann ihr «Hauptanwendungsfeld» folglich nicht im öffentlichen Sektor finden, stattdessen ist sie, zumindest theoretisch betrachtet, im privaten Bereich zu verorten.[456] Entsprechend setzt das schweizerische Datenschutzgesetz für die Datenverarbeitung im öffentlichen Sektor durch Bundesorgane zumindest formell durch den Grundsatz des Verarbeitungsverbotes mit Erlaubnistatbestand und der bloss restriktiven Zulassung eines Rechtfertigungsgrundes auch bei Missachtung des Legalitätsprinzips – zumindest theoretisch oder ideal gedacht – ein *hohes Datenschutzniveau* fest. Dass diese Idee allerdings teilweise naiv bleibt, wird sich im Zuge dieser Schrift zeigen: Denn auch gesetzliche Grundlagen und Rechtssätze, die ihrerseits als Legitimation zur Bearbeitung von Personendaten dienen sollen, sollten durchaus kritisch betrachtet werden. Ebendies wird vertiefend im letzten Teil und letzten Kapitel

454 Zum Legalitätsprinzip mit seinem allgemeinen rechtsstaatlichen Rahmen sowie spezifisch im Kontext des Datenschutzrechts vgl. insb. Glass, 5 ff., auch mit Hinweis auf die Neuerungen im Zusammenhang mit den Kategorien von «Gesetz im formellen und materiellen Sinne».

455 Rosenthal, HK-DSG, Art. 4 N 4.

456 Fasnacht, N 191 ff. und N 215 ff.; Rogosch, 34; grundlegend zur datenschutzrechtlichen Einwilligung, allerdings teilweise ohne Vertiefung der Frage der Differenzierung für die beiden Bereiche Radlanski, *passim*; Liedke, *passim;* Schunke, *passim* sowie die Beiträge von Rosenthal, Vasella und Bühlmann.

dieser Schrift ausgearbeitet werden anhand der geheimen Observation im Versicherungskontext.[457]

Zur gesetzlichen Grundlage wurde in der Botschaft von 1988 vertreten, dass keine rechtliche Spezialermächtigung, die sich spezifisch auf die Datenbearbeitung beziehen müsse, erforderlich sei. Vielmehr sei die Bearbeitung von Daten zulässig, wenn sie für die Erfüllung einer gesetzlichen Aufgabe erforderlich ist.[458] Eine solche Interpretation, die nicht zu überzeugen vermag, führt zu einer einschneidenden *Absenkung* des Datenschutzniveaus für den öffentlichen Bereich. Sieht das DSG als Ausgangspunkt für die Datenverarbeitung durch Bundesbehörden den *Grundsatz des Verarbeitungsverbotes mit Ausnahmetatbeständen* vor,[459] so deckt es sich insofern – in diesem Bereich – mit dem Regime der DSGVO, vgl. Art. 6 DSGVO. Allerdings gelten die Anforderungen an die Klarheit, Spezifizierung und Präzision ebenda als hoch.[460] 301

Wie aber präsentieren sich der im DSG implementierte Ansatz und das Schutzniveau für den *privaten Bereich*? Die im Rahmen der Gesetzgebungsarbeiten zur erstmaligen Verabschiedung des DSG gemachte Aussage, wonach das Datenschutzgesetz für den privatrechtlichen Sektor den Schutz der Persönlichkeit gemäss Art. 28 ZGB spezialgesetzlich gewährleisten solle, bedarf der Präzisierung. Die Worte in der Botschaft von 1988 zum Datenschutzgesetz von 1992 geben das später gesetzlich verabschiedete Regime prägnant wieder: 302

> «Gleichsam als Spiegelbild zum zivilrechtlichen Persönlichkeitsschutz besteht auch ein gewisser verfassungsrechtlicher Schutz gegen unzulässige und übermässige Datenbearbeitung.»[461]

Anders als im öffentlichen Bereich ist nicht jede Personendatenverarbeitung grundsätzlich verboten. Vielmehr implementiert Art. 12 ff. insb. i. V. m. Art. 4 DSG resp. Art. 30 ff. i. V. m. Art. 6 nDSG ein *System mit grundsätzlicher Freiheit der Datenbearbeitung, deren Schranken sich auf ein Prinzip der «Fairness»* beziehen.[462] Insofern aufschlussreich ist nochmals eine Passage aus der Botschaft von 1988, wonach die *Lauterkeit in der privaten Wirtschaftstätigkeit* auch im Umgang mit Personendaten gelte.[463] Die «Lauterkeit» wird in erster Linie durch die 303

457 Dritter Teil, IX. Kapitel; eindrücklich zur Problematik im Zusammenhang mit der verordneten Zwangsmedikation Bucher, ZBJV 2001, 764 ff.; seit jeher wird denn auch in der Schweiz die auf Bundesebene fehlende Überprüfung von Bundesgesetzen auf ihre Verfassungsmässigkeit hin diskutiert.

458 Vgl. auch BBl 1988 II 414 ff., 467; Ballenegger, BSK-DSG, Art. 17 N 18.

459 Vgl. Ballenegger, BSK-DSG, Art. 17 N 3.

460 Insb. bedarf es der spezifischen Zweckbestimmung mit Blick auf die Personendatenverarbeitung und die Gewährleistung der Vorhersehbarkeit der Verarbeitung, vgl. Buchner/Petri, Beck-Komm.-DSGVO, Art. 6 N 91.

461 BBl 1988 II 414 ff., 414; zum verfassungsmässigen Schutz und verfassungsmässigen Recht auf Privatsphäre im Zeitraum der Verabschiedung des ersten DSG Schrepfer, 19 ff.

462 Vertiefend hierzu zweiter Teil, VI. Kapitel, B.

463 BBl 1988 II 414 ff., 425.

allgemeinen Verarbeitungsgrundsätze gem. Art. 4 DSG resp. Art. 6 nDSG definiert. Erst der *qualifizierte Umgang mit Personendaten* – allem voran der Verstoss gegen die allgemeinen Verarbeitungsgrundsätze – begründet zugleich eine Persönlichkeitsverletzung, vgl. Art. 12 DSG resp. Art. 30 nDSG.[464]

304 Nach DSG liegen die *Schranken der grundsätzlichen Freiheit der Bearbeitung* vorab in den *allgemeinen Bearbeitungsgrundsätzen*, der Gewährleistung der Vorgaben an die *Datenrichtigkeit* sowie der Einhaltung der Datensicherheitsvorgaben, Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG.[465] Ein Verstoss gegen diese durch die Fixierung von Grundprinzipien gesetzten Schranken begründet eine Persönlichkeitsverletzung, die prinzipiell auch widerrechtlich ist, es sei denn, es liegt ein Rechtfertigungsgrund vor nach Art. 13 DSG resp. Art. 31 nDSG.[466]

305 Eine weitere Schranke der prinzipiellen Verarbeitungsfreiheit liegt in einer Widerspruchskonstellation: Die Verarbeitung von Personendaten entgegen dem ausdrücklichen Willen wird als qualifizierte Handlung taxiert, die – mangels Rechtfertigungsgrund – eine widerrechtliche Persönlichkeitsverletzung begründet, vgl. Art. 12 Abs. 2 lit. b i. V. m. Art. 13 DSG resp. Art. 30 Abs. 2 lit. b nDSG. In konsequenter Anlehnung des DSG für den privaten Bereich an Art. 28 ff. ZGB kann auch eine Verarbeitung gegen den ausdrücklichen Willen der Betroffenen zulässig sein, sofern hierfür ein Rechtfertigungsgrund angeführt werden kann gemäss Art. 13 DSG resp. Art. 31 nDSG.

306 Weiter begründet die *Bekanntgabe von besonders schützenswerten Daten oder von Persönlichkeitsprofilen an Dritte* eine widerrechtliche Persönlichkeitsverletzung, vgl. Art. 12 Abs. 2 lit. c i. V. m. Art. 3 lit. c, lit. d, lit. f. DSG. Auch hier besteht die Rechtfertigungsmöglichkeit gemäss Art. 13 DSG. Mit der Totalrevision wird das Konzept des Persönlichkeitsprofils aufgegeben. Neu geregelt werden stattdessen das Profiling sowie die automatisierte Einzelfallentscheidung, vgl. Art. 5 lit. f und lit. g nDSG und Art. 6 Abs. 7 nDSG und z. B. Art. 21, Art. 25 Abs. 2 lit. f. nDSG. Als Tatbestand der Persönlichkeitsverletzung gilt gemäss Art. 30 Abs. 2 lit. c nDSG einzig die Bekanntgabe besonders schützenswerter Personendaten an Dritte, vgl. zur Konkretisierung Art. 5 lit. c und lit. e nDSG. Eine Rechtfertigung ist nach Art. 31 nDSG möglich.

---

464 Vertiefend hierzu zweiter Teil, VI. Kapitel, A. und B.

465 Während der Grundsatz der Datenrichtigkeit noch in Art. 5 DSG eigenständig geregelt ist, wird er mit der Totalrevision in die allgemeinen Grundsätze gemäss Art. 6 nDSG, genauer in dessen Abs. 5 integriert. Separat finden sich in beiden Versionen die Vorgaben zur Datensicherheit, Art. 7 DSG resp. Art. 8 nDSG.

466 Zur Kontroverse mit Blick auf die unterschiedlichen Formulierungen betreffend die Rechtfertigungsgründe in den verschiedenen literae Rosenthal, HK-DSG, Art. 12 N 15 ff.; Auslegungshilfe des BJ vom 10. Oktober 2006, Ziff. 3.1.

Der Abriss hat gezeigt, wie eng das datenschutzgesetzliche System für den privaten Bereich an der Struktur von Art. 28 ZGB angelehnt ist. Es sind stets erst *qualifizierte Handlungen*, die als (persönlichkeits-)rechtlich relevant eingestuft werden.[467] Gleichzeitig wird damit ein *individualrechtlich sowie defensivrechtlich* gedachtes Regime im DSG implementiert. Die Totalrevision bringt, wie angedeutet und an späterer Stelle zu vertiefen, immerhin neue Akzente mit der Einführung eines Risiko- und Compliance-Ansatzes, die indes die persönlichkeitsrechtliche Anknüpfung nicht ersetzen, sondern ergänzen. 307

Damit ist erstellt, dass eine Behauptung, wonach das *DSG im privaten Bereich den Betroffenen ein Recht auf informationelle Selbstbestimmung in der Gestalt eines Herrschaftsrechts* einräume, aufgrund des gewählten Ausgangspunktes der grundsätzlichen Bearbeitungsfreiheit mit Schranken für den privaten Bereich im DSG *offensichtlich keine Grundlage* findet.[468] Das für den privaten Bereich gewählte Konzept, das an qualifizierte Verarbeitungshandlungen ansetzt, räumt dem Individuum kein «Herrschaftsrecht resp. Selbstbestimmungsrecht» an seinen Personendaten ein – auch nicht mit der Totalrevision.[469] Trefflicher dagegen ist die Charakterisierung des DSG für den privaten Bereich – namentlich vor der Totalrevision – als *Missbrauchsgesetzgebung*.[470] Diese Konzeptionierung wird anhand der Gestaltung des Massnahmenkatalogs, wie er dem EDÖB eingeräumt wird und wie gezeigt werden wird, bestätigt. Immerhin stärkt die Totalrevision seine Kompetenzen auch für den privaten Bereich. 308

Eine Folge der *persönlichkeitsrechtlichen Anknüpfung des Datenschutzgesetzes für den privaten Bereich* ist weiter, dass die Rechtsdurchsetzung resp. der Rechtsschutz – zumindest nach noch in Kraft stehendem DSG – weitgehend auf die Schultern der Datensubjekte gelegt wird.[471] Es obliegt in erster Linie den Datensubjekten, die Einhaltung des Datenschutzes sicherzustellen, sei es durch Ausübung der Betroffenenrechte, sei es weiter durch die Erhebung einer zivilgerichtlichen Klage gegen qualifizierte Personendatenverarbeitungen, was allerdings kaum je geschieht.[472] Die Totalrevision bringt insofern nicht nur über die 309

467 M. w. H. Haas, N 63 ff., N 70 ff. und N 80 ff.; vgl. unter Rückgriff auf das allgemeine Zivilrecht und damit das Persönlichkeitsrecht des ZGB in Bezug auf die Presseberichterstattung Lüthy, 59 ff.

468 Die Gewährleistung eines entsprechenden Rechts im DSG vertritt insb. Aebi-Müller, N 546 ff. und N 591 ff.; kritisch insofern zutreffend Gächter/Egli, Jusletter vom 6. September 2010, N 36; Belser, in: Epiney/Fasnacht/Blaser, 19 ff., 32 ff.; vgl. insofern die Botschaft von 1988, wo potentielle Risiken für den Menschen angedeutet werden, und: «er hat die Herrschaft über die Daten, die ihn angehen, weitgehend verloren»; BBl 1988 II 414 ff., 417.

469 Vertiefend hierzu zweiter Teil, V. Kapitel und VI. Kapitel.

470 Anders Aebi-Müller, N 546 ff. und N 591 ff.; zur Qualifikation auch Gächter/Egli, Jusletter vom 6. September 2010, N 36; Belser, in: Epiney/Fasnacht/Blaser, 19 ff., 32 ff.

471 Art. 12 ff. DSG und Art. 30 ff. nDSG; vertiefend zweiter Teil, VI. Kapitel sowie dritter Teil, VII. Kapitel, A.

472 Bolliger/Féraud/Epiney/Hänni, 4; sinngemäss Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.20 f.; vgl. auch Rudin, digma 2003, 4 f., wonach das Risiko für Unternehmen weniger in behördlichen resp. gerichtlichen Verurteilungen liegt als vielmehr in den Reaktionen der mün-

neuen Instrumente wie das Verarbeitungsverzeichnis oder die Datenschutz-Folgenabschätzung, sondern auch den Ausbau sowie die Verschärfung der rechtlichen Konsequenzen von DSG-Verletzungen eine gewisse Veränderung. Ob damit Datenschutzverstösse künftig effizienter sanktioniert werden wird sich weisen müssen.

310 Das Schweizer DSG definiert den *privaten Bereich* damit als *weitgehend resp. prinzipiell freien Bereich*. Es unterscheidet sich folglich grundlegend von einem Ansatz, wie ihn Art. 6 DSGVO auch für den privaten Bereich wählt: Die DSGVO sieht mit Blick auf den gewählten Ausgangspunkt für Personendatenverarbeitungen durch Behörden und Private keine Differenzierung vor (datenschutzrechtlicher Monismus) – ebenso gilt für den privaten Bereich das Prinzip der Spezialermächtigung, Art. 6 DSGVO.[473]

311 Mit beschriebenem *Dualismus adressiert und anerkennt die Schweiz die Einschlägigkeit*, datenschutzrechtlich *bereichsdifferenzierend zu normieren*. Insofern aufschlussreich ist nochmals die Botschaft, die auf die Bedeutung sowie Chancen der Datenverarbeitungen für Forschung, Wirtschaft und Verwaltung hinweist.[474] Die Ausdifferenzierung wird zudem zum einen im öffentlich-rechtlichen Bereich des Bundes qua Legalitätsprinzip mit der gesetzlichen Spezialregelung weiter ausgebaut. Zum anderen sind im privaten Bereich mehrere Spezialgesetze mit spezifischen Datenschutzbestimmungen zu beachten, so beispielsweise das Humanforschungsgesetz mit Art. 32 f. HFG.[475]

312 Eine *Schlussfolgerung*, wonach das *Datenschutzrecht die Integrität verschiedener Systeme resp. Bereiche* schützen soll, wurde in der Schweiz – soweit ersichtlich – bislang nicht gezogen. Immerhin wurde jüngst spezifisch im Zusammenhang mit dem Bankgeheimnis resp. den beruflichen Geheimhaltungspflichten und Cloud-Services zur Diskussion gestellt, ob der Datenschutz nicht nur Subjekte, sondern auch Systeme schütze.[476] In Frage gestellt wurden die Tauglichkeit eines Rechts

digen Konsumentinnen und Konsumenten; kritisch zur Gleichsetzung von öffentlicher und privater Datenverarbeitung gemäss BDSG und für eine Differenzierung plädierend Giesen, JZ 2007, 918 ff., 923.

473 Vgl. zu dieser Vereinheitlichung qua DSGVO von Lewinski, DuD 2012, 564 ff., 565, wobei der Autor weiter die Unitarisierung des Datenschutzrechts mit Blick auf den räumlichen Anwendungsbereich und die Vereinheitlichung der Datenschutzvorgaben bei Personendatenverarbeitungen mit EU-Bezug erwähnt, 569; entsprechend könnte nunmehr mit Blick auf die DSGVO von einem doppelten Unitarismus gesprochen werden.

474 BBl 1988 II 414 ff., 417; vgl. damit die Parallele zu Deutschland, wonach Datenschutz und Forschung seit Anbeginn der datenschutzrechtlichen Debatten relevant ist, Gerling, DuD 2008, 733 ff., 733.

475 Zu diesem vertiefend zweiter Teil, VI. Kapitel, B. 6.3.

476 Walder Wyss AG (Isler/Kunz/Müller/Schneider/Vasella), N 14 ff.

auf informationelle Selbstbestimmung und damit auch der datenschutzrechtliche Subjektschutz.[477]

313 Ungeachtet der exakten Ausgestaltung des datenschutzrechtlichen Subjektschutzes bleibt festzuhalten: Die Einschlägigkeit systemischer Schutzerwägungen als datenschutzrechtliches Koordinatensystem ist namentlich im Dualismus des DSG für den privaten gegenüber dem öffentlichen Bereich anerkannt. Dem Subjektschutz bleibt das DSG auch nach Totalrevision verpflichtet, Art. 1 DSG resp. Art. 1 nDSG.[478] Mit der Totalrevision erfolgen zwar Anpassungen oder Ergänzungen der Perspektiven. Gleichwohl wird das DSG nicht von einer Fokussierung auf das einzelne Subjekt und den Individualrechtsschutz abgehen. Exemplarisch für die *Einführung neuer, ergänzender Komponenten* die Botschaft zum Entwurf zur Totalrevision des DSG:

> «Eine erste Leitlinie der Revision bildet der risikobasierte Ansatz. Der Revisionsentwurf orientiert sich konsequent an den potenziellen Risiken für die betroffenen Personen, denn die Gefahren für die Privatsphäre der betroffenen Personen hängen weitgehend von den Aktivitäten der verschiedenen Verantwortlichen und Auftragsbearbeiter ab.»[479]

3.2.2. Resümee und Einbettung

314 An dieser Stelle seien die vorangehenden Ausführungen wie folgt *zusammengefasst:* Das eidgenössische Datenschutzgesetz ist entgegen seiner formellen Erscheinung und Titulierung als *Einheitsgesetz* gerade auch aus materiellrechtlicher Sicht als *duales Gesetz* zu qualifizieren.[480]

315 Von zentraler Bedeutung ist der Entscheid für jeweils *entgegengesetzte Ausgangspunkte*. Indem der Grundsatz der Freiheit der Datenbearbeitung mit Schranken für den privaten Sektor versus den Grundsatz des Verbotes der Datenbearbeitung mit Erlaubnisvorbehalt für den öffentlichen Sektor umgesetzt wird, geht das DSG in pointierter Weise von einer *bereichsspezifischen Differenzierung* im Datenschutzgesetz resp. -recht aus.[481] Dieser Dualismus, welcher das datenschutzrechtliche Regime für den privaten und den öffentlichen Bereich des Bundes differenziert, ist ein *primäres Charakteristikum des Schweizer Datenschutzgesetzes*.

---

477 So Passadelis mit den Worten «Am überkommenen Primat der informationellen Selbstbestimmung festzuhalten, bedeutet, noch mehr kostbare Zeit zu verlieren», Gastkommentar, NZZ vom 17. Mai 2017, abrufbar unter: <https://www.nzz.ch/meinung/datenschutzrecht-komplexe-regulierung-ld.1293903?reduced=true> (zuletzt besucht am 30. April 2021).

478 Die Totalrevision hält an der entsprechenden Bestimmung mit Art. 1 nDSG fest.

479 Botschaft DSG 2017–1084, 17.059, 6941 ff., 6970.

480 Vgl. Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.10.

481 Zur weiteren Ausdifferenzierungsmöglichkeit, indem die jeweiligen Ausnahmetatbestände weit definiert werden, vgl. Buchner, 81; so liesse sich eine Abschwächung des «pointierten» Dualismus zu einem leichten Dualismus vollziehen, indem Erlaubnistatbestände beim Verbotsgrundsatz gleichermassen wie die Verbote beim Erlaubnistatbestand weit gefasst würden.

316 Das Regelungsregime für die Personendatenverarbeitung durch öffentliche Stellen des Bundes setzt insb. auch das Legalitätsprinzip um, in Entsprechung der grund- resp. verfassungsrechtlichen Konzeptionierung, vgl. Art. 36, insb. Abs. 1 BV. Das Regelungsregime bezüglich Personendatenverarbeitungen durch Private und den privaten Bereich setzt an der qualifizierten Personendatenverarbeitung an. Erst sie ist es, die zu einer Persönlichkeitsverletzung führt: Die Struktur von Art. 28 ff. ZGB wird in das Datenschutzgesetz importiert. Entsprechend knüpft das DSG am *Subjektschutz* an.

317 Mit ebendieser *dualistischen Ausgestaltung qua entgegengesetztem Ausgangspunkt* ist im DSG die Relevanz *systemischer Schutzerwägungen* in markanter Weise angelegt. Sie finden weiterführende Anerkennung, indem für den öffentlichen Bereich die jeweiligen Spezialerlasse die rechtliche Grundlage zwecks Erfüllung des Legalitätsprinzips liefern. Aber auch im privaten Bereich existieren für spezifische Kontexte, z. B. im Bankenrecht, im Humanforschungsgesetz oder im Arbeitsrecht, bereichsspezifisch motivierte datenschutzrechtliche Sondernormen.

318 Die vorangehenden Ausführungen haben weiter gezeigt, dass im Rahmen der erstmaligen Verabschiedung des DSG der Datenschutz hauptsächlich als Gegenspieler von ökonomischen Interessen wahrgenommen wurde. Der Blick auf den Gesetzgebungsprozess des DSG zeigte, wie sehr ökonomische Rationalitäten die Datenschutzgesetzgebung für den privaten Bereich beeinflussten. Der Widerstand von Wirtschaftsvertretern gab dazu Anlass, zwei verschiedene Bereiche in einem Gesetz zur Verabschiedung zu bringen.

319 Die systemische Schutzdimension des Datenschutzes wurde in der Schweiz bei Lichte betrachtet bislang nur beschränkt bewusst und sachbezogen verhandelt, obschon die bereichsspezifische Differenzierung eigentlicher Brennpunkt im Zuge der Verabschiedung des ersten DSG war. Im Ergebnis zeigt sich die bereichsspezifische Differenzierung in beschriebener Grobstruktur stärker von politischen Kräften als von sachlogischen Argumenten getragen.

320 Wer heute das DSG als Einheitsgesetz in der Hand hält, das den Schutz der Persönlichkeit und der Grundrechte bezweckt, erahnt wenig von der Spannkraft, welche die Auseinandersetzung um die Bedeutung von Kontexten für das Datenschutzrecht in der Schweiz in sich trug. Die aktuellen Entwicklungen in Europa weisen in eine Richtung, in der die systemische Relevanz des Datenschutzrechts weiter in den Hintergrund gedrängt wird. Auch im Bericht der Begleitgruppe Revision DSG wurde dafürgehalten, dass die Bestimmungen für den öffentlichen und den privaten Bereich so weit wie möglich vereinheitlicht werden sollten.[482] Gleichwohl stand die Aufhebung der differenzierenden Mechanik mit Blick auf

482 EJPD, Bericht Begleitgruppe, 8.

den Ausgangspunkt von Personendatenverarbeitungen im öffentlichen gegenüber dem privaten Bereich niemals ernsthaft zur Debatte.

321 In Bezug auf die Frage der Relevanz und Angemessenheit der bereichsspezifischen Differenzierung datenschutzrechtlicher Vorgaben, welche die Schweiz innerhalb des DSG primär durch den entgegengesetzten Ausgangspunkt für den öffentlichen gegenüber dem privaten Bereich implementiert, nimmt das Schweizer System – vergleicht man das Regime mit denjenigen von Europa und den USA – eine *Zwischenposition* ein. Die DSGVO sieht sowohl für den privaten als auch für den öffentlichen Bereich den Ausgangspunkt des Verarbeitungsverbotes mit Erlaubnisvorbehalt vor, wobei diese Entscheidung das Ausgangselement für das monistische System der DSGVO darstellt. Anders dagegen die USA, die den öffentlichen Bereich einer allgemeinen Datenschutzgesetzgebung zuführen, den privaten Bereich indes sektoriell datenschutzrechtlich regulieren. Ein Blick auf den *Fair Credit Reporting Act* brachte hierbei eine in Europa nur ungenügend zur Kenntnis genommene Schutzdimension zu Tage: Der Erlass dient nicht an erster Stelle dem Subjektschutz, wie es der europäischen Tradition entsprechen würde. Vielmehr soll mit dem Erlass die *Integrität des Kredit- und Bankensektors* gewährleistet werden, dessen Effizienz vom Vertrauen in akkurate und faire Personendatenverarbeitungen abhängt. Zugleich macht der Erlass deutlich, dass ökonomische Rationalitäten nicht zwingend gegen, sondern auch für eine Datenschutzregulierung sprechen können.

3.3. Weitere Elemente zur Implementierung des dualen Systems

322 Der infolge der entgegengesetzten Ausgangspunkte *pointierte Dualismus* wird konsequent durch *zusätzliche Instrumente und deren Ausgestaltung* fortgeschrieben, z. B. bezüglich Transparenzvorgaben oder Kompetenzen des EDÖB.[483] Die Totalrevision wird hier allerdings einige Anpassungen bringen, teilweise im Sinne von Vereinheitlichungen.

323 Um in Anknüpfung an den über die Ausgangspunkte definierten Dualismus die Weite und Breite des Feldes zu umreissen: Die allgemeinen Verarbeitungsgrundsätze gemäss Art. 4 DSG resp. Art. 6 nDSG, die als «gemeinsames Fundament» jeder Personendatenverarbeitung bezeichnet wurden und als «gemeinsame Bestimmungen» für den öffentlichen und den privaten Bereich gelten, finden durch die verschiedenen Ausgangspunkte auch eine eigenständige Einbettung und damit Bedeutung.[484] Im privaten Bereich markieren sie die Schranken der grundsätzlich freien Personendatenverarbeitung, während sie im öffentlichen Be-

483 Partikulär ist immerhin der Import eines privatrechtlichen Instrumentariums im Rahmen der Rechtsdurchsetzung in den öffentlichen Sektor gemäss Art. 25 DSG.

484 Vertiefend zweiter Teil, Kapitel IV.–VI.

reich aufgrund des prinzipiellen Verarbeitungsverbotes gewissermassen eine weitere, zweite Schranke liefern. Die generalklauselartigen Bearbeitungsgrundsätze werden im V. Kapitel dieses zweiten Teils zu vertiefen sein.

324 Generalklauselartige Verarbeitungsgrundsätze liefern, sofern sie die Hauptschranke der Personendatenverarbeitung im privaten Bereich darstellen, nur einen *grosszügigen sowie vagen Rahmen*. Zwei Beispiele zur Veranschaulichung: Die Zweckgrundsätze gemäss Art. 4 Abs. 3 resp. Art. 6 Abs. 3 nDSG werden, *erstens*, für den privaten Sektor vom Gesetzgeber nur am Rande näher umrissen. Das DSG selbst verzichtet im privaten Bereich weitgehend darauf, konkretisierte Wertungen und Hierarchisierungen in Bezug auf verschiedene Zweckrelationen vorzusehen.[485] Dagegen werden die Verarbeitungszusammenhänge im öffentlichen Bereich aufgrund des Legalitätsprinzips die Verarbeitungszusammenhänge konkretisiert. *Zweitens* finden sich auch mit Blick auf die Rechtfertigungsgründe für persönlichkeitsverletzende Datenumgänge vom Gesetzgeber keine hinreichend konkretisierten Hinweise.[486]

325 Spezifisch beleuchtet werden in Bezug auf die dualistische Strukturierung die Transparenzvorgaben, denen im privaten Sektor von Gesetzes wegen aufgrund der persönlichkeitsrechtlichen Anknüpfung eine Hauptverantwortung für die Durchsetzung des DSG zugewiesen wird. Zudem werden die Funktion und namentlich die Kompetenzen des EDÖB beleuchtet, die ihrerseits für den öffentlichen und privaten Bereich differenziert werden. Die Totalrevision wird hier Anpassungen bringen, die aber nur angedeutet werden können. Mit ihnen geht eine vereinheitlichende Tendenz einher. Die Darstellung der weiter differenzierenden resp. mit Totalrevision angeglichenen Instrumente ist nicht abschliessend.

3.3.1. Unterschiedliche Transparenzvorgaben und jüngste Angleichungen

326 Ein tragendes Element datenschutzrechtlicher Regulierung ist die Gewährleistung von *Transparenz*.[487] In diesem Zusammenhang sind Auskunftsrechte, Registrierungs- und Informationspflichten sowie der Erkennbarkeitsgrundsatz relevant, vgl. unter noch geltendem DSG die Art. 4 Abs. 3 und Abs. 4 DSG.[488] Auch durch

485 Die wichtigsten Konkretisierungen finden sich für diesen Aspekt in einem gesetzgeberisch konkretisierten überwiegenden Interesse, vgl. Art. 13 Abs. 2 DSG resp. Art. 32 Abs. 2 nDSG.

486 Immerhin hat die Praxis hierbei wichtige Impulse gegeben, indem sie Rechtfertigungsgründe für die Verletzung der allgemeinen Verarbeitungsgrundsätze nur mit Zurückhaltung zulassen will, BGE 136 II 508, «Regeste» und E 5.; entsprechend auch EDÖB, Schlussbericht PostFinance, 6, 23; eine Forderung, wonach der Gesetzgeber vorstrukturierende konkrete Interessenabwägungen vorzunehmen habe, formulierte früh schon Bull, in: Hohmann (Hrsg.), 173 ff., 181.

487 Zur Stärkung der Transparenz mit der Totalrevision: Botschaft DSG 2017–1084, 17.059, 6941 ff., 6972 ff.; EJPD, Bericht Begleitgruppe DSG, 3.

488 Zu den Informationspflichten und dem Auskunftsrecht nach neuem DSG Bühlmann/Lagler, SZW 2021, 16 ff.

die gesetzgeberischen Entwicklungen hinsichtlich der Instrumente, die datenschutzrechtliche Transparenz gewährleisten, zieht sich erneut wie ein roter Faden die Frage nach der Differenzierung resp. Angleichung zwischen dem öffentlichen und dem privaten Bereich.[489] Die nachfolgenden Ausführungen zeichnen die gesetzlichen Entwicklungen aus der *Perspektive des Bereichsbezugs* nach. Hierbei wird sich zeigen, dass im Rahmen der Verabschiedung des ersten DSG über diese Instrumente eine weitere Ausdifferenzierung zwischen öffentlichem und privatem Bereich erfolgte; diese soll mit der Totalrevision indes beseitigt werden.[490]

327 Gemäss Art. 8 Abs. 1 DSG kann jede Person von Inhabern einer Datensammlung grundsätzlich Auskunft über sie betreffende personenbezogene Angaben erhalten. Das *Auskunftsrecht* ist entsprechend vorab an das Vorliegen einer Datensammlung i. S. v. Art. 3 lit. g DSG, nicht aber an deren Registrierung gemäss Art. 11a DSG geknüpft. Es erstreckt sich punktuell auch auf eine *Information über die Herkunft der Daten,* vgl. Art. 8 Abs. 2 lit. a in fine DSG. Im Gesetzgebungsverfahren wurde ein entsprechender Antrag von der Ständerätin Weber gestellt.[491] Vom Berichterstatter Danioth wurde dieses Anliegen, wenig sachlich, als «in der heutigen Zeit sympathisch»[492] bezeichnet. Er erklärte sich zwar mit der Zielsetzung einverstanden, wollte allerdings keine voraussetzungslose Informationspflicht zur Datenherkunft. Im Ergebnis wurde ein Auskunftsrecht verankert, das sich auf die «verfügbaren Angaben» zur Datenherkunft bezieht, vgl. Art. 8 Abs. 2 lit. a in fine DSG. Weiter erstreckt sich das Auskunftsrecht auf den *Zweck der Datenbearbeitung und eine allfällige gesetzliche Grundlage,* Art. 8 Abs. 2 lit. b DSG. Die Einschränkungen des Auskunftsrechts sind unter dem noch geltenden Recht beträchtlich, namentlich auch im privaten Bereich.[493] Gemäss Art. 9 Abs. 4 DSG kann spezifisch und weiterreichend als für den öffentlichen Sektor die Auskunft verweigert werden, sofern ein eigenes überwiegendes Interesse geltend gemacht werden kann und die Daten nicht an Dritte weitergegeben werden.

328 Das Auskunftsrecht verfolgt verschiedene *Stossrichtungen:* Zunächst wird dem betroffenen Datensubjekt ein Anspruch eingeräumt, welcher diesem zumindest formell eine aktive Rolle im Personendatenverarbeitungsprozess zuweisen und es so zumindest ansatzweise dem Status des Informationsobjektes entheben will. Zugleich soll dem Datensubjekt ein *Überprüfungsmechanismus* über die

489 BBl 1988 II 414 ff., 439, 484; EJPD, Erläuternder Bericht, 20 ff. und 56 ff.
490 Vertiefend zu den Entwicklungen mit Blick auf die Transparenzvorgaben Baeriswyl, digma 2020, 6 ff.
491 Weber, AB 88.032, 13. März 1990, 141.
492 Danioth, AB 88.032, 13. März 1990, 141.
493 Belser, in: Schweizer (Hrsg.), 55 ff., 61 ff. bemerkt hierzu, dass es kein Zufall sei, dass die Ausnahmen von der Regel mehr Platz einnähmen als die Regel selbst; zur Regelung nach neuem Recht Bühlmann/Lagler, SZW 2021, 16 ff.

Regelkonformität der Datenbearbeitungshandlungen zur Hand gegeben werden. Dagegen wurden weitere Kontrollinstrumente, beispielsweise eine Bewilligungspflicht für die Einrichtung von Datensammlungen und Informationssystemen durch Private, wie es gewisse ausländische Rechtsordnungen kannten, durch die wirtschaftlichen Interessenvertreter zu Fall gebracht.[494] Entsprechende Entscheidungen sind im Lichte eines Konzeptes zu lesen, das zum einen von einer klaren Differenzierung zwischen öffentlichem und privatem Bereich, zum anderen von einer Anknüpfung des Datenschutzes für den privaten Bereich an den zivilrechtlichen Persönlichkeitsschutz ausgeht. In einem solchen Konzept ist es das Individuum, das betroffene Datensubjekt, dem es an erster Stelle obliegt, die Einhaltung des Datenschutzes durchzusetzen. Das Auskunftsrecht, so wird behauptet, solle dem Subjekt die entsprechende Position einräumen:

> «Über das Auskunftsrecht soll eine betroffene Person […] feststellen können, *ob* und *welche* Personendaten über sie *in welcher Weise* bearbeitet werden. Diese Informationen sollen der betroffenen Person helfen, ihre gemäss DSG bestehenden weiteren Rechte auszuüben. Insofern wird insbesondere auf Art. 4 DSG verwiesen.»[495] [Hervorhebung durch die Autorin]

329 Allerdings hat sich gezeigt, dass Auskunftsrechte und eine daran anschliessende individualrechtliche Überprüfung von Personendatenverarbeitungen auf ihre Gesetzmässigkeit hin faktisch nur marginale Bedeutung erlangt haben.[496] Gleichwohl ist zu attestieren, dass im Zuge der Stärkung datenschutzrechtlicher Anliegen mit den Revisionswellen auch die Geltendmachung der Auskunftsbegehren in der Praxis an Bedeutung gewinnt. Die Implementierung eines Standardprozesses, welcher das Auskunftsrecht regelkonform abwickelt, ist mittlerweile zum Standard geworden.

330 Im Bestreben, das Auskunftsrecht in der Praxis wirksam werden zu lassen, auferlegt Art. 11a DSG Inhabern von Datensammlungen die Pflicht, diese beim EDÖB *registrieren* zu lassen. Es war Koller, der darauf hinwies, dass für ein Auskunftsrecht ein Register der Datensammlungen vorgesehen werden müsse. Zugleich müsse man sicherstellen, dass es nicht zu einer übertriebenen Datenschutzbürokratie komme.[497] Privaten gegenüber wurde die Registrierungspflicht entsprechend beschränkt: Registrierungspflichtig ist nicht jeder Inhaber einer Datensammlung. Vielmehr arbeitet das DSG auch an dieser Stelle mit qualifizierenden Elementen: Registrierungspflichtig ist die Inhaberin einer Datensammlung entweder, wenn sie nach Art. 11a Abs. 3 lit. a i. V. m. Art. 3 lit. c und lit. d DSG regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bear-

494 Vgl. BBl 1988 II 414 ff., 429; Danioth, AB 80.032, 13. März 1990, 142.
495 Rosenthal, HK-DSG, Art. 8 N 1; vgl. zur Auffassung, wonach das Auskunftsrecht der Schlüssel zum Datenschutz sei, auch Belser, in: Schweizer (Hrsg.), 55 ff., 55.
496 Vertiefend zu einem Vollzugsdefizit dritter Teil, VII. Kapitel.
497 Koller, AB 88.032, 13. März 1990, 134.

beitet, oder wenn nach Art. 11a Abs. 3 lit. n DSG regelmässig Personendaten an Dritte bekannt gegeben werden. Zudem finden sich in Art. 11a Abs. 5 DSG mehrere Ausnahmetatbestände («Escape»-Tatbestände), aufgrund derer die Registrierungspflicht entfallen kann. Dazu gehören die Einsetzung eines internen Datenschutzbeauftragten oder das erfolgreiche Durchlaufen eines Zertifizierungsverfahrens. Indem allerdings die Registersammlung Hilfsfunktionen wahrnimmt und die Ausübung des Auskunftsrechts erleichtern soll,[498] schwächt jede Lockerung der Registrierungspflicht die Durchsetzung des Auskunftsrechts. Dies hat Konsequenzen gerade für den privaten Bereich, für den die Einwilligung in die Personendatenerhebung keine grundsätzliche Voraussetzung für eine Verarbeitungshandlung ist. Die Registrierungspflicht von Datensammlungen wird mit der Totalrevision dahinfallen.

331 Ebenfalls das Ziel der Transparenz verfolgt das in der Schweiz unter den allgemeinen Verarbeitungsgrundsätzen formulierte *Erkennbarkeitsgebot*, vgl. Art. 4 Abs. 3 und 4 DSG resp. Art. 6 Abs. 3 nDSG. Das Erkennbarkeitsgebot wird im Zuge der generalklauselartigen Verarbeitungsgrundsätze genauer analysiert. An dieser Stelle genügt die Anmerkung, dass die im DSG gewählte Vorgabe der Erkennbarkeit ein tiefes Transparenzniveau umsetzt. Hier interessieren die Entwicklungen im Hinblick auf die Diskussionen rund um eine Informationspflicht durch die Datenverarbeitenden. Das DSG, wie es 1992 verabschiedet wurde, kannte keine allgemeine Informationspflicht. Dagegen wurde eine solche Informationspflicht im Rahmen der Teilrevision 2006, in Kraft ab 2008, als Antwort auf die «Motion erhöhter Transparenz» eingefügt.[499]

332 Die mit besagter Teilrevision vorgenommenen Änderungen erfolgten u. a. mit dem Ziel, dem Zusatzprotokoll vom 8. November 2001 zum Europarat-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung beitreten zu können.[500] Zudem wurde mit Art. 7a DSG eine Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen eingefügt, die für Bundesbehörden wie Private einschlägig war.[501] Art. 7a DSG vollzog entsprechend einen Vereinheitlichungsschritt, der indes bald wieder rückgängig gemacht wurde: Nur zwei Jahre später und im Jahr 2010 wurde die Bestimmung aufgehoben, ihr Inhalt zweigeteilt sowie mit jeweils eigenständigem, differenziertem Gehalt mit entsprechend divergierendem Schutzniveau implementiert: eine Informationspflicht, die sich auf die

498 Rosenthal, HK-DSG, Art. 11a N 1.
499 Vgl. Botschaft DSG 2003, 2101 ff., 2106 ff.; eine Übersicht über die am 1. Januar 2008 in Kraft getretene Revision des DSG verschaffen die Beiträge in Epiney/Hobi (Hrsg.), 1 ff.
500 Vgl. Botschaft DSG 2003, 2101 ff.
501 Die Durchsetzung eines Verstosses durch Private wurde als Antragsdelikt ausgestaltet, wobei eine Busse von bis zu CHF 10'000.00 ausgesprochen werden konnte.

Beschaffung von besonders schützenswerten Daten sowie diejenige von Persönlichkeitsprofilen im privaten Sektor beschränkt, vgl. Art. 14 DSG, gegenüber einer allgemeinen, nicht auf qualifizierte Daten oder Datenprofile gerichteten Informationspflicht für Bundesorgane, vgl. Art. 18a DSG. Der Mehraufwand hält sich damit für die personendatenverarbeitenden Privaten in Grenzen.

333 Folglich lässt sich festhalten, dass das noch geltende Schweizer Datenschutzgesetz auch im Rahmen der prozeduralen und organisatorischen Instrumente im Zusammenhang mit dem *Auskunftsrecht sowie der Informierungs- und Registrierungspflicht* den Dualismus fortsetzt.

334 Mit der Totalrevision hingegen werden diese Differenzierungen aufgegeben, indem Informationspflichten gemäss Art. 19 ff. nDSG für Datenverarbeitende sowohl des öffentlichen Bereichs des Bundes als auch des privaten Bereichs regeln. Zugleich wird das Instrument des vom EDÖB geführten Registers von Datensammlungen fallengelassen resp. ersetzt durch eine Pflicht der Verantwortlichen, ein Verzeichnis ihrer Verarbeitungstätigkeiten zu führen, Art. 12 nDSG.[502]

335 Folglich lässt sich nach Totalrevision eine Vereinheitlichungstendenz verzeichnen hinsichtlich der Instrumente und Vorgaben an die Transparenz, die bislang zur Akzentuierung des Dualismus eingesetzt wurden. Neben der Erhöhung der Transparenz ist ein zusätzliches Ziel der Totalrevision, den Datenschutz früher greifen zu lassen.[503] Insofern sind verschiedene neue Instrumente zu nennen, die gleichzeitig die Transparenz von Verarbeitungshandlungen wie auch die Eigenverantwortung der Verarbeitenden stärken. Sie werden einheitlich für Verarbeitende des öffentlichen wie des privaten Bereiches verankert. Zu diesen Instrumenten inspirierten die europäischen Entwicklungen: Neben dem Verzeichnis der Bearbeitungstätigkeiten, welches das Basisinstrument der Verantwortlichen zur Erfüllung ihrer datenschutzrechtlichen Pflichten und damit auch der Transparenzvorgaben darstellt, ist die Datenschutz-Folgenabschätzung zu nennen.[504] Sodann sind als Vorgaben, welche die Transparenz der Personendatenverarbeitungsprozesse stärken, die Meldepflichten bei Datensicherheitsvorfällen sowie die Informationspflichten bei automatisierten Einzelfallentscheidungen zu nennen.[505]

336 *Zusammenfassend* lässt sich festhalten, dass die Transparenzvorgaben unter geltendem Datenschutzgesetz für den öffentlichen Bereich dezidiert unterschiedlich

502 Insofern auch Art. 30 DSGVO.

503 Vgl. EJPD, Bericht Begleitgruppe, 3; Baeriswyl, digma 2020, 6 ff.; gefordert wurde dies bereits 2011 durch Brunner, Jusletter vom 4. April 2011, N 66, Zusammenfassung; dass allerdings auch die Transparenz keine Zauberformel ist, bemerkt bereits Bull, NVwZ 2011, 257 ff., 259.

504 Vgl. Art. 12 und Art. 22 nDSG; Art. 30 und Art. 35 DSGVO.

505 Vgl. Art. 24 nDSG und Art. 34 DSGVO; Art. 21 nDSG; zu den umfassenden Informationspflichten gemäss DSGVO Art. 13 f. DSGVO.

gegenüber dem privaten Bereich gestaltet werden. Die Totalrevision bringt sowohl den Ausbau als auch eine Vereinheitlichung der Transparenzvorgaben. Die Erweiterung des gemeinsamen Regelungskorpus bezieht sich damit *weniger auf die harmonisierende Gestaltung des materiellen Datenschutzrechts* für die beiden Bereiche als vielmehr auf die Schaffung gleichermassen zu beachtender Umsetzungsinstrumente sowie auf die Vereinheitlichung prozeduraler und organisatorischer Vorgaben. Damit ist auf den EDÖB und seine Kompetenzen sowie deren Ausbau durch die Totalrevision einzugehen.

3.3.2. Die behördlichen Kompetenzen, insbesondere diejenigen des EDÖB

337 Im Zusammenhang mit der Durchsetzung datenschutzrechtlicher Bestimmungen sind diverse Behörden aktiv: Neben den Zivilgerichten, dem Bundesverwaltungsgericht und dem Bundesgericht sind sodann die Strafbehörden (insb. im Zusammenhang mit der strafrechtlich sanktionierten Verletzung von Berufsgeheimnissen, aber auch nach Totalrevision gemäss Art. 60 ff. nDSG), sodann insb. der EDÖB und auf kantonaler Eben im öffentlichen Bereich die jeweiligen kantonalen Datenschutzbeauftragten.[506] Die Wirksamkeit des Datenschutzrechts hängt von der Ausgestaltung des Rechtsdurchsetzungsinstrumentariums ab.

338 In der Schweiz wurde von Beginn an vertreten, dass die Verwirklichung des Datenschutzrechts auf die Installation *spezieller Organe* angewiesen sei: Danioth äusserte in der Differenzbereinigung im Ständerat seine feste Überzeugung, wonach es sich beim Datenschutzbeauftragten um den «eigentlichen Dreh- und Angelpunkt eines effizienten Datenschutzes» handle.[507] Mit Art. 18 BGÖ wurde die Position des EDB zu derjenigen des EDÖB erweitert.[508] Zuvor war die Funktion auf den Datenschutz beschränkt. Das vom DSG geschaffene Amt ist im fünften Abschnitt des DSG und Art. 26 ff. resp. nach Totalrevision im 7. Kapitel und Art. 43 ff. nDSG geregelt. Die Totalrevision stärkt die Kompetenzen des EDÖB.

339 Die Position des EDÖB nach DSG ist resp. war *ein wirksames Steuerungsinstrument hinsichtlich der Differenzierung des Datenschutzrechts für den öffentlichen gegenüber dem privaten Bereich*.[509] Zudem artikuliert sich mit dieser Funktion, dass der Datenschutz in der Schweiz – anders als es sich aufgrund der Konsultation des Zweckartikels des DSG oder der zivilrechtlichen Rechtsinstrumente für den privaten Bereich, vgl. Art. 15 DSG und Art. 32 nDSG, vermuten liesse – *keineswegs ausschliesslich dem Individualgüterrechtsschutz* dient. Vielmehr wird

506 Zu Aufgaben und Bedeutung der öffentlichen Datenschutzbeauftragten Jöhri, in: Passadelis/Rosenthal/Thür (Hrsg.), § 8.
507 Danioth, AB 88.032, 12. Dezember 1991, 1063.
508 Öffentlichkeitsgesetz vom 17. Dezember 2004, SR 152.3.
509 Vertiefend zur Sanktionierung von Datenschutzverstössen vgl. Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7.

eine spezifische Funktion geschaffen, um der Einhaltung und Durchsetzung des Datenschutzrechts Nachachtung zu schaffen.[510] Anders gewendet: Es greift in der Konzeptionierung des Gesetzgebers zu kurz, die Rechtsdurchsetzung einzig und allein dem Individuum aufzubürden. Der Einhaltung des Datenschutzes wird über die Funktion des EDÖB als eine Aufgabe anerkannt, die durchaus auch von gesellschaftlicher, nicht nur individueller Relevanz ist.

340 Die Einsetzung eines Datenschutzbeauftragten wurde in der Schweiz mit der Hürdenhaftigkeit individueller Rechtsdurchsetzung begründet.[511] Den Gesetzgebungsmaterialien ist zugleich zu entnehmen, dass man schon früh der *Durchschlagskraft der materiellrechtlichen Normen* des DSG skeptisch gegenüberstand; allem voran wurde das Defizit der ungenügende Strukturierungskraft der generalklauselartigen Regeln antizipiert – chiffriert in den Worten von Bundesrat Koller:

> «Die Aufsichtskompetenzen in diesem Gesetz sind nämlich deshalb besonders wichtig, weil das Gesetz ja wirklich nur grundsätzliche Regeln des Datenschutzes aufstellt und daher ihre Konkretisierung auch aufgrund der voraussehbaren technischen Entwicklungen durch die Aufsichtsorgane zu realisieren ist.»[512]

341 Die Einführung der Funktion eines Datenschutzbeauftragten zielte damit auch darauf ab, die Schwächen eines Regelungssystems, das vorrangig mit *Generalklauseln* arbeitet, abzufedern. Die Relevanz des Amtes wird für den privaten wie den öffentlichen Bereich gar als so hoch eingeschätzt, dass erst seine Kontrollen sicherstellen würden, dass die datenschutzrechtlichen «Vorschriften nicht toter Buchstabe blieben.»[513]

342 In den Kompetenzen des EDÖB werden die bereichsspezifische Differenzierung resp. der duale Ansatz des DSG konsequent fortgesetzt. Die grössten Differenzen zwischen den Räten richteten sich auf den Umfang der Kompetenzen – namentlich im privaten Sektor.[514] Nochmals sei der Prozess im Rahmen der Verabschiedung des DSG eingeblendet: Der Entwurf des Bundesrates schlug einen Datenschutzbeauftragten vor, der auch im privaten Sektor Verfügungsgewalt haben sollte.[515] Die ständerätliche Kommission lehnte diesen Vorschlag ab; sie habe sich den «berechtigten Anliegen nach einer Liberalisierung im Bereich der Wirtschaft nicht verschlossen».[516] Im Ständerat wurde später viel daran gesetzt, dem Datenschutzbeauftragten nur restriktive Kompetenzen zuzubilligen – und

510 Vertiefend zu Aufgabe und Bedeutung des öffentlichen Datenschutzbeauftragten Jöhri, in: Passadelis/Rosenthal/Thür (Hrsg.), § 8.
511 Danioth, AB 88.032, 13. März 1990, 127.
512 Koller, AB 88.032, 12. Dezember 1991, 1064.
513 Vgl. Huber, BK-DSG, Art. 27 N 26a; Peter, 276.
514 Vgl. zum Ganzen namentlich Koller, AB 88.032, 12. Dezember 1991, 1064.
515 Vgl. Koller, AB 88.032, 13. März 1990, 146.
516 Danioth, AB 88.032, 13. März 1990, 127.

ein zunächst angedachtes Verbandsklagerecht zu verhindern. Der Datenschutzbeauftragte sollte im privaten Bereich grundsätzlich lediglich eine Ombudsstellung mit beratender Funktion einnehmen und bloss im Falle von Systemfehlern über weiterreichende Kompetenzen verfügen. Verbindliche Verfügungen sollte er, weil man keinen «Datenschutzpolizisten» wolle, im privaten Bereich (vorbehältlich Verfügungen im Zusammenhang mit der Registrier- und Meldepflicht) nicht erlassen können. Im Übrigen sollten «Kontrahenten» an den Zivilrichter verwiesen werden.[517] Entsprechend wurde im Rahmen der Verabschiedung des ersten DSG in der kleinen Kammer die Funktion des Eidgenössischen Datenschutzbeauftragten für den privaten Bereich konsequent auf diejenige eines reinen Ombudsmanns reduziert.[518]

343 Die nationalrätliche Kommission nahm sowohl die Verfügungs- als auch die Klagelegitimation des Datenschutzbeauftragten wieder in den Entwurf auf. Zugleich sollte nach ihr ein eingeschränktes Verbandsklagerecht vorgesehen werden.[519]

344 Im Ergebnis wurde nicht nur die Verfügungskompetenz für den privaten Bereich, sondern auch die Klagelegitimation gestrichen. Und auch das als Kompensation für besagte Streichungen in den privatrechtlichen Verhältnissen diskutierte *Verbandsklagerecht* setzte sich nicht durch.[520] Eine Verbandsklage hatte bereits der Vernehmlassungsentwurf vorgesehen, wobei eine Datenschutzkommission als Rechtsmittelinstanz vorgeschlagen worden war.[521] Zwei Argumente wurden für einen solchen Vorschlag angeführt: Erstens würde sie als prozedurales Instrument eine Kompensationsfunktion für die zurückgestutzten materiellrechtlichen Normen aufweisen. Zweitens habe sie eine andere Stossrichtung, welche die individualrechtliche Konzeption aufweiche:

> «[…] [D]as Verbandsklagerecht im privatrechtlichen Bereich [ist] eine Norm […], die dazu beigetragen hat, auch Enttäuschte versöhnlich zu stimmen und einen gewissen Ausgleich herzustellen. […] Das bedeutet gleichzeitig auch eine Abkehr von der individualistischen Konzeption, wie sie ursprünglich vorgesehen war, die dem einzelnen die ganze Last aufbürdet, den Rechtsweg zu gehen, sein Recht zu suchen mit allen Schwierigkeiten, die damit verbunden sind, mit allen Auflagen, mit allen Kosten […].»[522]

345 Doch auch die Verbandsklage konnte sich im Zuge der Differenzbereinigung nicht durchzusetzen. Sie – die Verbandsklage – stelle

> «im Privatrecht einen Fremdkörper dar […]. Wir haben heute zur Genüge gehört, dass dem Datenschutzgesetz der Persönlichkeitsschutz zugrunde läge. Es geht also um die

517 Danioth, a. a. O.
518 Vgl. Nabholz, AB 88.032, 10. März 1992, 389.
519 Vgl. Koller, AB 88.032, 5. Juni 1991, 874.
520 Rhinow, AB 88.032, 13. März 1990, 146.
521 Danioth, AB 88.032, 13. März 1990, 127.
522 Onken, AB 88.032, 13. März 1990, 146.

> Rechte der Persönlichkeit, es geht nicht um Kollektivinteressen. Und diese Persönlichkeitsrechte kann jeder ohne weiteres selbst vertreten. Er ist nicht darauf angewiesen, dass irgendein Verband für ihn Klage erhebt.»[523]

346 Der Ständerat setzte sich somit weitgehend durch. Das einzige Entgegenkommen bestand darin, dass der Eidgenössische Datenschutzbeauftragte bei sog. Systemfehlern an die Kommission gelangen können sollte.[524]

347 Im Ergebnis wurde eine Regulierung verabschiedet, die einen Datenschutzbeauftragten mit Kompetenzen sowohl für den öffentlichen als auch den privaten Bereich vorsah. Die Gesetzgebungsmaterialien offenbarten, dass dessen hoheitliche Kompetenzen für den privaten Bereich weitreichend *beschnitten wurden*. Er wurde weder mit Verfügungs- noch mit Klagekompetenz ausgestattet. Für deren Fehlen findet sich alsdann keine Verbandsklage als Kompensation. Wenn auch der Datenschutzbeauftragte, wie in den parlamentarischen Beratungen immer wieder betont, keine Entscheidungs- und Verfügungskompetenz haben solle, so sei doch seine «Funktion als Vermittler und Berater Dreh- und Angelpunkt des Datenschutzrechts».[525]

348 Die Ausführungen zum Gesetzgebungsprozess bezüglich der Ausgestaltung der *prozeduralen Instrumente* dokumentieren erneut, dass das *Verhältnis von Subjektschutz einerseits sowie einer systemischen Schutzdimension resp. kollektiven Schutzinteressen andererseit*s – wenn auch nicht explizit unter diesen Titeln verhandelt – von massgeblicher Bedeutung war. Erneut setzte sich der Entscheid für ein duales Regime, welches den privaten gegenüber dem öffentlichen Bereich differenzierend behandelt, in konsequenter Weise in der Ausgestaltung der prozeduralen Instrumente durch. Der grundsätzlich freie private Bereich sollte ebenso wenig durch eine «starke behördliche Hand» zurückdividiert werden. Für den Privatsektor wurde folglich in Bezug auf den Rechtsschutz der individualrechtliche Ansatz recht konsequent implementiert.

349 Die Hauptaufgaben des Eidgenössischen Datenschutzbeauftragten im Privatbereich nach noch geltendem DSG lassen sich anhand *dreier Kompetenzbereiche* strukturieren: *Beratung* gemäss Art. 28 DSG, *Aufsicht resp. Kontrolle* gemäss

523 Schönenberger, AB 88.032, 13. März 1990, 147; in Bezug auf die Verbandsklage im privaten Bereich lässt sich indes im Zuge der ZPO sowie der geplanten Revision ein Wandel der Ansichten nachzeichnen; vgl. zum kollektiven Rechtsschutz Art. 89 ZPO und zur geplanten Änderung Domanig, Jusletter vom 17. Juni 2019, N 8; zur datenschutzrechtlichen Einschlägigkeit von Art. 89 ZPO Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.14; zur Notwendigkeit, kollektive Rechtsdurchsetzungsinstrumente im Feld des «Bioinformationsrechts» anzuerkennen Gruber, 185 ff.

524 Vgl. Danioth, AB 88.032, 12. Dezember 1991, 1064.

525 Huber, BSK-DSG, Art. 28 N 2; zu den Aufgaben des Datenschutzbeauftragten im Privatbereich vgl. Schweizer, in: Schweizer (Hrsg.), 91 ff., 94 ff.

Art. 29 DSG sowie *Information* gemäss Art. 30 DSG.[526] Entsprechend hilfreiche Informationen finden sich themenspezifisch in den Leitfäden des EDÖB.[527]

Das erste Feld «Beratungsaufgaben und -aufwand» des EDÖB gegenüber Privaten wird auf rund 20 Prozent seines Gesamtaufwandes geschätzt.[528] Gleichwohl wird angenommen, dass das Beratungsangebot des EDÖB von vielen Unternehmen und weiteren privaten Datenbearbeitenden gemieden wird, da bei Mängeln stets mit weiteren Kontrollen im Rahmen der Aufsichtskompetenz des EDÖB gerechnet werden müsse.[529] Dass es sich beim Verhältnis privater personendatenverarbeitender Stellen und dem EDÖB folglich eher um ein Verhältnis des Misstrauens als eines der Kooperation handelt, spiegelt sich in einer Aussage eines privaten Datenbearbeiters, wonach er auf die Beratungsdienste des EDÖB verzichte und es stattdessen vorziehe, sich auf einen wirtschaftsfreundlicheren privaten Berater zu stützen.[530] Die Doppelrolle von Beratung und Aufsicht wird dementsprechend als Grund dafür genannt, weshalb Private Beratungen beim EDÖB vermeiden. Sie fürchten dessen Aufsichtsfunktion. Diese doppelte Funktion wird damit als «Schwachpunkt» bezeichnet; dies ungeachtet der Tatsache, dass die Kompetenzen des EDÖB ohnehin schwach sind.[531] 350

Das zweite Kompetenzfeld, die *Aufsichtsfunktion* mit Abklärungs- und Empfehlungsbefugnissen, basiert auf Art. 29 DSG.[532] Die Aufsichtsbefugnis im Privatbereich nach Art. 29 DSG greift indes – anders als diejenige im öffentlichen Bereich nach Art. 27 DSG – *nur in Konstellationen erhöhter oder grundlegender Relevanz*, was das Gesetz unter dem Begriff des Systemfehlers erfasst.[533] Unter noch geltendem Recht stehen damit im Privatsektor nicht alle Datenbearbeitungen unter der Aufsichtshoheit des Datenschutzbeauftragten. Vielmehr wird die *Aufsicht auf drei bestimmte Sachverhalte beschränkt*: Erfasst werden sog. Systemfehler, Art. 29 Abs. 1 lit. a DSG, Aufsichtsaufgaben im Rahmen der Registrierung von Datensammlungen, Art. 29 Abs. 1 lit. b i. V. m. Art. 11a DSG, sowie Informationspflichten nach Art. 29 Abs. 1 lit. c i. V. m. Art. 6 Abs. 3 DSG. 351

Von *besonderem Interesse* für diese Studie sind die «Bearbeitungsmethoden, die geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler)». Der Ausdruck *Systemfehler* wurde vorab mit möglichen Konfigurationsfehlern der Grossrechner in den 1980er Jahren assoziiert. Heute 352

526 Zu den (auch weiteren) Aufgaben, dargelegt für die beiden Bereiche, Jöhri, in: Passadelis/Rosenthal/Thür (Hrsg.), § 8 N 8.29 ff.
527 Abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden.html> (zuletzt besucht am 3. September 2021).
528 Bolliger/Féraud/Epiney/Hänni, 163; Huber, BSK-DSG, Art. 28 N 12a.
529 Huber, BSK-DSG, Art. 28 N 7.
530 Bolliger/Féraud/Epiney/Hänni, 169.
531 Dies., 191 f.
532 Dazu Jöhri, HK-DSG, Art. 27 N 2 f.; BBl 1988 II 414 ff., 414.
533 Art. 29 Abs. 1 lit. a DSG; Rosenthal, HK-DSG, Art. 29 N 1.

werden indes unter den Begriff «Systemfehler» keineswegs bloss technische Defizite i. S. v. Konfigurations- oder Programmierungsfehlern subsumiert. Vielmehr wird damit auch einfach die Art und Weise von Personendatenverarbeitungen adressiert.[534] Würden durch Personendatenverarbeitungen eine Vielzahl von Personen in ihrer Persönlichkeit verletzt, mache es wenig Sinn, jede einzelne Person den Weg über das Zivilgericht beschreiten zu lassen.[535]

353 Das Tatbestandselement will umgekehrt Datenbearbeitungen, die nur wenige Personen in ihrer Persönlichkeit verletzen, von der Aufsicht des EDÖB ausklammern. Die Bestimmung macht eine Vielzahl von Betroffenen, mithin ein *quantitatives Kriterium*, zur Voraussetzung einer Intervention des EDÖB mittels einer Empfehlung. Damit anerkennt das Gesetz, dass die individualrechtliche Durchsetzung, die eine logische Folge der persönlichkeitsrechtlichen Anknüpfung bildet, nicht per se das angemessene Instrumentarium zur Durchsetzung des Datenschutzrechts ist.[536]

354 Ob die *Quantität* der betroffenen Personen das (isoliert) einschlägige Kriterium sein soll, um das Beurteilungselement für den Systemfehler zu liefern und damit die Untersuchungsbefugnis auszulösen resp. um die individualrechtliche Konzeption zu durchbrechen, wird im Laufe dieser Arbeit an verschiedenen Stellen vertieft werden.[537]

355 Jedenfalls ist in den letzten Jahren eine erhöhte Behördenaktivität gestützt auf Art. 29 Abs. 1 lit. a DSG zu verzeichnen.[538] Ein Blick auf die Praxis des EDÖB belegt, dass dieser den Begriff des Systemfehlers nach Art. 29 Abs. 1 lit. a DSG weit auslegt.[539] Der EDÖB hat wiederholt Empfehlungen gegenüber personendatenverarbeitenden Privaten erlassen und diese bei Nichteinhaltung konsequent zur Beurteilung dem Bundesverwaltungsgericht vorgelegt.

356 Neuer der *Entscheid des Bundesverwaltungsgerichts A-3548/2018 i. S. Helsana+ vom 19. März 2019*, in welchem sich das Gericht nicht nur mit der Aktiv- und Passivlegitimation von Kläger und Beklagter befasste, sondern auch mit dem Tatbestand des Systemfehlers, Art. 29 Abs. 1 lit. a DSG.[540] Hierzu führte es aus, dass

534 Meier, N 1903.
535 Huber, BSK-DSG, Art. 29 N 7.
536 Vgl. Brunner, Jusletter vom 4. April 2011, der die individuelle Kontrolle im Datenschutzrecht für den Privatbereich als zu stark ausgeprägt beurteilt.
537 Die Totalrevision gestaltet die Untersuchungskompetenz des EDÖB für den privaten und öffentlichen Bereich deckungsgleich, wobei das Tatbestandselement des Systemfehlers aufgegeben wird, vgl. Art. 49 ff. nDSG; vertiefend zu den Neuerungen dritter Teil, VIII. Kapitel, A.2.; kritisch beurteilt wird das individualistische Privatheitsparadigma auch von Schwartz, Wis. L. Rev. 2000, 743 ff., 759 ff.
538 Bolliger/Féraud/Epiney/Hänni, 161; die Empfehlungen gestützt auf Art. 29 DSG sind abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/empfehlungen.html> (zuletzt besucht am 30. April 2021).
539 Huber, BSK-DSG, Art. 29 N 12.
540 BVGer A-3548/2018, Urteil vom 19. März 2019, E 1 und E 1.6.2.

ein Systemfehler vorliege, wenn «Verarbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen».[541] Eine Empfehlung sei basierend auf Abklärungen möglich, Art. 29 Abs. 3 DSG; wird dieser nicht Folge geleistet, steht dem EDÖB die Klage an das Bundesverwaltungsgericht offen, Art. 29 Abs. 4 i. V. m. Art. 35 lit. b VGG. Passivlegitimiert sei der Empfehlungsadressat. Hinsichtlich der Aktivlegitimation des Klägers und dessen Rechtsbegehren führte das Bundesverwaltungsgericht aus, dass die Beschaffung der Postleitzahl, Geburtsdatum und Versichertennummer eine Verarbeitung von Personendaten i. S. v. Art. 2 Abs. 1 DSG sei. Beim 2. Rechtsbegehren handle es sich nicht um eine Bearbeitungsmethode i. S. v. Art. 29 Abs. 1 DSG; es gehe nur um die Rechtmässigkeit des Endzweckes, über die der EDÖB keine Klagelegitimation habe. Zum Systemfehler führt das Bundesverwaltungsgericht in E 1.6.3. aus, dass hierunter alle Datenbearbeitungen fallen, die sich nicht auf einzelne Fälle beziehen, sondern methodisch, mithin wiederkehrend sind und die potentiell eine grössere Zahl von Personen betreffen können, wobei der EDÖB bei der Beurteilung des Vorliegens des Tatbestandselementes einen weiten Ermessensspielraum habe. Ob die Verarbeitungshandlungen gegen das Rechtmässigkeitsprinzip verstossen, sei dagegen eine Frage des Rechts. Unbestritten sei i. c., dass eine grosse Zahl von Personen von Verarbeitungshandlungen betroffen ist. Folglich wurde die Aktivlegitimation des EDÖB und die Passivlegitimation der Beklagten bejaht.[542] Gemäss Art. 44 Abs. 2 VGG gälte der Grundsatz der Sachverhaltsabklärung von Amtes wegen.[543]

Mit entsprechenden behördlichen Aktivitäten des EDÖB hat das Datenschutz- 357
recht für den privaten Bereich wichtige Impulse erfahren und seiner Einhaltung ist ein gewisser Nachdruck verliehen worden.[544] Damit werden die gesetzlich markant unterschiedlich stark ausgestalteten Aufsichtsniveaus des privaten und des öffentlichen Sektors einander durch die Praxis etwas angenähert. Von Gesetzes wegen bleibt das Schutzniveau im privaten Sektor dennoch geringer, so dass bei Privaten nicht abschliessend feststeht, welche Handlungen der Kontrolle durch den EDÖB zugänglich sind. Es ist nicht jede Verarbeitungshandlung und jedweder Einzelfall, bei der der EDÖB in seiner Aufsichtsfunktion aktiv werden kann. Zudem hat eine Empfehlung vonseiten des EDÖB keinen Verfügungscharakter. Gleichwohl beurteilt der EDÖB die Empfehlung als seine härteste «Sanktionsmöglichkeit».[545]

541 BVGer A-3548/2018, Urteil vom 19. März 2019, E 1.6.3.
542 BVGer A-3548/2018, Urteil vom 19. März 2019, E 1.7. und E 1.8.
543 BVGer A-3548/2018, Urteil vom 19. März 2019, E 2.
544 Vgl. dritter Teil, VII. Kapitel, A., wo eine *Tour d'Horizon* über die entsprechende Behördenpraxis gegeben wird; vgl. sodann die Übersicht über die Empfehlungen: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/empfehlungen.html> (zuletzt besucht am 30. April 2021).
545 Bolliger/Féraud/Epiney/Hänni, 181.

358 Wird gemeinhin von der Kompetenz zu Empfehlungen gesprochen, drängt sich umgekehrt die Frage nach einer *Pflicht zum Erlass einer Empfehlung* auf. In der ständerätlichen Differenzbereinigung wurde zwar eine graduelle Verstärkung angedacht, die Kann-Vorschrift durch eine Muss-Vorschrift zu ersetzen.[546] Letztere konnte sich jedoch nicht durchsetzen. Gemäss Art. 29 Abs. 3 DSG *kann* der EDÖB eine Empfehlung abgeben, er *muss* aber *nicht*.

359 Immerhin wird in der Lehre eine Pflicht zum Erlass einer Empfehlung angenommen, allerdings unter restriktiven Voraussetzungen. So soll gemäss Huber das formelle Verfahren nach Art. 29 DSG mit einer Empfehlung abgeschlossen werden, wenn ein «sehr problematisches Vorgehen, das zentrale Rechte massiv einschränkt», vorliege.[547] Anders gilt im öffentlichen Sektor der Erlass einer Empfehlung von Gesetzes wegen grundsätzlich als zwingend.[548]

360 Der EDÖB hat darüber hinaus nach noch geltendem Recht gegenüber Privaten keine eigentlichen Sanktionsmöglichkeiten; das Verhängen von Bussen resp. Strafen oder die rechtswirksame Anordnung von Massnahmen ist ihm nach DSG nicht erlaubt. Dies gilt auch im Rahmen der Untersuchungskompetenzen gemäss Art. 29 Abs. 2 DSG. Wird ihm die Mitwirkung verweigert, stehen ihm selbst keine Zwangsmassnahmen offen. Anders als beispielsweise die Wettbewerbskommission, kann er auch keine Hausdurchsuchung anordnen.[549] Immerhin hat der EDÖB die Möglichkeit, bei einer verweigerten Mitwirkung Strafanzeige zu erstatten, vgl. Art. 34 DSG.[550]

361 Wird eine Empfehlung des EDÖB gemäss Art. 29 Abs. 3 DSG durch den Adressaten des privaten Sektors missachtet, kann der EDÖB den Fall dem Bundesverwaltungsgericht vorlegen, Art. 29 Abs. 3 i. V. m. Art. 33 DSG. Stützt dieses die Empfehlung des Beauftragten durch einen Entscheid, erlangt die Angelegenheit Rechtsverbindlichkeit. Für den Fall, dass die Empfehlung gerichtlich nicht bestätigt wird, vgl. 29 Abs. 4 a. E. DSG, ist der EDÖB zur Verwaltungsgerichtsbeschwerde an das Bundesgericht legitimiert: Eine Empfehlung des EDÖB im Privatrechtsbereich nach Art. 29 DSG gilt als öffentlich-rechtliche Angelegenheit gemäss Art. 82 ff. BGG. Damit wird eine ursprünglich aus dem Privatbereich hervorgehende und auf dem DSG für den privaten Sektor basierende Empfehlung des EDÖB im Instanzenzug als öffentlich-rechtliche Angelegenheit gehandhabt.[551]

546 Danioth, AB 88.032, 12. Dezember 1991, 1064.
547 Huber, BSK-DSG, Art. 29 N 26.
548 Ders., a. a. O., Art. 27 N 13 f. und zu Art. 29 N 26.
549 Zur Wettbewerbskommission mit ihren umfangreichen Kompetenzen vgl. Art. 18 ff. KG, insb. auch Art. 42 KG.
550 BBl 1988 II 414 ff., 485.
551 Huber, BSK-DSG, Art. 29 N 35b.

Ergänzend ist auf die Möglichkeit des EDÖB hinzuweisen, eine *vorsorgliche Massnahme* (ggf. selbst im Superprovisorium) beim Präsidium der ersten Abteilung des Bundesverwaltungsgerichts zu beantragen, Art. 33 Abs. 2 DSG. Zudem kann der EDÖB innerhalb gewisser Schranken die Öffentlichkeit über seine Empfehlungen informieren, Art. 30 Abs. 2 DSG (vgl. zum Informationsauftrag sogleich). 362

Kaum Anlass zur Diskussion gab im Lichte des gewählten Ausgangspunktes für den privaten Sektor und der persönlichkeitsrechtlichen Anknüpfung die *dritte Aufgabe und Kompetenz* des EDÖB, dessen *Informationstätigkeit*. Der EDÖB erstattet jährlichen Bericht an die Bundesversammlung, mit zeitgleicher Aushändigung an den Bundesrat. Diese periodischen Berichte werden publiziert, vgl. Art. 30 Abs. 1 DSG.[552] Ausserdem kann der EDÖB in Fällen des Allgemeininteresses die Öffentlichkeit in geeigneter Weise informieren, vgl. Art. 30 Abs. 2 DSG. Dieses Instrument ist in seiner Wirkungsmacht für die Einhaltung des Datenschutzrechts gerade auch im Zuge des Bedeutungswandels, der dem Datenschutz zugemessen wird, nicht zu unterschätzen, zumal datenschutzrechtliche Verfehlungen heute als Risiko für die Reputation eines Unternehmens gelten. Die Informierung der Öffentlichkeit durch den EDÖB kann folglich durchaus ein wirksames Instrument sein, um datenschutzrechtlichen Belangen Nachdruck zu verleihen. 363

Nach dieser *Tour d'Horizon* über die Kompetenzen des EDÖB, namentlich im privaten Bereich, vor Totalrevision ist festzustellen, dass diese im internationalen Vergleich – bereits vor den mit der DSGVO einhergehenden Neuerungen – als schwach zu bewerten sind.[553] Auf Kritik stiess in der Schweiz insb. die niedrige Aufsichts- sowie die fehlende Verfügungskompetenz des EDÖB für den privaten Sektor.[554] Allerdings ist das gewählte Regime vor dem Hintergrund des für den privaten Bereich gewählten Ausgangspunktes *systemkongruent*. 364

In einer Rückblende lässt sich in der Auseinandersetzung um die Kompetenzen des EDÖB und die Ausgestaltung der prozeduralen Durchsetzungsinstrumente im Zuge der Verabschiedung des ersten DSG eine hohe Ambivalenz hinsichtlich des Entscheides für einen weitgehend freien, privaten Verarbeitungsbereich mit seiner persönlichkeitsrechtlichen Anknüpfung ausmachen. Die Frage nach der Bedeutung systembedingter Trennungen resp. Durchbrechungen zeigt sich ebenso im Themenfeld rund um die Kompetenzen des EDÖB in eindrücklicher Weise. Aufgrund der dualen Struktur mit der Entscheidung für einen prinzipiell freien Bereich im privaten Sektor (nicht jede Personendatenverarbeitung ist verboten, sondern erst die qualifizierte – vertiefend hierzu die nachfolgenden Teile) sowie der persönlichkeitsrechtlichen Anknüpfung des DSG erschiene es inkonsequent, 365

552 Vgl. <https://www.edoeb.admin.ch/edoeb/de/home.html> (zuletzt besucht am 30. April 2021).
553 Huber, BSK-DSG, Art. 29 N 1a; Bolliger/Féraud/Epiney/Hänni, 199, 213.
554 Meier, N 1878.

dem Datenschutzbeauftragten Verfügungs- und Klagekompetenzen zuzuweisen. Anders präsentiert sich das Bild dagegen beispielsweise im Bereich des Wettbewerbsrechts, wo der Markt tiefgreifend reguliert ist und dementsprechend auch behördliche Verfügungskompetenzen vorgesehen sind.

366 Zudem ist es mit Blick auf den «rasanten technischen Fortschritt» fraglich, ob die (bessere) Einhaltung des Datenschutzrechts *in erster Linie* durch die starke Hand eines interventionsmächtigen Staates sichergestellt werden kann. Eine Strategie der DSGVO liegt in einem weit angelegten behördlichen Massnahmen- und Sanktionskatalog, vgl. Art. 83 f. DSGVO. In der Schweiz wurden in diesem Kontext allem voran die drakonischen Bussen zur Kenntnis genommen, die sich der Höhe von Bussen bei Kartellrechtsverstössen annähern.[555]

367 *Zweierlei* gilt es anzufügen: *Zum einen* beschränkt sich die DSGVO keineswegs auf die besagten Bussen, um der Einhaltung der datenschutzrechtlichen Vorgaben Nachachtung zu verschaffen. Vielmehr kommt den Behörden ein weit- und tiefgreifendes Arsenal an hoheitlichen Befugnissen und möglichen Massnahmen zur Verwirklichung des europäischen Datenschutzrechts zu.[556] Die DSGVO wählt somit den Ansatz, die datenschutzrechtlichen Vorgaben mittels starker obrigkeitlicher Massnahmen zu sichern. Der entsprechende behördliche Massnahmenkatalog gemäss DSGVO steht im Einklang mit einem Regime, das von einem grundsätzlichen und einheitlichen Verarbeitungsverbot für den privaten wie den öffentlichen Bereich ausgeht, und ist insofern systemisch kongruent. *Zum anderen* allerdings ist nicht zu übersehen, dass die DSGVO die «Verantwortlichen» (und Auftragsverarbeiter), die personendatenverarbeitenden Stellen selbst, an erster Stelle nachdrücklich in die Pflicht nimmt, für die Einhaltung der datenschutzrechtlichen Vorgaben zu sorgen. Insoweit bringt die DSGVO zugleich eine Stärkung der *Eigenverantwortung* mit sich.

368 Damit ist auf die Neuerungen gemäss Totalrevision einzugehen. Im Rahmen der Verabschiedung des Gesetzes stiessen gerade die Neuordnung der Befugnisse sowohl durch den EDÖB, Art. 49 ff. nDSG, als auch durch die kantonalen Strafbehörden, Art. 60 nDSG ff., auf Widerstand.[557] Die Totalrevision stärkt die Position des EDÖB für den privaten Bereich.[558] Insofern ist eine Annäherung der Normierung des Sanktionssystems für den privaten Bereich gegenüber dem öffentlichen

555 Vgl. Passadelis/Roth, Jusletter vom 4. April 2016, N 23; eine Übersicht über die Bussgeldentscheidungen unter DSGVO geben Kehr/Zapp, CB 2020, 100 ff.; Schweighofer, Jusletter IT vom 9. Februar 2016, N 9.

556 Hierzu auch Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f.

557 Vgl. Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zum Vorentwurf, 44 ff., abrufbar unter: <https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ve-berd.pdf> (zuletzt besucht am 30. April 2021).

558 Vertiefend vgl. Rosenthal, Jusletter vom 16. November 2020, N 181 ff.; vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff., 7168 ff.

Bereich festzustellen. Die über die Gestaltung der Sanktionen bislang erfolgte Fortsetzung und Ausprägung des dualistischen Konzeptes wird nunmehr überwunden. Neu beschränkt sich das «schärfste Instrument» des EDÖB im privaten Bereich nicht mehr auf die «Empfehlung». Vielmehr agiert er nach Totalrevision über das ordentliche Verwaltungsverfahren und kann Verfügungen erlassen, vgl. Art. 51 nDSG. Im Rahmen der durchzuführenden Untersuchungen, die nicht nur beim Vorliegen eines Systemfehlers angezeigt sind, werden ihm mehrere Befugnisse zugesprochen, Art. 50 nDSG. Ein Verstoss gegen datenschutzrechtliche Vorgaben ist von Amtes wegen zu *untersuchen*, vgl. Art. 49 Abs. 1 nDSG, wobei nach Abs. 2 ein Opportunitätsprinzip für Verletzungen von geringfügiger Bedeutung greifen kann. An dieser Stelle kann das nach bisherigem Recht etablierte Kriterium des Systemfehlers als Auslegungshilfe dienen: Beim Vorliegen eines Systemfehlers dürfte das Opportunitätsprinzip nicht greifen.

369 Der EDÖB selbst kann auch nach totalrevidiertem DSG keine Verwaltungsbussen erlassen. Immerhin ist festzustellen, dass in der Unternehmenspraxis die Verfügung, eine bestimmte Verarbeitungshandlung zu unterlassen, einschneidender als eine Bussgeldzahlung sein kann. Strafbestimmungen und einen Bussenkatalog führen die Art. 60 ff. nDSG ein. Zuständig für die Aussprache entsprechender Bussen bei Vorliegen der Tatbestände gemäss Art. 60 ff. nDSG sind die kantonalen Strafbehörden. Bemerkenswerterweise nicht von einer Bussenandrohung erfasst ist die Verletzung der allgemeinen Verarbeitungsgrundsätze, das Herzstück des materiellrechtlichen Datenschutzrechts. Nach Art. 60 nDSG ist insb. eine Verletzung der im Rahmen der Untersuchung durch den EDÖB statuierten Mitwirkungspflichten strafbewehrt. Mit den Bussen belegt sind nicht die Unternehmen, stattdessen die verantwortlichen Personen. Wer dies allerdings im Unternehmen ist (der Datenschutzbeauftragte, die Mitglieder der Geschäftsleitung oder des Verwaltungsrates oder auch Mitarbeitende niedrigerer Hierarchiestufen), ist aktuell nicht geklärt.

370 Mit dem Fokus auf den Ausbau und die Verschärfung der behördlichen Massnahmen vermag man indes eine Stossrichtung, welche die Neuerungen sowohl nach DSGVO als auch nach totalrevidiertem DSG verfolgen, nicht in den Blick zu nehmen: Betont und gestärkt wird die *primäre Verantwortung der jeweils personendatenverarbeitenden Stellen für die Einhaltung der datenschutzrechtlichen Vorgaben*. Symbolhaft ausgedrückt wird dies auch in der neuen Bezeichnung der Verarbeitenden als «Verantwortliche».[559] Diese «präventive» Funktionsmechanik

559 Der Bericht der Begleitgruppe Revision DSG, Normkonzept zur Revision des DSG vom 29. Oktober 2014, spricht von dem Ziel, dass das Datenschutzrecht früher greifen solle, vgl. EJPD, Bericht Begleitgruppe, 3; vgl. Art. 5 lit. j nDSG, wobei die Rolle des Verantwortlichen namentlich auch im Zusammenspiel mit der Rolle des Auftragsverarbeitenden relevant ist, vgl. Art. 5 lit. k nDSG; vgl. Art. 24 ff. DSGVO. Zudem wird das Konzept der gemeinsam Verantwortlichen anerkannt; die Rol-

wird über (teilweise neue) Instrumente wie das Verzeichnis der Verarbeitungstätigkeiten und umfassende Dokumentations- und Rechenschaftspflichten, aber auch die Datenschutz-Folgenabschätzung, die Strategien von «privacy by design» und «privacy by default» sowie die allfällige Funktion eines betrieblichen Datenschutzbeauftragten (beachte die unterschiedliche Forderung qua DSGVO und totalrevidiertem DSG) verwirklicht. Eine richtungsweisende Stossrichtung der Neuerungswellen ist darin zu sehen, dass die personendatenverarbeitenden Stellen selbst in die Pflicht und Verantwortung genommen werden. Das führt im Ergebnis zur Forderung einer umfassenden Daten-Governance und Datenschutz-Compliance.[560] Folglich greift es zu kurz, die «Verbesserung» des Datenschutzes allein im Ausbau der behördlichen Kompetenzen oder der Betroffenenrechte zu verorten. Eine wirksame Rechtseinhaltung im Feld des Datenschutzes im privaten Bereich kann weder isoliert über das (persönlichkeitsrechtlich verletzte) Datensubjekt noch durch einen «starken» Staat – beides «retrospektive» Ansätze – gewährleistet werden. Vielmehr bedarf es an erster Stelle der Verantwortung der Verarbeitenden. Die Einhaltung des Datenschutzrechts fusst offensichtlich auf mehreren Säulen. Welche Bedeutung die bei Datenschutzverletzungen zuständigen Behörden in der Schweiz den neu eingeräumten und verschärften Rechtsdurchsetzungsinstrumenten einräumt, wird sich erst weisen müssen. Unter der DSGVO kann festgestellt werden, dass die zuständigen Behörden der verschiedenen Länder sehr unterschiedlich scharf vorgehen.[561]

C. Ergebnisse und zusammenfassende Kontextualisierung

371 Das *primäre Charakteristikum* des DSG ist sein *Dualismus* mit divergierendem Schutzniveau für den öffentlichen Bereich des Bundes gegenüber dem privaten Bereich. Er wird über einen materiellrechtlichen Grundsatzentscheid vollzogen. Der Dualismus wird in markanter Weise durch einen *entgegengesetzten Ausgangspunkt* für die beiden Sektoren implementiert: Das Datenschutzgesetz sieht für den öffentlichen Bereich der Bundesbehörden ein grundsätzliches Verbot der Personendatenverarbeitungen mit Erlaubnistatbeständen vor. Für den privaten Bereich hingegen gilt die Maxime der Bearbeitungsfreiheit, die durch Schranken begrenzt wird. Die wichtigsten Schranken sind die generalklauselartigen Bearbeitungsgrundsätze, denen sich nachfolgend das Kapitel V. widmet. Der besagte

lendefinierung ist eine zu klärende Vorfrage, an die sich die jeweils zu beachtenden Datenschutzpflichten anschliessen.

560 Vgl. zum Begriff der Compliance und spezifisch zur Datenschutz-Compliance einige Jahre vor dem Inkrafttreten der DSGVO Petri, Jusletter IT vom 1. September 2010, N 3 ff. und N 13 ff.; m. E. zu eng die Beschreibung unter dem Titel der Governance Räther, ZHR 2019, 94 ff., 97; vertiefend hierzu dritter Teil, VIII. Kapitel, A.2.6.

561 Vgl. <https://datenrecht.ch/behoerden/page/2/> (zuletzt besucht am 30. April 2021).

Dualismus, der über einen entgegengesetzten Ausgangspunkt umgesetzt wird, gilt nach geltendem Recht und wird auch mit der Totalrevision nicht aufgegeben, vgl. Art. 12 i. V. m. Art. 4 ff. DSG und Art. 17 ff. i. V. m. Art. 4 DSG resp. Art. 30 ff. i. V. m. Art. 6 ff. nDSG und Art. 33 ff. i. V. m. Art. 6 ff. nDSG.

372 Den Dualismus aufzugeben und einen monistischen Ansatz zu implementieren, stand in der Schweiz weder im Zuge der beiden Teilrevisionen noch im Zuge der Totalrevision zur Debatte.[562] Das DSG setzt damit nach geltendem Recht wie nach Totalrevision – in Abbildung der Mechanik von Art. 28 ZGB – *für den privaten Bereich an der qualifizierten Personendatenverarbeitung* an. Nicht jede Personendatenverarbeitungshandlung begründet eine Persönlichkeitsverletzung. Vielmehr sind es nur qualifizierte Verarbeitungshandlungen, die eine Persönlichkeitsverletzung markieren, die indes gerechtfertigt werden können. Dagegen gilt das Legalitätsprinzip resp. Prinzip des Verarbeitungsverbotes mit der Notwendigkeit eines Erlaubnistatbestandes, der i. d. R. in einem Spezialgesetz definiert wird, für den öffentlichen Bereich des Bundes. Das Datenschutzrecht der Schweiz ist somit ein bereichsspezifisch stark ausdifferenziertes Rechtsgebiet.

373 Materiellrechtlich anders definiert die DSGVO heute sowohl für die Personendatenverarbeitung durch Behörden als auch für diejenige durch Private ein Verarbeitungsverbot mit Erlaubnisvorbehalt, vgl. Art. 6 DSGVO – ein Monismus, umgesetzt durch den datenschutzrechtlich strikteren Ausgangspunkt.

374 In der Schweiz wird der mit den entgegengesetzten Ausgangspunkten dezidiert bereichsspezifisch differenzierende, dualistische Ansatz *im noch geltenden DSG konsequent weiter umgesetzt*. Zwei Instrumente, die eher umsetzungsrechtlicher Natur sind, wurden genauer beleuchtet: zum einen die Transparenzvorgaben, zum anderen die Kompetenzen des EDÖB. Nach noch geltendem DSG setzte sich der Dualismus entsprechend konsequent fort, namentlich über *unterschiedliche Transparenzvorgaben* für die beiden Bereiche, aber auch über die *unterschiedliche Gestaltung der Kompetenzen des EDÖB*. Seine Kompetenzen waren für den privaten Bereich schwach gestaltet. Die Rechtsdurchsetzung wird im noch geltenden Recht in konsequenter Umsetzung des Dualismus und der persönlichkeitsrechtlichen Anknüpfung in erster Linie den Individuen zugewiesen.[563]

375 In Bezug auf besagte Instrumente bringt die *Totalrevision* bedeutsame Neuerungen, die zu einer Annäherung resp. Vereinheitlichung und damit zu einer Abmilderung der bereichsbezogenen Ausdifferenzierung der beiden Bereiche führen. Zum einen werden die Transparenzvorgaben für die beiden Bereiche vereinheitlicht,

562 Brunner, Jusletter vom 4. April 2011, N 1; kritisch zum Festhalten am bisherigen System Wermelinger/Schweri, Jusletter vom 3. März 2008, N 64 ff.; die Frage, ob sich die ursprüngliche Unterscheidung zwischen den beiden Bereichen weiterhin durchführen lasse, wirft explizit auf Baeriswyl, in: Baeriswyl/Rudin (Hrsg.), 47 ff., 59.

563 Vertiefend zweiter Teil, VI. Kapitel.

zum anderen werden die Kompetenzen des EDÖB für den privaten Bereich sowie für die strafrechtliche Verantwortung ausgebaut. Selbst wenn der Massnahmenkatalog in der Schweiz gestärkt wird, bleibt der behördliche Massnahmen- und Sanktionskatalog hinter demjenigen der DSGVO zurück. Die Schweiz wählt hinsichtlich der bereichsspezifischen Ausdifferenzierungsentscheidung also einen Mittelweg: Annäherungen *ja* (insb. durch die Umsetzungsinstrumente), durchgängige Vereinheitlichung *nein* (insb. durch Beibehaltung des materiellrechtlichen Dualismus, basierend auf dem entgegengesetzten Ausgangspunkt).

376 Wenn sich gerade in der DSGVO eine Überzeugung niederschlägt, wonach die Einhaltung des Datenschutzes einer starken behördlichen resp. staatlichen Hand bedarf, setzt sie, wie auch die Totalrevision des DSG, auf eine weitere Strategie: Die personendatenverarbeitenden Stellen werden durch zusätzliche Instrumente – z. B. das Verarbeitungsverzeichnis – als *primär Verantwortliche* in die Pflicht genommen, proaktiv die Vorgaben des Datenschutzrechts zu implementieren. Die DSGVO wie das totalrevidierte DSG zielen darauf ab, eine bessere faktische Einhaltung des Datenschutzrechts zu erreichen. Dies geschieht keineswegs bloss durch eine Stärkung der Position des Individuums sowie der behördlichen Massnahmen und Sanktionen, sondern in erster Linie dadurch, dass die *Verarbeitenden früher und nachdrücklicher in die Pflicht und Eigenverantwortung* genommen werden, datenschutzkonform zu handeln und sich entsprechend organisatorisch sowie prozedural aufzustellen. Insofern folgt die Totalrevision einem von der DSGVO vorgezeichneten Entwicklungstrend in Richtung einer umfassenden Datenschutz-Compliance.

377 Diesen Vereinheitlichungs- und Weiterentwicklungslinien zum Trotz hat die Betrachtung der Entstehungsgeschichte des DSG vor Augen geführt, von welch zentraler Bedeutung die Frage nach der Ausdifferenzierung des Datenschutzrechts zwischen Bereichen war: Die *Auseinandersetzung um die Bereichsdifferenzierung der datenschutzgesetzlichen Regulierung* für den öffentlichen und privaten Bereich war die eigentliche Ursache für die lange Dauer des Gesetzgebungsprozesses zur Verabschiedung des DSG. Sowohl der gescheiterte Versuch, ein Datenschutzgesetz für den privaten Bereich gänzlich zu verhindern, als auch die Abschwächung der Vorgaben für den privaten Bereich gingen massgeblich von der Privatwirtschaft aus. Nach langem Ringen konnte ein Gesetz in Kraft gesetzt werden, dessen Basiskonstruktion im Zweikammersystem zu verorten ist.

378 Dass die datenschutzrechtlichen Herausforderungen gleichwohl facettenreicher sind und spezifische Erwägungen weiterer Verarbeitungskontexte nicht ausgeblendet werden, zeigt sich anhand mehrerer Elemente: im öffentlichen Bereich anhand des Verarbeitungsverbotes mit Erlaubnistatbestand und der damit verbundenen hohen Bedeutung des Legalitätsprinzips, wonach jede Personendatenverarbeitung, um rechtens zu sein, einer rechtlichen Grundlage ausserhalb

des DSG bedarf. Hier liegt die Bruchstelle, an welcher plurale Verarbeitungszusammenhänge – Steuerbereich, Migrationskontext, Strafverfolgung usf. – datenschutzrechtlich angekoppelt werden.[564] Aber auch der private Bereich zeigt sich nicht als einheitlicher Bereich. Vielmehr ist insofern auf spezialrechtliche Gesetze und Bestimmungen zu verweisen, so beispielsweise auf das Humanforschungsgesetz oder den arbeitsrechtlichen Kontext. Zudem ist die Funktion des EDÖB indikativ für den Gedanken, dass es im Datenschutzrecht keineswegs bloss isoliert um den Individualrechtsschutz geht, sondern dass das Rechtsgebiet allgemeiner gesellschaftliche Anliegen schützt.

379 Kernstrukturelement des schweizerischen Datenschutzgesetzes bleibt allerdings – zumindest materiellrechtlich – der Dualismus zwischen öffentlichem und privatem Bereich. Die Beschreibung des Dualismus im DSG, des insofern einschlägigen Gesetzgebungsprozesses im Rahmen seiner Verabschiedung sowie der jüngsten Entwicklungslinien hat die Relevanz rund um die *Fragen systemdifferenzierender Normierungen für den Datenschutz* explizit gemacht. Dieser Dimension allerdings wurde – gerade auch von wissenschaftlicher Seite – nicht zuletzt aufgrund der Anknüpfung von datenschutzrechtlichen Regelungen am Subjektschutz bislang nicht die gebührende Aufmerksamkeit geschenkt.[565]

380 Die Varianzen der gesetzgeberischen Ansätze sind aktuell beträchtlich: Während die DSGVO einen Monismus vorsieht und die Dualität datenschutzrechtlicher Vorgaben zwischen öffentlichen und privaten Personendatenverarbeitenden aufgibt, die Schweiz hingegen am Dualismus zwischen öffentlich und privat festhält, implementiert man in den USA einen anderen Ansatz. Der öffentliche Bereich wird datenschutzgesetzlich reguliert: auf Bundesebene durch den *Privacy Act* 1974. Dagegen kennt das US-amerikanische System kein datenschutzrechtliches Querschnittsgesetz für den privaten Bereich. Im privaten Bereich wird datenschutzrechtlich -nicht zuletzt infolge des tiefliegenden Misstrauens gegenüber staatlichen Eingriffen – mit sektorspezifischen Erlassen legiferiert.[566] Exempla-

564 Für die Schweiz wurde die Bekanntgabe von Personendaten resp. die informationelle Trennung zwischen verschiedenen Bundesbehörden mit jeweils unterschiedlichen Aufgaben von Baumann, SJZ 2006, 1 ff., 3 ff. thematisiert; anwendbar seien teilweise spezialgesetzliche Regelungen, teilweise das DSG und hierbei insb. auch der Zweckbindungsgrundsatz, wobei die öffentliche Verwaltung keine Informationseinheit sei.

565 Druey attestiert im Jahr 1990 sinngemäss, dass trotz der Verabschiedung des DSG das Bewusstsein aufseiten der Juristen für informationsrechtliche Fragen eher peripher sei, vgl. Druey, «Daten-Schmutz», 379 – eine solche Einschätzung wird noch einige Jahre zutreffend bleiben – trotz der Verabschiedung des DSG; vgl. immerhin die Frage nach einer systemischen Schutzdimension des Bankkundengeheimnisses Walder Wyss AG (Isler/Kunz/Müller/Schneider/Vasella), N 14 ff.

566 Hierzu Buchner, 15 ff.; mit dem hier vorgeschlagenen Recht auf informationellen Systemschutz wird in die Richtung sektorspezifischer Regulierung gewiesen. Eine solche darf sich indes nicht auf die innersektorielle Gestaltung beschränken; vielmehr sind insb. die Datenflüsse zwischen verschiedenen Sektoren resp. Gesellschaftsbereichen zu gestalten; eine sektorspezifische Lösung erwähnt Cichocki, Jusletter IT vom 21. Mai 2015, N 51; zur Tendenz der Gesetzgebungen in den 1970er Jahren ausserhalb von Deutschland in Richtung bereichsspezifischer Regelungen zu gehen, vgl. Mallmann, 11.

risch wurde auf den *Fair Credit Reporting Act* hingewiesen, dessen einleitender § 602 festhält, dass die akkurate und faire, transparente Personendatenverarbeitung im Kontext des Credit Reporting der Effizienz des Kreditwesens und Banksystems dient, wohingegen unfaire Methoden das Vertrauen in den Sektor erodieren und sich damit der Bereich selbst unterminiert.[567] Bemerkenswerterweise wurde in der Schweiz genau in diesem Kontext und in Bezug auf das Bankkundengeheimnis die Frage nach einer Systemschutzdimension aufgeworfen.[568]

381 Eine solche *systemische Schutzdimension* wird in einem Modell, wie es die Schweiz vorsieht, gerade auch aufgrund der Anknüpfung an die Individualrechte des Datenschutzrechts nur beschränkt sichtbar. Noch weiter in den Hintergrund gedrängt wird sie in einem monistischen System, wie es die DSGVO implementiert, die bereits auf die Basiskategorisierung von öffentlichem und privatem Sektor verzichtet. Immerhin ist in Bezug auf eine systembezogene Differenzierung auf Folgendes hinzuweisen: Indem die DSGVO ebenso Instrumente der «Selbstregulierung» vorsieht, namentlich den betrieblichen Datenschutzbeauftragten, die Integration bereichs- und branchenspezifischer Verhaltensregeln sowie die Zertifizierung, anerkennt sie trotz ihres Monismus die Relevanz bereichsspezifischer Differenzierungen.[569] Mit dem betrieblichen Datenschutzbeauftragten, aber auch mit Zertifizierungen oder der Berücksichtigung branchenspezifischer «Codes of Conduct» wird gewissermassen die «Re-Strukturierung» der Bereiche, in der Grobstruktur auch des privaten Bereiches, vollzogen. Umgangssprachlich ausgedrückt: Der Datenschutz und dessen Einhaltung wird über solche Instrumente der Selbstregulierung in die «Hände» der jeweiligen (privaten) Akteure zurückgespielt. Diese sind es, in primärer Selbstverantwortung, die durch die Erfüllung der zahlreichen Pflichten sicherzustellen haben, konform («compliant») mit dem Datenschutzrecht zu sein. Das Konzept setzt damit früher an und ergänzt so ein Konzept, das Personendatenverarbeitung primär in ihrer Relevanz als Persönlichkeitsverletzung liest.

382 Gänzlich aus dem Blick gerät bei einem Fokus auf das (statisch-räumlich gedachte) Zweikammersystem (Dualismus öffentlich versus privat) und die Person sowie Personendaten als Quasi-Objekte (Dualismus Subjekt versus Objekt) die *dynamische Dimension* der Thematik, wie sie im ersten Teil dieser Arbeit herausgearbeitet wurde. Der historische Teil hat u. a. anhand der Geheimworte und Geheimhaltungspflichten eine Sichtweise herausgearbeitet, welche Datenflüsse innerhalb, namentlich aber ebenso zwischen verschiedenen Kontexten und Berei-

567 Zum Rechtstext vgl. <https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf> (zuletzt besucht am 4. Juli 2021).
568 Walder Wyss AG (Isler/Kunz/Müller/Schneider/Vasella), N 14 ff.
569 Vgl. Art. 37 ff. DSGVO; zur Zertifizierung gemäss DSGVO für Cloud-Dienste als effizientes Überwachungsinstrument vgl. Borges, Jusletter IT vom 23. Februar 2017, N 3 f.

chen in das Blickfeld rücken lässt. Die Frage nach einer Systemschutzdimension wird denn auch jüngst im Zusammenhang mit dem Bankgeheimnis aufgeworfen.[570]

383 Zwei zeitgenössische Beispiele sollen die *datenschutzrechtliche Herausforderung und Brisanz von Personendatenflüssen zwischen verschiedenen Kontexten und Bereichen* veranschaulichen: Hierzu an erster Stelle ein Zeitungsbericht mit dem Titel «Das Geschäft mit den Daten. Schweizer Gemeinden verdienen an Adressen».[571] Der Beitrag legt in der Rubrik «Wirtschaft» den Finger auf den Knotenpunkt. Mehrere Gemeinden hatten auch an Private Adressen verkauft und damit ökonomische Interessen verfolgt. Diese Adressen hatten die Gemeinden infolge erfüllter staatlicher Meldepflichten gegenüber der Einwohnerkontrolle bei einer Niederlassung auf dem Gemeindeterritorium erlangt. Für die Gemeinden wurde damit der Adresshandel zu einem Geschäft, das die Staatskasse alimentierte. Die Transferproblematik bei bereichsspezifisch differenzierenden Regulierungen beschrieb für Deutschland grundlegend Buchner, der die Zugriffsbegehrlichkeiten des einem strengeren Datenschutzregime unterliegenden öffentlichen Sektors auf die Datenbestände des niederschwelliger geregelten privaten Bereichs thematisiert.[572] Illustrativ ist in diesem Zusammenhang zweitens der jüngste Facebook-Skandal, wo Personendaten aus persönlichen Kommunikationsbeziehungen, ausgetauscht über Facebook, zu Cambridge Analytica flossen (mutmasslich gegen Entgelt), wobei in der Folge Auswertungen stattfanden und gezielt auf das Wahlverhalten der Facebook-Nutzenden eingewirkt wurde.[573]

384 Nachdem in diesem IV. Kapitel gezeigt wurde, inwiefern die bereichsspezifische Differenzierung für und im Datenschutzrecht eine Kernfrage ist, wendet sich das V. Kapitel den *generalklauselartigen Verarbeitungsgrundsätzen* zu. Diese wurden als das «gemeinsame Fundament» des DSG für den öffentlichen und privaten Bereich beschrieben.[574] Allerdings sind die Grundsätze, wegen des gerade beschriebenen Dualismus, in *je unterschiedliche Funktionsmechanismen* eingebettet – je nachdem, ob sie für den öffentlichen oder den privaten Bereich zur Anwendung kommen. Ihre Bedeutung gilt es in diesen unterschiedlichen Anknüpfungen zu untersuchen.

570 Walder Wyss AG (Isler/Kunz/Müller/Schneider/Vasella), N 14 ff.
571 Vetsch, Weltwoche vom 24. Oktober 1979, 9.
572 Vgl. Buchner, 72 ff.; zum kommerziellen Adresshandel zwischen dem deutschen öffentlich-rechtlichen Rundfunk und privaten Adresshändlern aus datenschutzrechtlicher Perspektive Hermerschmidt, MMR 2005, 155 ff., 156 ff.
573 Vgl. insofern exemplarisch den Bericht: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> (zuletzt besucht am 30. April 2021); Söbbing, InTeR 2018, 182 ff.
574 So Danioth, AB 88.032, 13. März 1990, 127.

V. Kapitel: Zweites Strukturmerkmal – Generalklauseln

A. Die gemeinsamen Verarbeitungsgrundsätze

1. Vorbemerkungen

385 Wie sieht die materielle Datenschutzregulierung aus, welche die Schweiz an ihr duales System anknüpft? Im Zentrum stehen die *generalklauselartigen Bearbeitungsgrundsätze,* wie sie sich als Kernelemente datenschutzrechtlicher Normierung etabliert haben. Sie sind heute namentlich in Art. 4 DSG sowie in Art. 5 DSGVO niedergelegt. Mit der Totalrevision finden sich diese in Art. 6 nDSG. Im Zuge der Verabschiedung des ersten eidgenössischen Datenschutzgesetzes warb Bundesrat Koller, im Bewusstsein um den Widerstand von privatwirtschaftlicher Seite, für die Implementierung eines «gemeinsamen Minimal-Standards» mit den Worten:

> «Ein wesentliches Merkmal des schweizerischen Entwurfs besteht darin, dass dieser sowohl den Datenschutz in der Bundesverwaltung wie auch jenen im privaten Bereich im gleichen Gesetz regelt. Für eine solche Konzeption spricht, dass die allgemeingültigen Datenschutzgrundsätze auf beiden Gebieten die gleichen sind. Der Betroffene kann durch die Informationsbeschaffung und -weitergabe Privater ebenso stark wie durch Datenbearbeitungen von Privaten verletzt werden. Aber auch das Anliegen einer ökonomischen Gesetzgebung legt eine solche Lösung nahe, denn so lassen sich Überschneidungen und Wiederholungen vermeiden, letztlich also Normen sparen.»[575]

386 Allerdings wurden auch in der Schweiz die *Defizite generalklauselartiger Regelungen* anerkannt. Das Datenschutzrecht blieb nicht von der Kritik verschont, die wiederholt und allgemein an Regulierungen per Generalklauseln geübt worden war.[576] Für Deutschland war es namentlich Simitis, der den Preis eines solchen Normierungskonzeptes als hoch bezeichnete. Allem voran das «Allgemeininteresse» würde mit seiner «kaum zu übertreffenden Elastizität» als «Über-Generalklausel» alles in den Schatten stellen.[577] In der Schweiz wurden die Schwächen des generalklauselartigen Regimes im Gesetzgebungsprozess wie folgt adressiert:

---

575 Koller, AB 88.032, 5. Juni 1991, 949.

576 Kritisch zu den exzessiven Generalklauseln im Datenschutzrecht Simitis, NJW 1997, 281 ff.; Wächter, Falsifikation; Rosenthal, in: Datenschutz-Forum Schweiz (Hrsg.), 69 ff., 70 ff.; grundlegend zu Generalklauseln u. a. Auer, Materialisierung, 1 ff., 130; Röthel, in: Riesenhuber (Hrsg.), 225 ff.; Teubner, *passim*; zur Einschätzung, wonach die ungenügende Steuerungswirkung der Generalklauseln einen bedeutsamen Grund für das sog. Vollzugsdefizit des DSG liefern, dritter Teil, VII. Kapitel.

577 Simitis, NomosKomm-BDSG., Einleitung: Geschichte – Ziele – Prinzipien, N 44 f.

> «M. Danioth s'est félicité tout à l'heure de la densité réglementaire réduite de ce projet de loi, par conséquent de la marge d'appréciation et d'interprétation laissée pour son application. Il n'est pas question d'instruire ici un procès d'intention, Mais il nous reste qu'à espérer que notre confiance est en l'occurrence bien placée. Au fond, toute cette affaire de protection des données est bel et bien basée sur la confiance. Durant des années, les maîtres de fichiers, qu'il s'agisse de fichiers publics ou privés, ont abusé de l'incroyable crédulité des citoyens, des consommateurs, des patients, des assurés, des locataires, des bénéficiaires de prestations sociales, bref, de tous ces très ou trop braves gens. Presque tous avaient un sentiment de confiance et de crédulité qui confinait à la naïveté la plus totale.»[578]

387 Ähnlich skeptisch äusserte sich im Gesetzgebungsprozess Onken im Zusammenhang mit der bereits dargelegten Änderung betreffend die Verweigerung des Auskunftsrechts.[579] Sollte eine Auskunft im ursprünglichen Vorschlag nur sofern unbedingt notwendig verweigert werden dürfen, könnte nunmehr ein Auskunftsbegehren abschlägig behandelt werden, sofern ein «diffuses» überwiegendes Interesse dazu bestünde.[580] Gleichwohl setzte sich in der Schweiz die Überzeugung durch, wonach die Vorteile einer generalklauselartigen Regulierung überwiegen würden:[581]

> «Im Rahmen der Regulierungsfolgenabschätzungen wurde angetönt, unbestimmte Rechtsbegriffe seien nach Möglichkeit zu vermeiden. Beim Datenschutzgesetz handelt es sich indes um eine technologieneutrale Rahmengesetzgebung, welche auf eine Vielzahl unterschiedlich gelagerter Fälle anwendbar bleiben und sich dynamisch weiterentwickeln können muss. Dem Bedürfnis nach exakteren, bereichsspezifischen Ausführungsbestimmungen dienen jedoch die Empfehlungen der guten Praxis.»[582]

388 Damit ist das *zweite Strukturelement* des DSG eingeführt: *die Regelung mittels Generalklauseln resp. unbestimmten Rechtsbegriffen*. Der letzte Passus bezeichnet nicht nur ein Charakteristikum des eidgenössischen Datenschutzgesetzes, sondern problematisiert und rechtfertigt es zugleich.

389 Wenn auch mit der Totalrevision die Systematisierung, Redaktion sowie Gewichtung der allgemeinen Bearbeitungsgrundsätze punktuell neugestaltet wird, bleiben insb. die Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, Zweckbindung und Erkennbarkeit sowohl für den privaten als

578 Jaggi, AB 88.032, 13. März 1990, 132.
579 Hierzu zweiter Teil, IV. Kapitel, B.3.3.1.
580 Onken, AB 88.032, 13. März 1990, 129.
581 Mit der Totalrevision werden generalklauselartige Vorgaben auch in Zukunft im Regelungs- und Gesetzeskonzept eine zentrale Bedeutung einnehmen. Die gesetzliche Leitidee, gleichermassen wie diejenige des Dualismus (vgl. insofern zweiter Teil, IV. Kapitel) sowie diejenige der persönlichkeitsrechtlichen Anknüpfung für den privaten Bereich (vgl. insofern zweiter Teil, V. Kapitel), wird auch in Zukunft die Struktur des DSG prägen. Die Totalrevision weicht folglich von den in dieser Schrift herausgearbeiteten drei Strukturmerkmalen nicht ab. Gleichwohl werden ergänzende und flankierende neue Akzente und Aspekte vorgesehen. Dargestellt werden diese Entwicklungen im dritten Teil, insb. im XIII. Kapitel, A.
582 EJPD, Erläuternder Bericht, 36; zur Regelung des Datenschutzes in einem Rahmengesetz auch Danioth, in: Schweizer (Hrsg.), 9 ff., 10.

auch den öffentlichen Sektor zentrale Verarbeitungsvorgaben, vgl. Art. 6 nDSG. Im privaten Bereich greift darüber hinaus die «Persönlichkeit» resp. der Persönlichkeitsschutz als generalklauselartiges Regime, vgl. Art. 12 f. DSG resp. Art. 30 f. nDSG, insb. mit der Generalklausel im Zusammenhang mit den Rechtfertigungsgründen.

390 Die *generalklauselartigen Verarbeitungsgrundsätze* sind *Kernelemente des materiellen Datenschutzrechts*. Sie werden nachfolgend analysiert, mit dem Ziel, Wirkungsweisen, Stärken und Schwächen für ein effektives Datenschutzkonzept herauszuschälen. An den Verarbeitungsgrundsätzen ändert die Totalrevision nichts Wesentliches; die bislang entwickelte Lehre und Rechtsprechung dürfte künftig ebenso einschlägig sein. Da beim Abschluss dieser Studie Totalrevision des DSG gerade erst verabschiedet worden war, bleibt es bei punktuellen Hinweisen auf deren Neuerungen. Immerhin ist dies materiellrechtlich nicht sonderlich problematisch, da die generalklauselartigen allgemeinen Verarbeitungsgrundsätze keine namhaften Veränderungen erfahren. Ins Zentrum gerückt wird somit die datenschutzrechtliche Normierung des noch in Kraft stehenden DSG anhand der gemeinsamen, weitgehend generalklauselartigen Verarbeitungsgrundätze, an die sich private wie öffentliche Stellen des Bundes zu halten haben. Auf die DSGVO wird ebenso bloss am Rande eingegangen. Immerhin ist in Erinnerung zu rufen, dass diese wegen ihres extraterritorialen Anwendungsbereiches auch für personendatenverarbeitende Stellen in der Schweiz einschlägig sein kann, vgl. Art. 3 Abs. 2 lit. a und lit. b DSGVO. Sie ist indes nicht nur aus diesem Grund richtungsweisend für das zeitgenössische Datenschutzrecht.

2. Einbettung

391 Es ist Art. 4 DSG resp. Art. 6 nDSG, der die wichtigsten Vorgaben – «les grands principes», wie Meier sie nennt – für Verarbeitungen von personenbezogenen Angaben durch Bundesbehörden wie Private formuliert.[583] Die Verarbeitungsgrundsätze werden, obschon sehr allgemein gehalten, als «harter Kern» des Datenschutzgesetzes bezeichnet.[584] Sie sind stets dann zu beachten, wenn keine spezifischen anderen Vorgaben greifen. Damit bilden sie zugleich eine Art Auffangregime. Einige der Generalklauseln haben ausserhalb des Datenschutzrechts als eher junge Rechtsmaterie eine lange Rechtstradition, andere gelten als spezifischer mit datenschutzrechtlicher Intention aus der Wiege gehoben, obschon sie

583 Meier, N 621 ff.
584 Ders., N 621; zu den datenschutzrechtlichen Grundsätzen vgl. auch Epiney, in: Epiney/Theuerkauf (Hrsg.), 1 ff., 23 ff.

sich durchaus aus bereits bekannten Grundsätzen ableiten lassen.[585] Der vertieften Analyse sind *fünf Bemerkungen* vorauszuschicken:

392 *Erstens* eröffnet jede Normierung mittels unbestimmter Rechtsbegriffe Räume der Flexibilisierung, Konkretisierung und Rechtsfortbildung.[586] Seit jeher versuchte die juristische Methodenlehre mittels einer trennscharfen Klassifizierung und Kategorisierung der verschiedenen offenen Rechtsbegriffe – unbestimmte Rechtsbegriffe, Generalklauseln, Blankett-Normen, Ermessensbegriffe usf. – eindeutige Vorgaben und damit klare methodische Anweisungen für die Rechtsanwendung zu präsentieren.[587] Im Privatrecht werden bis heute leidenschaftliche Debatten rund um die Lückentheorie und das Verhältnis von Art. 1 und Art. 2 ZGB sowie über das Verhältnis ihrer Absätze geführt. Ebenso intensiv verhandelt werden Fragen nach der Abgrenzung von Konstruktionen, die ein Vorgehen nach Art. 1 ZGB und damit die sog. Auslegung ansprechen, gegenüber den Ermessensentscheidungen nach Art. 4 ZGB.[588] Zu Recht wird festgehalten, dass einige Abgrenzungen und Begrifflichkeiten keineswegs eindeutig und strukturierend ausfallen.[589] Entsprechende Spannungsfelder finden sich selbstredend ebenso in einem Datenschutzrecht wieder, das seine allgemeinen Verarbeitungsgrundsätze in Gestalt unbestimmter Rechtsbegriffe zu einem tragenden Fundament seiner Normierung macht. Die Konkretisierung und deren Methode zeigt sich in einem jungen Rechtsgebiet, das im Schatten der «undurchschaubaren Technologien» operiert und das bislang gerade in der Schweiz – zumindest bis es zum Entwicklungsanstoss qua DSGVO und zur Verabschiedung der Totalrevision des DSG kam – wenig wissenschaftliche wie behördliche Aufmerksamkeit fand, als gleichermassen akut wie herausfordernd. Denn die Wirksamkeit des Datenschutzrechts hängt auch davon ab, wie erfolgreich konkretisierte und damit strukturierende Vorgaben an Datenverarbeitungen formuliert werden.[590]

393 *Zweitens* sind die entgegengesetzten Ausgangspunkte, wie sie im Rahmen des *Dualismus* des DSG im IV. Kapitel dieses zweiten Teils beschrieben wurden,

585 Meier, N 629.
586 Vgl. hierzu z. B. Auer, Materialisierung, *passim*.
587 Dazu Pfaffinger, ZSR 2011, 417 ff., 426.
588 Vgl. Meier-Hayoz, BK-1962-ZGB, Art. 4 N 19 ff.; Hrubesch-Millauer, ZBJV 2013, 469 ff.; BGE 141 III 43, E 2.5.1., Analogie nur bei Lücke; BGE 140 III 636, E 2.1.; 140 III 206, E 3.5.; 138 V 346, E 5; vgl. Dürr, ZK-ZGB, Art. 1 N 230 ff., 525 ff.; zur Analogie als Art. 1 Abs. 1 ZGB zugehöriges Auslegungselement vgl. Hausheer/Jaun, Art. 1 ZGB N 202 f.; zum Analogieschluss als Instrument der Lückenfüllung und Art. 1 Abs. 2 ZGB zugehörend s. Kramer, 191 ff., 211; Honsell, BSK-ZGB I, Art. 1 N 12; vertiefend zur Analogie Emmenegger/Tschentscher, BK-ZGB, Art. 1 N 376 ff. mit Zuweisung zur Lückenfüllung, N 380 und N 164 mit Präsentation eines Vierphasenmodells; kritisch zur etablierten Methodenlehre mit Blick auf Art. 1 ZGB und das Verhältnis von Gesetzestext und Auslegung Amstutz, ZSR 2007, 233 ff., wobei er spezifisch auf die Relevanz der Polykontextualität der modernen Gesellschaft eingeht, 242 ff.
589 Vgl. Kramer, 183 ff. und 199 ff.
590 Eindrücklich insofern Bull, NVwZ 2011, 257 ff., 258, wonach ein Ausweichen in höchstrangige Grossformeln vom Problem ablenke.

ebenso in Bezug auf die allgemeinen Verarbeitungsvorgaben einschlägig. Die allgemeinen Bearbeitungsgrundsätze werden in den beiden Bereichen auf *unterschiedlichen Stufen wirksam*: Im öffentlichen Bereich ist gesetzlich eine *doppelte Schranke* vorgesehen, wohingegen im privaten Sektor nur eine *einfache Schrankenlösung* greift: Im öffentlichen Sektor definiert das prinzipielle Verarbeitungsverbot eine *erste Schranke* für Personendatenverarbeitungen durch Bundesbehörden, vgl. Art. 17 DSG resp. Art. 34 nDSG; eine *zweite Schranke* setzen daran anschliessend, gewissermassen auf einer zweiten Stufe, die allgemeinen Verarbeitungsgrundsätze, vgl. Art. 4 DSG resp. Art. 6 nDSG. Einer solchen doppelten Schrankenordnung entspricht auch das in der DSGVO gewählte Konzept, vgl. Art. 5 f. DSGVO, wenn auch für beide Sektoren. Anders definiert das DSG vor und nach Totalrevision im privaten Bereich die allgemeinen Verarbeitungsgrundsätze als die entscheidenden Schranken der prinzipiell zulässigen Personendatenverarbeitung, vgl. Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 nDSG. Weil die generalklauselartigen Bearbeitungsgrundsätze insb. gemäss Art. 4 DSG resp. Art. 6 nDSG das Kernstück des materiellen Datenschutzrechts im privaten Sektor darstellen – ihnen kommt die entscheidende Schrankenfunktion zu –, räumt diese Arbeit ihnen einen zentralen Platz ein.

394 *Drittens* ist festzustellen, dass infolge des Dualismus als erstem Charakteristikum des DSG auch der *Interpretationsspielraum* für die beiden Sektoren *nicht identisch* ist. Eine entsprechende Differenzierungsnotwendigkeit wird ungenügend reflektiert, sowohl was die Anwendung als auch was die Auslegung der generalklauselartigen Bearbeitungsgrundsätze betrifft. Wenn oftmals davon gesprochen wird, dass der öffentliche und der private Sektor im DSG ein *gemeinsames Fundament* aufweisen, namentlich mit den allgemeinen Bearbeitungsgrundsätzen gemäss Art. 4 DSG resp. Art. 6 nDSG, dann ist diese Aussage unter Anerkennung des *entgegengesetzten Ausgangspunktes für den privaten gegenüber dem öffentlichen Bereich* zu lesen.

395 *Viertens* ist im Rahmen einer Konkretisierung der generalklauselartigen Verarbeitungsgrundsätze nicht nur ihre Verortung *innerhalb des DSG* relevant, sondern auch ihre *allgemeine Einbettung in die Schweizer Rechtsordnung*, allem voran in das *Verfassungsrecht*. Allerdings finden sich für Art. 13 Abs. 2 BV und dessen Schutzgehalt divergierende Interpretationen – sie reichen von einem behaupteten Recht auf informationelle Selbstbestimmung über die Verbürgung eines Privatsphärenschutzes bis zu einer wortgetreuen «Interpretation» als Missbrauchsgarantie.[591] Solche verfassungsrechtlichen Interpretationsdivergenzen schlagen sich

591 Beispielhaft zu einem Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV mit analogem Gehalt gemäss Rechtsprechung des Volkszählungsurteils des Bundesverfassungsgerichts Baumann, SJZ 2006, 1 ff., 2; Schweizer, SG-Komm.-BV, Art. 13 Abs. 2 N 72; Graham-Siegenthaler, 155; Aebi-Müller, N 541 ff.; Belser, in: Epiney/Fasnacht/Blaser (Hrsg.), 19 ff., 34 ff.; von der

in der Nomenklatur von Lehre und Rechtsprechung zum eidgenössischen Datenschutzgesetz nieder.[592]

Zur Behauptung, wonach in der Schweiz ein Recht auf informationelle Selbstbestimmung garantiert werde – entgegen dem Wortlaut von Art. 13 Abs. 2 BV und der Beschreibung des Systems des DSG für den privaten Bereich als eines der Bearbeitungsfreiheit mit Schranken –, mag die verfehlte Einordnung der *Gültigkeitsvoraussetzungen* der datenschutzrechtlichen Einwilligung bei den allgemeinen Verarbeitungsgrundsätzen, Art. 4 Abs. 5 DSG, verleiten. Die Totalrevision hält an dieser Systematik fest, vgl. Art. 6 Abs. 6 und Abs. 7 nDSG. Der Einwilligung kommt im Schweizer DSG für den privaten Sektor indes *nicht* dieselbe Funktion zu wie in einem System des Verarbeitungsverbotes mit Erlaubnisvorbehalt, wie es Art. 6 DSGVO vorsieht. Ebenda ist die Einwilligung, mangels anderweitigem Erlaubnistatbestand, Voraussetzung für eine rechtmässige Datenverarbeitung. Bei Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG handelt es sich weniger um einen allgemeinen Bearbeitungsgrundsatz als vielmehr um die grundsätzlichen Voraussetzungen für eine rechtsgültige Einwilligung für den Fall, dass eine solche verlangt wird. 396

Fünftens: Die *allgemeinen Bearbeitungsgrundsätze* können in der Schweiz aus *zwei Perspektiven* gelesen werden: Auf der einen Seite formulieren sie gegenüber den Verantwortlichen Vorgaben an die Verarbeitung von Personenangaben, indem sie für den privaten Bereich die Schranken der im Ausgangspunkt grundsätzlich freien Bearbeitung festlegen. Auf der anderen Seite wird anhand der Verarbeitungsgrundsätze und namentlich des Verstosses gegen dieselben die datenschutzrechtliche Persönlichkeitsverletzung – der privatrechtliche Datenschutz gilt als Emanation von Art. 28 ZGB – markiert.[593] Ein Verstoss gegen die allgemeinen Datenverarbeitungsgrundsätze wird vom Gesetzgeber als Persönlichkeitsverletzung definiert. In der Lehre besteht insofern Konsens, als ein Verstoss gegen die Grundsätze von Art. 4 Abs. 1–4 DSG *per se eine Persönlichkeitsverletzung* begründet.[594] Diese Regelmechanik gilt auch nach der Totalrevision. *E contrario* heisst dies, dass Datenbearbeitungen im privaten Sektor, welche die anhand der allgemeinen Bearbeitungsgrundsätze definierten Mindestvorgaben *einhalten*, *keine* Persönlichkeitsverletzung darstellen. Das ist in doppelter Hinsicht konsequent: Zum einen spiegelt es das System von Art. 28 ZGB wider. Demnach be- 397

Gewährleistung eines privatrechtlichen Rechts auf informationelle Selbstbestimmung spricht Probst, in: Epiney/Sangsue (Hrsg.), 41 ff., 52 f.; zum verfassungsrechtlichen Schutz der informationellen Privatheit Rudin, in: Sutter-Somm/Hafner/Schmid/Seelmann (Hrsg.), 416 ff. und 425.

592 Zum Ganzen Rosenthal, HK-DSG, Art. 4 N 1 f.

593 Vgl. vertiefend zweiter Teil, VI. Kapitel.

594 Rosenthal, HK-DSG, Art. 4 N 2; damit eröffnet sich die Frage, ob Rechtfertigungsgründe die Widerrechtlichkeit entfallen lassen, wobei die persönlichkeitsrechtliche Methode der Abwägung von Interessen vorgesehen wird; vgl. hierzu Art. 12 f. DSG und Art. 30 f. nDSG, vertiefend zweiter Teil, VI. Kapitel, B.

gründen nur «qualifizierte» Handlungen resp. Eingriffe eine Persönlichkeitsverletzung. Nicht hinreichend schwere Eingriffe sind persönlichkeitsrechtlich irrelevant – sie tangieren unter Umständen die Persönlichkeit, verletzen diese aber nicht.[595] Zum anderen implementiert das Regelungskonzept konsequent den Entscheid für den Ausgangspunkt der grundsätzlichen Datenverarbeitungsfreiheit mit Schranken im privaten Bereich.

398 Die Grundsätze gemäss Art. 4 Abs. 1–4 DSG resp. Art. 6 Abs. 1–5 nDSG sind die *bedeutsamsten materiellen Vorgaben der Datenschutzgesetzgebung*.[596] Weitere Leitprinzipien, Pflichten und Rechte werden aus ihnen abgeleitet. Sie lassen sich als allgemeinste Vorgaben im Sinne eines Mindeststandards zur *Gewährleistung der fairen oder integren Datenverarbeitung* beschreiben.

B. Die generalklauselartigen Verarbeitungsgrundsätze im Einzelnen

1. Das Rechtmässigkeitsprinzip

1.1. Grundlagen

399 Das Prinzip der Rechtmässigkeit erscheint selbsterklärend, ist es doch Fundament der *gesamten Rechtsordnung und des Rechts an sich*: Jedes individuelle wie behördliche Handeln hat im Einklang mit den Forderungen des Rechts zu stehen – in diesem Sinne artikuliert das Rechtmässigkeitsprinzip seinen eigenen Geltungsanspruch. Folglich ist der Grundsatz der Rechtmässigkeit nicht auf bestimmte Rechtsfelder beschränkt. Vorrangige Bedeutung hat er im öffentlichen Recht als *Verfassungsgebot in Gestalt des Legalitätsprinzips resp. Gesetzmässigkeitsgebotes* erlangt, vgl. Art. 5 Abs. 1 BV, zunächst für die *Grundrechtsdogmatik* und das *Verwaltungsrecht*.[597] Verankert wird der Rechtmässigkeitsgrundsatz sodann im *Strafrecht*, Art. 1 StGB. Im *Privatrecht* hingegen dominiert ein Gegenbegriff – die Widerrechtlichkeit, vgl. Art. 28 ZGB oder Art. 41 OR.

400 In der allgemeinen Datenschutzgesetzgebung figuriert die *Rechtmässigkeit meist an erster Stelle der allgemeinen Verarbeitungsgrundsätze*. An vorderster Stelle des materiellen Datenschutzrechts und der allgemeinen Verarbeitungsvorgaben steht der Grundsatz der Rechtmässigkeit mit Art. 5 Abs. 1 lit. a DSGVO im Datenschutzrecht der EU. Die Schweiz verankert den Verarbeitungsgrundsatz in Art. 4

595 Meili, BSK-ZGB I, Art. 28 ZGB N 38.
596 Mit der Totalrevision wird das Richtigkeitsgebot in den Artikel zu den allgemeinen Verarbeitungsgrundsätzen integriert.
597 Vgl. BGE 142 II 182; spezifisch zur Rechtmässigkeit und Zweckmässigkeit als rechtliche Entscheidungsräume der Verwaltung und damit zum Ermessen im Verwaltungsrecht vgl. Neupert, 3 ff.

Abs. 1 DSG in seiner geltenden Fassung wie folgt: «Personendaten dürfen nur rechtmässig bearbeitet werden.» Art. 6 Abs. 1 nDSG lautet neu «Personendaten müssen rechtmässig bearbeitet werden.» Die Totalrevision des DSG verwendet damit eine imperative Formulierung. Es war nicht immer so, dass sämtliche Verarbeitungen von Personendaten allgemein unter das Rechtmässigkeitsgebot gestellt wurden. Vielmehr fand anfänglich eine Beschränkung auf die Beschaffung von Personendaten mit rechtmässigen Mitteln statt. Damit wurde der Anwendungsbereich und Gehalt des Grundsatzes deutlich enger gesetzt.[598]

Welche konkrete Bedeutung und Rolle wird dem Rechtmässigkeitsgrundsatz als Verarbeitungsgrundsatz in der Schweizer Datenschutzlehre und -rechtsprechung zugewiesen? Gehalt und Umfang gelten als umstritten.[599] Vorhandene Konkretisierungsversuche weisen beträchtliche Divergenzen auf. 401

Nachfolgend wird ein Befund vertieft, der sich bereits in den bisherigen Erörterungen andeutete und der den datenschutzrechtlichen Rechtmässigkeitsgrundsatz als *facettenreich sowie multifunktional* benennt. Denn der Grundsatz ermöglicht es, die *komplette Landschaft datenschutzrechtlicher Regulierung* innerhalb, aber auch ausserhalb des Datenschutzgesetzes in den Blick zu nehmen. In diesem Sinne hat das Rechtmässigkeitsprinzip eine *Brückenfunktion*. Parallel dazu lassen sich anhand des Grundsatzes systemische Ansätze des Datenschutzrechts freilegen. Der Rechtmässigkeitsgrundsatz ist somit weit mehr als eine rhetorische Selbstbeschwörung des Datenschutzgesetzes bezüglich seines eigenen Geltungsanspruches.[600] 402

Die folgende Analyse wird von einer Überzeugung angestossen, wonach sich eine konzeptionelle Schwachstelle des Datenschutzrechts dort auftut, wo man sich mit dem Rechtmässigkeitsprinzip auf eine Selbstbestätigung des rechtlichen Geltungsanspruches zurückzieht. Wenn einem prioritär angesiedelten Verarbeitungsgrundsatz keine oder kaum darüber hinausreichende Wirkung verliehen wird, gebietet sich ein kritisches Hinterfragen. An dieser Stelle soll geprüft werden, ob dem Rechtmässigkeitsprinzip weiterreichende Gestaltungsmacht im und für das Datenschutzrecht innewohnt. Ziel der Reflexion ist, den Verarbeitungsgrundsatz dergestalt produktiv zu machen, wie es einem auf dem ersten Platz des materiel- 403

598 BBl 1988 II 414 ff., 460 und 517.

599 M. w. H. BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4., insb. 5.4.1.; zu den gerichtlichen Ausführungen in Bezug auf die datenschutzrechtlichen Vorgaben vgl. Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f.; Vasella/Ziegler, digma 2019, 80 ff.; Pärli, SZS 2018, 107 ff.; vertiefte Analysen stehen gleichwohl aus.

600 Vgl. zum Vollzugsdefizit des Datenschutzes dritter Teil, VII. Kapitel; veranschaulichend der Beitrag von Baeriswyl, digma 2010, 140 ff. unter dem Haupttitel «Geschichten aus dem Wilden Westen», wobei er beschreibt, dass der Datenschutz im Zeitalter der Digitalisierung aufgrund des Regelungsregimes des DSG für den Privatbereich auf der Strecke bleibt.

len Datenschutzgesetzes angesiedelten «allgemeinen Verarbeitungsgrundsatz» gebührt.

1.2. Facettenreiche Konkretisierungen – Systematisierung

404 Ein Blick auf die Erwägungen von Lehre und Rechtsprechung zum Rechtmässigkeitsprinzip im Datenschutz für den privaten Sektor dokumentiert, dass sein Gehalt von einer Konsolidierung weit entfernt ist.[601] Als unbestritten gilt einzig, dass eine

> «Datenbearbeitung immer dann unrechtmässig im Sinne von Art. 4 Abs. 1 DSG ist, wenn der Datenbearbeiter dabei gegen eine Rechtsnorm verstösst, die den Schutz der Persönlichkeit bezweckt, dies unabhängig davon, ob sich die Rechtsnorm im Datenschutzgesetz oder in einem anderen Erlass befindet. Nicht geklärt ist jedoch, ob auch der Verstoss gegen eine Rechtsnorm, die nicht (zumindest auch) dem Schutz der Persönlichkeit dient, die Bearbeitung von Personen-daten unrechtmässig macht. Das Bundesgericht hat sich zu dieser Frage bisher nicht geäussert.»[602]

405 Mit diesem Passus hat das Bundesverwaltungsgericht das Rechtmässigkeitsprinzip strikt und m. E. nicht überzeugend resp. unnötig zurückgebunden: Lediglich die Verletzung von Rechtsnormen, welche dem persönlichkeitsrechtlichen Subjektschutz dienen, sollen in eine datenschutzrechtliche Unrechtmässigkeit münden.[603]

406 Unklar ist sodann spezifisch die Relation zwischen Rechtmässigkeit, Unrechtmässigkeit resp. Widerrechtlichkeit. Die Passagen zum Rechtmässigkeitsprinzip und dessen Konkretisierung zeichnen im Verbund gelesen ein diffuses Bild:

> «Eine rechtswidrige Datenbeschaffung durch Private oder Bundesorgane ist immer dann gegeben, wenn ein Verstoss gegen Normen des StGB vorliegt […].»[604]

407 Anders dagegen:

> «Ein rechtswidriges Verhalten liegt dabei immer schon dann vor, wenn die Bearbeitung der Daten gegen eine in der Schweiz geltende rechtlich verbindliche Norm verstösst.»[605]

408 Und eine weitere inhaltliche Variante verleiht der EDÖB dem datenschutzrechtlichen Rechtmässigkeitsprinzip mit den teilweise missverständlichen Worten:

> «Die Bearbeitung von Personendaten darf nur rechtmässig erfolgen. Das heisst, es wird ein Rechtfertigungsgrund benötigt, entweder in Form einer Einwilligung der betroffenen Person, eines überwiegenden öffentlichen oder privaten Interesses oder eines Gesetzes.

601 «Gehalt und Umfang des Rechtmässigkeitsprinzips gemäss Art. 4 Abs. 1 DSG sind umstritten», vgl. BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.1.
602 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.2.
603 Die entsprechende Auslegung ist dem subjektivrechtlich verhafteten Datenschutzkonzept geschuldet. Sie exkludiert das Konzept eines datenschutzrechtlichen Systemschutzes.
604 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6.
605 So Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.62.

> So ist die Bearbeitung von Daten, die ein Fernmeldedienstanbieter für den Verbindungsaufbau und die Rechnungsstellung benötigt, gesetzlich abgedeckt. Falls dieser jedoch weitere Datenbearbeitungen vornehmen möchte, z. B. zum Aufbau eines Kundentreueprogramms, so braucht er dazu die vorgängige Einwilligung des Kunden.»[606]

409 Regelmässig wird eine persönlichkeitsverletzende Datenverarbeitung angenommen, wenn mit ihr *gegen eine Norm der Schweizer Rechtsordnung verstossen wird*.[607] Dass eine solche rechtfertigbar ist, scheinen die zitierten Passagen m. E. fälschlicherweise auszuschliessen.

410 Umstritten ist, ob eine Datenbearbeitung lediglich dann eine «Persönlichkeitsverletzung gemäss Art. 4 Abs. 1 DSG begründet» (will meinen: i. V. m. Art. 12 DSG), sofern sie auf einem diese erst ermöglichenden oder umsetzenden Verhalten beruht, das unabhängig vom DSG widerrechtlich ist,[608] oder ob auch Verstösse gegen die Vorgaben des *Datenschutzgesetzes selbst verpönt sind* und entsprechend unter Art. 4 Abs. 1 DSG zu subsumieren sind.[609]

411 Dass sich die Verletzung des Rechtmässigkeitsgrundsatzes auf Verstösse gegen Normen *ausserhalb* des Datenschutzgesetzes beschränke, versuchen einige Autoren mit einer Probe aufs Exempel zu erhärten: Wäre beispielsweise die Nichtbeachtung der Registerpflicht gem. Art. 11a DSG ein Fall von Art. 4 Abs. 1 DSG, würde die Nichtanmeldung automatisch eine Persönlichkeitsverletzung aller Personen, die in der Datensammlung aufgeführt werden, begründen. Ebendies, so Rosenthal, könne «niemand ernsthaft behaupten wollen».[610] Im Rahmen des Rechtmässigkeitsprinzips wird somit primär die Konformität von *Datenverarbeitungen mit Normen ausserhalb des DSG* eingefordert.[611]

412 Als Rechtsnormen, deren Nichteinhaltung eine Verletzung des Rechtmässigkeitsgrundsatzes begründet, kommen nicht nur zahlreiche Normen aus dem *Strafgesetz* in Betracht, beispielsweise die Berufsgeheimnisse, sondern auch – im Zusammenhang mit der kommerziellen Datenbearbeitung – Art. 27 ff. ZGB und Art. 3 UWG.[612] Als *unrechtmässig* im Sinne von Art. 4 Abs. 1 DSG gilt indes eine Datenbearbeitung bloss, wenn der Verstoss gegen eine Norm der Schweizer Rechtsordnung *ausserhalb des DSG* liegt und dieser nicht aufgrund einer vorrangigen Gegennorm erlaubt sei.[613]

606 Vgl. hierzu den EDÖB, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/telekommunikation/telefonie/allgemeine-grundsaetze.html> (zuletzt besucht am 30. April 2021).
607 Rosenthal, HK-DSG, Art. 4 N 6 f.; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 5 f.; Rampini, BSK-DSG, Art. 12 N 9.
608 So Ders., a. a. O., Art. 4 N 9 f.
609 In diesem Sinne Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6.
610 Rosenthal, HK-DSG, Art. 4 N 11 f.
611 Vgl. Meier, N 640.
612 Vgl. Ders., N 641; vgl. auch Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6.
613 Rosenthal, HK-DSG, Art. 4 N 11 f.

413 Wenn Personendatenverarbeitungen im Einklang mit der gesamten Rechtsordnung zu stehen haben, sind sodann für das Privatrecht ZGB und OR zu beachten. Für das OR hat der Datenschutz im Arbeitsverhältnis besondere Bedeutung erlangt, vgl. Art. 328b OR.[614] Für das ZGB ist das Familienrecht spezifisch erwähnenswert, das für den Kontext der Familie mehrere Normierungen zum Umgang mit personenbezogenen Angaben vorsieht, namentlich im Zusammenhang mit Rechten auf Kenntnis der genetischen Elternschaft resp. Vaterschaft.[615] Eine besondere Auseinandersetzung fand die Frage nach Informationsansprüchen im Adoptionskontext.[616]

414 Die Landschaft einschlägiger Datenschutznormen wird sodann vervollständigt durch zahlreiche *bereichsspezifische Spezialgesetze*, die als Kernthema oder als Teilthema den Datenschutz normieren. Zu nennen sind das Humanforschungsgesetz, vgl. Art. 3 lit. f, lit. h und lit. i sowie Art. 17, Art. 18 Abs. 3 und Art. 32 f. HFG, das Fernmeldegesetz, das Bankengesetz mit Art. 47 BankG. Vor diesem Hintergrund vermag das jüngste Diktum des Bundesverwaltungsgerichts, wonach es unter dem Rechtmässigkeitsprinzip um die Verletzung von Rechtsnormen geht, die dem Schutz der Persönlichkeit dienen würden, nicht zu überzeugen.

415 Trotz Interpretationsdivergenzen lässt sich folgern, dass dem Rechtmässigkeitsprinzip nach DSG eine *Brücken-, Integrations- oder Koppelungsfunktion* zukommt. Es könnte auch als *Drehkreuz* beschrieben werden. In Bezug auf diese Brücken- oder Koppelungsfunktion lassen sich *drei Richtungen* beschreiben. Mit diesen wird deutlich, dass über den Grundsatz datenschutzrechtliche *Präzisierungen und Ausdifferenzierungen* vorgenommen werden.

416 Erstens verbindet das Rechtmässigkeitsprinzip gemäss DSG das *Datenschutzgesetz mit der weiteren Rechtsordnung*. Es geht um die Einbettung des DSG in die gesamte Rechtsordnung resp. die Integration von Normen ausserhalb des DSG in dieses (Koppelungsfunktion nach «aussen»). Eine ähnliche Mechanik ist aufgrund von Art. 7 ZGB bekannt, nach welchem bestimmte Normen des OR ebenso für die zivilrechtlichen Verhältnisse als anwendbar gelten. Dieses zunächst unauffällige Element *vervollständigt das Bild der datenschutzrechtlichen Landschaft*. Es zeigt sich, dass die datenschutzrechtliche Regulierung der Schweiz, trotz des DSG als «Querschnittsgesetz», hoch ausdifferenziert ist. Zwar hat sich die Schweiz mit ihrem DSG – wie die EU mit der DSGVO – für einen «Omnibus»-Ansatz entschieden, wohingegen die USA im privaten Bereich einen sektori-

614 Vgl. insofern die einschlägige Kommentarliteratur. Spezifisch und grundlegend zum Verhältnis und zur Problematik des Datenaustausches zwischen Arbeitgeber und Versicherung Pärli, 1 ff.; Wildhaber, Jusletter vom 6. Dezember 2010.

615 Zum Recht des Ehemannes auf Kenntnis seiner genetischen Vaterschaft ausserhalb des Anfechtungsprozesses Entscheid der 3. Abteilung des Obergerichts des Kantons Luzern (Oger LU) vom 18. September 2012, FamPra.ch 2013, 220; hierzu Pfaffinger, FamPra.ch 2014, 604 ff.

616 Vgl. Art. 286b f. ZGB; vertiefend Dies., *passim*.

ellen Ansatz vorsehen.[617] Das DSG als «Querschnittsgesetz» unterstellt Verarbeitungen von Personendaten durch die Bundesbehörden wie durch Private einer allgemeinen Datenschutznormierung. Allerdings differenziert die Schweiz, wie im IV. Kapitel dieses zweiten Teils herausgearbeitet wurde, innerhalb dieses Querschnittsgesetzes pointiert zwischen dem öffentlichen und privaten Bereich. Spezialgesetzgebungen bringen eine zusätzliche Ausdifferenzierung des datenschutzrechtlichen Regimes mit sich. Damit wird offensichtlich anerkannt, dass *diverse gesellschaftliche Bereiche resp. Kontexte*, wie beispielsweise der Humanforschungsbereich, der Telekommunikationssektor, der Bankensektor, der Arbeitsbereich oder der Bereich der Familie, (zumindest punktuell) datenschutzrechtlich differenziert zu behandeln sind. Entsprechend ist die *Kontextrelevanz* für die datenschutzrechtliche Regulierung selbst in Ländern, die sich für einen «Omnibus»-Ansatz entschieden haben, erstellt.[618] Aus dem Befund, wonach über das datenschutzgesetzliche Rechtmässigkeitsgebot Normen in Spezialerlassen für besondere Verarbeitungskontexte adressiert werden, ergibt sich, dass die Schweiz, trotz der Entscheidung für ein «Querschnittsgesetz», *einen kontextuellen Ansatz* kennt. Ein kontextueller Ansatz, der über den Dualismus von öffentlich und privat gemäss DSG hinausgeht. Diese Charakterisierung des Rechtmässigkeitsprinzips in seiner Koppelungsfunktion wird jüngst eindrücklich bestätigt im Helsana+-Urteil des Bundesverwaltungsgerichts, selbst wenn seine Argumentation stark im Persönlichkeitsparadigma verhaftet bleibt.[619]

In den Erwägungen zum Rechtmässigkeitsprinzip gemäss DSG stehen indes *weniger Integrations- als vielmehr Abgrenzungsthemen* im Vordergrund, die im Lichte der Gesetzeshistorie nachvollziehbar werden. So bereitet insb. die Abgrenzung zum Zweckbindungsgrundsatz Schwierigkeiten. Zudem münden Konkretisierungsversuche nicht selten in eine Vermengung mit dem Verarbeitungsgrundsatz von Treu und Glauben oder in die Aussage, dass den beiden Grundsätzen kein materieller Unterschied eigen sei.[620] Die Abgrenzungsthematik ist nicht neu, wurde doch in den 1980er Jahren eine vereinte Regelung geplant:[621] So lautete ein ursprünglicher Vorschlag für einen Art. 4 Abs. 1: «Personendaten dürfen nur *mit rechtmässigen Mitteln und nicht wider Treu und Glauben* [Hervorhebung durch die Autorin] beschafft werden».[622] In Kraft trat 1992 ein Art. 4 Abs. 1 DSG mit 417

617 Nissenbaum, 235.

618 wegweisend zu diesem zentralen Konzept für Privacy-Belange Nissenbaum, *passim*; in Europa weniger offensichtlich als in den USA mit seinem sektorspezifischen Ansatz für den privaten Bereich.

619 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018; zum Urteil s. auch Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f.; Vasella/Ziegler, digma 2019, 80 ff.; kritisch zur verordneten Selbstverantwortung Pärli, SZS 2018, 107 ff.

620 Vgl. Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 5; Pedrazzini, Grundlagen, 26; Meier, N 641 sieht in der Beschaffung von Daten zu Marketingzwecken unter der falschen Angabe, dass die Erhebung zu Forschungs- oder Statistikzwecken erfolgt, einen Verstoss gegen Art. 4 Abs. 1 DSG.

621 Vgl. Steinauer, in: Schweizer (Hrsg.), 43 ff., 45.

622 Vgl. BBl 1988 II 414 ff., 460 und 517.

dem Wortlaut: «Personendaten dürfen nur rechtmässig beschafft werden». Man separierte in einem *ersten Schritt* den Bearbeitungsgrundsatz der Rechtmässigkeit von Treu und Glauben; letzterer wurde in einen Abs. 2 ausgelagert. Der so verselbstständigte Rechtmässigkeitsgrundsatz fokussierte eingrenzend auf die Personendaten*beschaffung*. Es folgte *in einem zweiten Schritt* mit der Teilrevision von 2003 eine Ausdehnung des Rechtmässigkeitsgebotes, wobei die bis heute in Kraft stehende Version von Art. 4 Abs. 1 DSG lautet: «Personendaten dürfen nur rechtmässig bearbeitet werden.»

418 Gesetzlich wird folglich die Einschlägigkeit des Rechtmässigkeitsprinzips *für den gesamten Verarbeitungszyklus* von Personendaten verbürgt.[623] In der Lehre gilt gleichwohl die unrechtmässige Beschaffung und hierbei namentlich diejenige *durch unrechtmässige Mittel wie Drohung, Diebstahl, Arglist und Täuschung, Zwang* als paradigmatisch für eine Verletzung des Rechtmässigkeitsgebotes gemäss Art. 4 Abs. 1 DSG.[624]

419 Art. 4 Abs. 1 DSG resp. nach Totalrevision Art. 6 Abs. 1 nDSG sieht ein *umfassendes Rechtmässigkeitsgebot für die Bearbeitung von Daten auf jeder Prozessstufe vor*, was internationalen Vorgaben entspricht. Dennoch steht die Rechtmässigkeit hinsichtlich der Beschaffung von Personendaten im Vordergrund. Der Grundsatz richtet sich, wenn auch nicht ausschliesslich, auf die «*Eintrittskontrolle*». Dass der rechtmässigen Erhebung besondere Relevanz zugemessen wird, ist in Anbetracht der Tatsache angemessen, wonach einmal erhobene Personendaten kaum mehr aus dem «Informationskreislauf» eliminiert werden können. Speichermöglichkeiten und Weiterverarbeitungen sind technisch nahezu unbeschränkt möglich und Löschungen stellen heute in der Realität eine grosse Herausforderung dar. Wird also dem «initialen» Eintritt von Personendaten in Bearbeitungsprozesse – der Erhebung – auch in der Schweiz über das Rechtmässigkeitsgebot erhöhte Aufmerksamkeit geschenkt, bleibt man damit dennoch – zumindest formell betrachtet – weit von Systemen entfernt, die einen Grundsatz der *Direkterhebung* anerkennen.[625]

420 Mit der Akzentuierung der Rechtmässigkeit auf den Zeitpunkt der Personendaten*erhebung* wird man auf den Grundsatzentscheid für einen Ausgangspunkt der Datenschutzgesetzgebung zurückgeführt und sieht sich mit dieser Korrelation

623 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 5.
624 Vgl. Meier, N 369 f.
625 So Deutschland in § 4 Abs. 2 BDSG vor den Anpassungen des Gesetzes an die Vorgaben der DSGVO. Die DSGVO verankert kein Direkterhebungsgebot, womit die Entwicklungen in diesem Bereich in den Mitgliedstaaten der EU, welche aufgrund der Öffnungsklauseln Regelungsräume haben und diese durch Ausführungsgesetzgebungen nutzen, offen sind; vgl. auch <https://www.cr-online.de/blog/2016/05/04/dsgvo-was-wird-aus-dem-grundsatz-der-direkterhebung/> (zuletzt besucht am 30. April 2021).

konfrontiert. Auch in diesem Zusammenhang findet das Rechtmässigkeitsprinzip verschiedene Bedeutungsgehalte.

421 Somit ist auf eine *zweite*, etwas anders gelagerte *Koppelungs- und Koordinationsmechanik* des Rechtmässigkeitsprinzips einzugehen: diejenige «nach innen» im Sinne der Referenz auf den datenschutzgesetzlichen Ausgangspunkt der Personendatenverarbeitung. In Systemen mit prinzipiellem Verarbeitungsverbot sind Personendatenverarbeitungen erst und nur dann rechtmässig, wenn sie von einem Erlaubnistatbestand gedeckt werden, vgl. Art. 6 i. V. m. Art. 5 Abs. 1 lit. a DSGVO.[626] Die Unrechtmässigkeit jeglichen Umgangs mit Personendaten ist die gesetzlich angenommene Regel, es sei denn, es liegt ein Erlaubnistatbestand vor. Das Vorliegen eines Erlaubnistatbestandes ist folglich vorrangige Bedingung für eine rechtmässige Personendatenverarbeitung. Gründet der Privatsektor der Schweiz datenschutzrechtlich in der Basisannahme der «Rechtmässigkeit» der Verarbeitung, wird die Ausnahme – die *Unrechtmässigkeit* – zum eigentlichen Bezugspunkt. Eine Hauptherausforderung im Umgang mit dem Rechtmässigkeitsprinzip im privaten Bereich liegt in der Koordinierung des Begriffs der «Rechtmässigkeit» der Datenbearbeitung i. S. v. Art. 4 Abs. 1 DSG mit der persönlichkeitsverletzenden Datenbearbeitung, Art. 12 f. DSG, neu vgl. Art. 30 f. und Art. 6 Abs. 1 nDSG. Die unrechtmässige Datenverarbeitung ist grundsätzlich widerrechtlich, es sei denn, es liegen Rechtfertigungsgründe vor.[627] Es fragt sich: Bedeutet ein Verstoss gegen das Rechtmässigkeitsgebot i. S. v. Art. 4 Abs. 1 DSG per se eine widerrechtliche Persönlichkeitsverletzung, womit also die Rechtfertigung ausgeschlossen würde? Ist der Begriff «unrechtmässig» i. S. v. Art. 4 Abs. 1 DSG gleichzusetzen mit demjenigen der Widerrechtlichkeit i. S. v. Art. 12 f. DSG? Wie lassen sich «Rechtmässigkeit», «Unrechtmässigkeit» resp. «Widerrechtlichkeit» verstehen und koordinieren? Offenkundig lässt sich das Rechtmässigkeitsprinzip harmonischer in das System des öffentlichen Bereiches als in dasjenige des privaten Bereichs einfügen.

422 In Bezug auf den *Dualismus* zeigt sich das Rechtmässigkeitsprinzip als *Drehkreuz*, das unterschiedliche Ausrichtungen erhält, je nachdem, für welchen Bereich – den öffentlichen oder den privaten – man an dieses herantritt. Die Rechtmässigkeit einer Datenbearbeitung im *öffentlichen Bereich* setzt entsprechend dem Legalitätsprinzip eine rechtliche Grundlage ausserhalb des DSG voraus, Art. 4 Abs. 1 i. V. m. Art. 17 DSG, nach Totalrevision Art. 34 i. V. m. Art. 6 Abs. 1 nDSG. Die fehlende gesetzliche Grundlage gemäss Art. 17 DSG gilt als

626 Vgl. § 4 Abs. 1 BDSG; Art. 6 Abs. 1 DSGVO; zur humoristischen «Verarbeitung» der DSGVO/GDPR mit den GDPRTOONS und den Cartoon von Dreyer, abrufbar unter: <http://www.gdprtoons.com> (zuletzt besucht am 30. April 2021).

627 Illustrativ hierfür Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6 f.

klassisches Beispiel für einen Verstoss gegen Art. 4 Abs. 1 DSG.[628] Hingegen ist die rechtmässige Datenbearbeitung im *privaten Bereich* eine, die nicht widerrechtlich das Persönlichkeitsrecht verletzt, Art. 4 Abs. 1 i. V. m. Art. 12 f. DSG resp. Art. 6 Abs. 1 i. V. m. Art. 30 f. nDSG. Die Aussage in der Botschaft zur Verabschiedung eines ersten Datenschutzgesetzes, wonach die allgemeinen Bearbeitungsgrundsätze als «gemeinsames datenschutzrechtliches Fundament» für den öffentlichen und den privaten Bereich gelten, bedarf damit der *Präzisierung: Der Rechtmässigkeitsgrundsatz entfaltet sich unterschiedlich für den privatrechtlichen und den öffentlich-rechtlichen Datenschutz der Schweiz, weil er divergierend eingebettet ist*. Seine prominenteste Anknüpfung hat das Rechtmässigkeitsprinzip seit jeher im öffentlich-rechtlichen Legalitätsprinzip mit der Funktion, staatliches Handeln zu legitimieren. Hier verlangt das Legalitätsprinzip, staatliches Handeln an das Recht zu binden («Verboten ist, was nicht erlaubt ist»). Für den privaten Bereich ist die Rechtmässigkeit die implizite Basisannahme. Es sind die Schranken, deren Durchbrechung Datenverarbeitungen zu unrechtmässigen Datenverarbeitungen machen und damit zu einer Persönlichkeitsverletzung führen, die mangels Rechtfertigungsgrund auch widerrechtlich ist.

423 An dieser Stelle kann im Sinne eines *Zwischenergebnisses* festgehalten werden, dass dem Rechtmässigkeitsprinzip eine *Koppelungsfunktion* in *zweierlei Richtungen* zukommt: Zum einen erfolgt über dieses die *Inklusion von Normen ausserhalb des DSG* in das allgemeine Datenschutzregime, zum anderen dient es der Anknüpfung an die innerhalb des DSG gewählten, entgegengesetzten Ausgangspunkte für den öffentlichen und privaten Sektor. Über das Rechtmässigkeitsprinzip wird der jeweils in einem Datenschutzsystem gewählte *Ausgangspunkt* – Verarbeitungsverbot mit Erlaubnistatbeständen oder Grundsatz der Freiheit der Datenverarbeitung mit Schranken – *angekoppelt*. Mit Blick auf den Dualismus zeigt sich das Rechtmässigkeitsprinzip als *Drehkreuz*, das unterschiedliche Ausrichtungen erhält, je nachdem, für welchen Bereich – den öffentlichen oder den privaten – man es liest. Der Rechtmässigkeitsgrundsatz entfaltet sich unterschiedlich für den privatrechtlichen und den öffentlich-rechtlichen Datenschutz der Schweiz, weil er divergierend eingebettet ist.

424 Es verbleibt, *drittens*, eine «Koordinierungsaufgabe», die Koordinierung des *Rechtmässigkeitsprinzips im privaten Bereich* mit dem *privatrechtlichen Persönlichkeitsschutz* und dessen Dogmatik. Die nachfolgenden Erwägungen gehen der Frage nach, wie die Koordinierung des Rechtmässigkeitsprinzips mit dem System des Persönlichkeitsschutzes gemäss Art. 28 ZGB und dem dort verwendeten Begriff der *Widerrechtlichkeit* bewerkstelligt werden kann.[629] Bezüglich der Harmo-

628 So Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6.
629 Hierzu sogleich mehr zweiter Teil, VI. Kapitel, B., insb. 2.–4.

nisierung der Figuren der «Rechtmässigkeit» resp. «Unrechtmässigkeit» sowie der «Widerrechtlichkeit» werden verschiedene Meinungen präsentiert.

425 Vertreten wird, dass vorab ein Verstoss gegen eine Rechtsnorm (ausserhalb des DSG) die Verletzung des Rechtmässigkeitsgebots i. S. v. Art. 4 Abs. 1 DSG begründet. Eine so erstellte Unrechtmässigkeit gemäss Art. 4 Abs. 1 DSG begründet eine Persönlichkeitsverletzung, vgl. Art. 12 Abs. 2 lit. a DSG, womit das Vorliegen eines Rechtfertigungsgrundes zu prüfen ist.[630]

426 Anders die Argumentation des EDÖB im Fall Logistep, der zum Bundesgerichtsentscheid BGE 136 II 508 führte. Die Frage der Rechtmässigkeit wird auf die Frage der Widerrechtlichkeit einer Persönlichkeitsverletzung ausgerichtet. Der EDÖB monierte einen Verstoss gegen das Rechtmässigkeitsprinzip und hielt dem Bundesverwaltungsgericht vor, «Art. 12 Abs. 2 lit. a DSG falsch ausgelegt zu haben».[631] Die aktuelle Bestimmung schliesse seiner Meinung nach Rechtfertigungsgründe aus. Stattdessen müsse geprüft werden, ob ein Grundsatz der Datenbearbeitung verletzt worden sei. Dies erfordere eine Verhältnismässigkeitsprüfung, welche die bestehenden Rechtfertigungsgründe mitberücksichtige. Das Bundesverwaltungsgericht habe die dabei notwendige Interessenabwägung fehlerhaft vorgenommen, denn es bestünden keine überwiegenden privaten oder öffentlichen Interessen. Die Persönlichkeit der betroffenen Personen sei somit widerrechtlich verletzt worden. Indem die Vorinstanz dies verkannt habe, habe sie auch gegen das in Art. 4 Abs. 1 DSG verankerte *Legalitätsprinzip* verstossen.[632] Das Bundesgericht dagegen hielt dafür, dass eine Rechtfertigung ebenso im Rahmen von Art. 12 Abs. 2 lit. a DSG denkbar sei.

427 Die heute wohl herrschende Lehre und Rechtsprechung vertritt die Ansicht, dass auch ein Verstoss gegen die allgemeinen Verarbeitungsgrundsätze, wie sie in Art. 4 DSG und in Art. 12 Abs. 2 lit. a DSG formuliert werden, einer Rechtfertigung zugänglich sind. Allerdings dürfe dies nur mit Zurückhaltung angenommen werden.[633] Die Frage nach dem Rechtmässigkeitsprinzip und der Widerrechtlichkeit im privaten Bereich ist damit indes noch nicht spezifisch beantwortet. Im Zentrum steht die Frage, welche Verstösse gegen Vorgaben innerhalb des DSG als «Verstoss gegen das Rechtmässigkeitsprinzip» zu qualifizieren sind. Sie stellt sich nicht nur aufgrund der Tatsache, dass das Rechtmässigkeitsprinzip dem Grundsatz nach selbst unbeschränkt auf das Normgefüge eines Regelungsregimes verweist. Hieraus würde für das Datenschutzrecht im privaten Sektor folgen,

630 So Rosenthal, HK-DSG, Art. 4 N 7 ff.; vgl. insofern neu Art. 6 Abs. 1 i. V. m. Art. 30 Abs. 2 lit. a nDSG.
631 BGE 136 II 508, E 2.1.
632 BGE 136 II 508, E 2.1.
633 Mit Hinweis auf BGE 136 II 508, E 5.2.4.; Hussein, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.126; Rosenthal, HK-DSG, Art. 12 N 16 ff.; mit Hinweis des Auslegungshinweises des BJ Rampini, BSK-DSG, Art. 12 N 9b.

dass Verstösse gegen bestimmte Datenschutzvorgaben, die nicht explizit von Art. 12 DSG als persönlichkeitsverletzend taxiert werden, über das Rechtmässigkeitsprinzip und damit Art. 12 Abs. 2 lit. a DSG in den persönlichkeitsverletzenden Bereich fallen. Eine weite Auslegung wird mit dem Ingress von Art. 12 Abs. 2 DSG eröffnet, indem er die durch Datenverarbeitungen erfolgenden persönlichkeitsverletzenden Tatbestände *enumerativ* aufführt. Zwar liesse sich mit Fug und Recht anführen, dass ein Umweg über das Rechtmässigkeitsgebot überflüssig ist. Je grosszügiger man Verstösse gegen Vorgaben des Datenschutzgesetzes direkt oder über das Rechtmässigkeitsprinzip in die Persönlichkeitsverletzung inkludiert, desto höher wird das Datenschutzniveau.

428 Was aber ist von der engen Auslegung zu halten, wonach einzig Verstösse gegen Normen ausserhalb des DSG zur Verletzung des Rechtmässigkeitsprinzips führen, namentlich wenn diese den Individualrechtsschutz garantieren?[634] Rosenthal ist durchaus beizupflichten, wenn er eine Interpretation, die nicht nur Verstösse gegen bestimmte Vorgaben *ausserhalb* des DSG, sondern auch eine Interpretation, die *Verstösse gegen Vorgaben innerhalb des DSG* in den Rechtmässigkeitsgrundsatz inkludiert, im Lichte des Konzeptes des DSG problematisiert.[635]

429 Die unterschiedlichen Auslegungen – Inklusion oder Exklusion von Verstössen gegen weitere Vorgaben des Datenschutzgesetzes in das Rechtmässigkeitsgebot – beeinflussen das Datenschutzniveau im privaten Sektor: Werden Verstösse gegen datenschutzgesetzlich «interne» Regeln unter den Tatbestand von Art. 4 Abs. 1 DSG subsumiert, führt dies zum Ausbau der individualrechtlichen Position gemäss Art. 12 i. V. m. Art. 4 Abs. 1 DSG. Das Datensubjekt könnte konsequent Verstösse gegen datenschutzgesetzliche Vorgaben als Persönlichkeitsverletzung rügen, weil diese als Verstoss gegen das Rechtmässigkeitsprinzip über Art. 12 Abs. 2 lit. a DSG in die Annahme einer Persönlichkeitsverletzung münden würden. Auf Art. 11a DSG exemplarisch angewendet hiesse dies, dass die Nichtanmeldung einer Datensammlung als Verstoss gegen das Datenschutzgesetz vom Betroffenen über Art. 12 Abs. 1 i. V. m. Art. 4 Abs. 1 DSG gerügt werden könnte, dem Individuum mithin ein zivilrechtlicher Anspruch zukäme. Den Verstoss gegen die Registrierung über das Rechtmässigkeitsprinzip in den zivilrechtlichen Persönlichkeitsschutz einfliessen zu lassen, erscheint gut begründbar, zumal Betroffene von Gesetzes wegen ein Recht auf Auskunft gegenüber dem Betreiber einer Datensammlung haben, ob sie in dieser aufgeführt werden. Die Registrierung ist nahezu *conditio sine qua non* zur Realisierung der Betroffenenrechte. Verstösst der Betreiber einer Datensammlung gegen die Anmeldungspflicht, erschwert er zugleich das Recht der Betroffenen, eine entsprechende Auskunft zu

634 Rosenthal, HK-DSG, Art. 12 N 7; jüngst BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.

635 Ders., a. a. O., Art. 12 N 7 und N 11.

erhalten. So wird in doppelter Hinsicht gegen den Anspruch auf Transparenz verstossen, der eine tragende Säule datenschutzrechtlicher Normierungen ist: Weder die Kenntnis um die Existenz der Sammlung an sich noch die Kenntnis um die Erfassung des Individuums in der Sammlung wird gewährleistet. Folglich liesse sich vertreten, dass eine Verletzung der Anmeldepflicht gemäss Art. 11a DSG über Art. 12 Abs. 2 lit. a i. V. m. Art. 4 Abs. 1 DSG zu erfassen ist, womit ein zivilrechtlicher Anspruch des Individuums begründbar wird. Eine solche Interpretation des noch geltenden Rechts stünde in Einklang mit den jüngsten Rechtsentwicklungen. Zwar entfällt mit Totalrevision die Registrierungspflicht. Allerdings greift eine allgemeine Informationspflicht sowie eine Pflicht zur Erstellung eines Verarbeitungsverzeichnisses. Diese Pflichten bilden die Grundlage für die sowohl mit der DSGVO als auch mit der Totalrevision einhergehende Stärkung der Individualrechte, namentlich auch des Auskunftsrechts. Um Auskunftsrechte wirksam gewährleisten zu können, ist eine systematische Organisation der Informationen erforderlich.

Die hier vertretene Auslegung stärkt die *Transparenz*, was dem *Trend der jüngsten datenschutzrechtlichen Entwicklungen* entspricht.[636] In Anbetracht der Tatsache, dass die Registrierung von Datensammlungen ein Schlüsselelement für die Ausübung der Betroffenenrechte darstellt, scheint eine andere Auslegung, als dass deren Verletzung über den Rechtmässigkeitsgrundsatz oder direkt als Persönlichkeitsverletzung zu qualifizieren ist, nicht überzeugend.[637] Die Diskussion verliert mit der Totalrevision allerdings ihre Bedeutung. 430

Anzufügen bleibt, dass Verstösse gegen datenschutzgesetzliche Vorgaben, die nicht explizit in Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG aufgeführt werden, bereits aufgrund des nicht abschliessend formulierten Tatbestandes als persönlichkeitsverletzende Verarbeitungen qualifiziert werden können. Welche dies sind, bedarf der wertenden Auslegung. Der Umweg über das Rechtmässigkeitsprinzip wäre folglich überflüssig. Damit bestätigt sich, dass die *Kernbedeutung des Rechtmässigkeitsprinzips für den privaten Bereich* – anders als im öffentlichen Bereich – in der Vorgabe besteht, wonach auch *einschlägige Normen ausserhalb des DSG einzuhalten* sind. 431

636 Vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff., 6943 und 6972.

637 Man mag nun einwenden, dass ein Umweg über das Rechtmässigkeitsgebot und dessen Verletzung überflüssig wäre, könnte man doch den Verstoss gegen weitere datenschutzrechtliche Verstösse direkt über das «insbesondere» in Art. 12 Abs. 2 DSG einfliessen lassen; die Abstützung über Art. 4 Abs. 1 DSG wäre hierfür nicht erforderlich. Die Diskussion mag somit als überflüssig resp. sinnfrei erscheinen. Dennoch verdeutlicht die Inklusion von Verletzung weiterer datenschutzrechtlicher Pflichten und Vorgaben in das Rechtmässigkeitsprinzip die Geltungskraft datenschutzrechtlicher Regelung. Namentlich die datenschutzrechtlichen Vorgaben, die im Kontext mit der Absicherung des Transparenzgebotes verankert werden und dieses quasi flankieren, fliessen damit sichtbar in ihrer Gewichtung in die allgemeinen Bearbeitungsvorgaben ein.

432 In Erinnerung zu rufen bleibt, dass der Helsana+-Entscheid des Bundesverwaltungsgerichts eine *enge Auslegung zum Rechtmässigkeitsgebot* vertrat:[638] Das Gericht prüfte, ob die Datenbearbeitung der Beklagten im Rahmen des Programmes Helsana+, soweit es Personen betreffe, die nur eine Grundversicherung bei einer Versicherungsgesellschaft der Helsana-Gruppe haben, grundsätzlich unrechtmässig i. S. v. Art. 4 Abs. 1 DSG sei, da sie zu einem rechtswidrigen Zweck erfolge, nämlich eine indirekte Rückerstattung von Versicherungsprämien für die obligatorische Krankenversicherung ermögliche. Hierzu führte das Bundesverwaltungsgericht aus, dass Inhalt und Umfang des Rechtmässigkeitsgebotes nach Art. 4 Abs. 1 DSG umstritten seien. Unbestritten sei, dass Datenbearbeitungen immer dann unrechtmässig seien, wenn gegen eine Rechtsnorm verstossen werde, die den Schutz der Persönlichkeit bezwecke, unabhängig davon, ob sich die Rechtsnorm im DSG oder anderen Erlassen finde.[639] Ein Teil der Lehre beurteile eine Datenbearbeitung immer dann als unrechtmässig, wenn ein Verstoss gegen irgendeine Rechtsnorm vorliege.[640] Ein anderer Teil der Lehre will nur Verstösse gegen solche Verhaltensnormen, die direkt oder indirekt auch den Schutz vor einem Eingriff in die Persönlichkeit bezwecken, unter den Tatbestand subsumieren.[641] Niemand vertrete explizit, dass ein rechtswidriger Zweck der Datenbearbeitung in jedem Fall zur Unrechtmässigkeit der fraglichen Datenbearbeitung führe; alle Lehrmeinungen stellten vielmehr darauf ab, dass die Datenbearbeitung an sich gegen keine Rechtsnorm verstossen dürfe. Art. 4 Abs. 1 DSG beziehe sich, so führt das Bundesverwaltungsgericht fort, im Wortlaut auf die Rechtmässigkeit der Bearbeitung.[642]

433 Nach Ansicht der Autorin wird mit dieser Rechtsprechung der Aspekt der *Akzessorietät datenschutzrechtlicher Vorgaben, ein Terminus, wie er im historischen Teil entwickelt wurde,* übersehen.[643] Das DSG, so fährt das Gericht fort, äussere sich nicht dazu, zu welchen Zwecken Personendaten erhoben werden dürfen.[644] Es verlange nur, dass der Verarbeitungszweck bei der Beschaffung nach den Umständen erkennbar sei, dabei auch auf die Zweckbindung verwiesen werde. Alsdann findet eine Rechtsvergleichung statt, wobei die Differenz des DSG gegenüber der DSGVO herausgestellt wird: Art. 5 Abs. 1 DSGVO sage, anders als das DSG, dass Personendatenverarbeitungen nur für legitime Zwecke verfolgt wer-

638 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.4.
639 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.2.
640 Die Autorin schliesst sich dieser Auffassung an.
641 Die Auslegung vermag im Lichte der Erkenntnisse dieser Schrift nicht zu überzeugen, muss doch als ratio und Ziel und Zweck des Datenschutzrechts auch der Schutz von bereichsspezifisch definierten Schutzzwecken und Zielen sein.
642 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.3.
643 Erster Teil, I. Kapitel.
644 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.3., was kritisch beurteilt wurde. Zudem ist im Versicherungskontext auf die Spezialgesetze hinzuweisen, welche die systemische Schutzdimension des Datenschutzrechts dokumentieren und erfüllen.

den dürfen.[645] Mit der Totalrevision des DSG plane man indes keine Anpassung. Zudem führe eine teleologische Betrachtung von Art. 4 Abs. 1 DSG zu dem Schluss, dass das DSG dem Schutz der Persönlichkeit diene. Die allgemeine Zweckrichtung aller Datenschutzvorschriften lege nahe, dass sich das Rechtmässigkeitsprinzip nur darauf beziehe, dass Personendatenverarbeitung gegen Normen verstosse, die dem Schutz der Persönlichkeit dienen. Im Ergebnis hält das Bundesverwaltungsgericht fest, dass der Grundsatz der Rechtmässigkeit gemäss Art. 4 Abs. 1 DSG so zu verstehen sei, dass eine Datenbearbeitung zu einem rechtswidrigen Zweck erst dann unrechtmässig sei, wenn dabei gegen eine Norm verstossen wird, die zumindest auch, direkt oder indirekt, dem Schutz der Persönlichkeit dient.[646]

Eine solche Auslegung greift nach hier vertretener Ansicht zu kurz. Sie bindet das 434
Datenschutzrecht auf den Subjekt- und Persönlichkeitsschutz zurück. Die Vorgabe, dass eine unrechtmässige Datenverarbeitung nur dann vorliege, wenn gegen eine Norm verstossen werde, die dem Persönlichkeitsschutz diene, übersieht die Relevanz des Systemschutzes im Datenschutzrecht.[647]

Zusammenfassend präsentiert sich das Rechtmässigkeitsprinzip im Datenschutz 435
nach der hier vertretenen Ansicht als weit mehr denn ein Instrument der Selbstbeschwörung und -bestätigung des Rechts. Die Analyse des Rechtmässigkeitsprinzips macht es möglich, die Gesamtlandschaft des (Datenschutz-)Rechts wie auch den hohen Ausdifferenzierungsgrad des Schweizer Datenschutzrechts in den Blick zu nehmen. Aus funktionaler Sicht zeigt es namentlich eine *Anknüpfungs- resp. Ankoppelungsfunktion*, die mit einer *Differenzierungsfunktion* einhergeht. Die Qualifizierung des DSG als Querschnittsgesetz ist zwar nicht falsch, sie vermag indes nicht abzubilden, dass sich über das Rechtmässigkeitsprinzip eine *differenzierte und komplexe datenschutzrechtliche Landschaft* erschliesst. Drei Richtungen wurden insofern systematisiert: *Erstens* diejenige «nach aussen», also die Einbettung des DSG in die gesamte Rechtsordnung resp. Integration von Normen ausserhalb des DSG in dieses, *zweitens* jene «nach innen», also die Referenz auf den datenschutzgesetzlichen Ausgangspunkt der Personendatenverarbeitung (Grundsatz des prinzipiellen Verarbeitungsverbots) und insb. das Legalitätsprinzip resp. die prinzipielle Verarbeitungsfreiheit für den privaten Be-

645 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.3.; m. E. hätte man hier in einer systematischen Interpretation und einer europarechtskompatiblen Auslegung auch in der Schweiz die systemische Datenschutzdimension inkludieren können – vertiefend zu diesem Ansatz dritter Teil, IX. Kapitel.

646 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.3.

647 Eine systemtheoretische Analyse des Datenschutzrechts mit einer präzisierten Darstellung der modernen Systemtheorie und ihrer Kritiker findet sich bei Donos, 21 ff.; die vorliegende Arbeit beschreibt das Recht auf informationellen Systemschutz in erster Linie als Paradigma, welches das Recht auf informationellen Subjektschutz als individualistisches Privatheitsparadigma wenn auch nicht ersetzt, so doch ergänzt.

reich, und *drittens* geht es innerhalb des Datenschutzgesetzes für den privaten Sektor um dessen Koordinierung mit dem persönlichkeitsrechtlichen System und den Kategorien der Persönlichkeitsverletzung, der Widerrechtlichkeit sowie der Rechtfertigungsgründe. Folglich greift es zu kurz, den Ansatz des Schweizer Datenschutzrechts isoliert anhand des DSG als «Omnibus»-Ansatz zu qualifizieren. Mit und über das Rechtmässigkeitsprinzip wird in der Schweiz ein *differenziertes und abgestuftes Datenschutzregime abgebildet und implementiert, das sich harmonisch in die gesamte Rechtsordnung mit ihren für die jeweiligen Bereiche etablierten Leitprinzipien einfügt*.

2. Treu und Glauben

2.1. Grundlagen

436 Getreu der Redewendung «Nützt es nicht, so schadet es auch nicht» liess sich der bei der Schweizer Datenschutzgesetzgebung federführende Pedrazzini mit den Worten vernehmen: «Treu und Glauben sei immer recht am Platze».[648] Etwas anders gestaltet sich die Einschätzung von Druey, demzufolge Treu und Glauben für das Informationsrecht eine ungleich höhere Bedeutung zukomme als für andere Gebiete.[649] Die Zitate zweier Schweizer Experten für den Bereich des Informationsrechts liefern im Verbund ein ambivalentes Bild zur Bedeutung des Prinzips im Datenschutzrecht: Für den einen Verlegenheitslösung weist der andere dem Grundsatz dagegen besonderes Gewicht im Informationskontext zu. Die nachfolgenden Ausführungen gehen der Bedeutung von Treu und Glauben für das Datenschutzrecht auf den Grund.[650] Dabei wird eine Erkenntnis, die aus den Erörterungen zum Rechtmässigkeitsprinzip gewonnen wurde, nutzbar gemacht. Demnach vermag namentlich eine systematische und eingebettete Betrachtungsweise produktive Erkenntnisse zu generieren.

437 Treu und Glauben ist fester Bestandteil der allgemeinen datenschutzrechtlichen Verarbeitungsgrundsätze, vgl. Art. 4 Abs. 2 1. Satzteil DSG, vgl. auch Art. 6 Abs. 2 erster Teil nDSG und Art. 5 Abs. 1 lit. a DSGVO. Gerade *weil* die generalklauselartigen Bearbeitungsgrundsätze und damit Treu und Glauben im privaten Sektor gemäss DSG *die wichtigsten Schranken der grundsätzlich freien Bearbeitung definieren*, kommt der Aufgabe, diesen konkretisierte Handlungsanleitungen zu verleihen, besondere Relevanz zu.

---

648 Pedrazzini, in: Schweizer (Hrsg.), 19 ff., 26.
649 Druey, 315.
650 Zu Vertrauen und Glaubwürdigkeit im Zeitalter des Internets Müller, NZZ am Sonntag vom 4. Februar 2018, 20 f.; zu Vertrauen (und Risiko) als zentralen Elementen modernen Zusammenlebens Hotter, 74 ff.; zum Vertrauen durch das Recht Druey, Rechtswissenschaftliche Abteilung der Universität St. Gallen (Hrsg.), 525 ff.

438 Für das Datenschutzrecht prägt die *Abgrenzung* von Treu und Glauben gegenüber anderen Verarbeitungsgrundsätzen die Debatte zum Verarbeitungsgrundsatz: Wie gezeigt, wurde gesetzgeberisch eine vorab geplante gemeinschaftliche Normierung des Gebotes der Rechtmässigkeit mit demjenigen von Treu und Glauben in einem Absatz aufgegeben und Letzteres in eine vereinte Regelung mit dem Verhältnismässigkeitsgrundsatz in einen Absatz transferiert. Diese Systematik wird mit der Totalrevision und Art. 5 Abs. 2 nDSG beibehalten. Die folgenden Reflexionen werden indes den *eigenständigen Gehalt sowie spezifische Funktionen von Treu und Glauben, aber auch Schwächen für das Informations- und namentlich das Datenschutzrecht* vor Augen führen. Hierzu beginnt die Untersuchung mit allgemeineren methodischen Erwägungen zu den Generalklauseln und dem traditionsreichen Grundsatz. Nach dieser Betrachtung von Treu und Glauben auf abstraktester Ebene wird der Fokus verengt auf Treu und Glauben im Datenschutzrecht. Anschliessend wird analysiert, welche Impulse der Grundsatz dem Datenschutzrecht verliehen hat, aber auch, welche Defizite ihm eigen sind.

439 Bedeutsame Themen sind bei der Konkretisierung von Treu und Glauben die *culpa in contrahendo*, die Vertrauenshaftung und damit die Begründung vorvertraglicher Informationspflichten, die Inhaltskontrolle bei AGB sowie der Vertrag mit Schutzwirkung zugunsten Dritter.[651] Zudem kommt Treu und Glauben eine wichtige Funktion bei der *Interpretation* von Gesetzen, Verträgen und allgemeinen Willenserklärungen zu.[652] Entsprechend spielt *Treu und Glauben seit jeher eine zentrale Rolle im Zusammenhang mit informationsrechtlichen Fragen und Ansprüchen*.

440 Der Appell an *ein faires, loyales, vertrauenswürdiges, verlässliches, nachvollziehbares, redliches Verhalten* hat im Kontext von Information und Kommunikation einen prominenten Stellenwert.[653] Das Recht wird im Umgang mit Information, Kommunikation und Beziehungen mit ganz eigenen Herausforderungen konfrontiert.[654] Allgemein haben Informationen und deren Verarbeitung eine eigene Wirkungsmacht und -logik; Verstösse gegen informationelle Normen und Erwartungen sind schwieriger zu handhaben als beispielsweise der unrechtmässige Umgang mit einer Sache, einem körperlichen Gegenstand. Lassen sich «treuwidrige» Verhaltensweisen im Rahmen der Erfüllung eines Sachkaufes oder einer

651 Vgl. BGE 125 III 86, E 3.c.; BGE 121 III 350; BGE 116 II 431, E 3; vertiefend Kuonen, *passim*; BGE 140 III 200, E 5.2.: vgl. Honsell, BSK-ZGB, Art. 2 N 14 ff.; Auer, Materialisierung, 122; Druey, 525 ff.; kritisch zur Idee, wonach Information und Transparenz per se Vertrauen sowie Werte schaffen, Druey, in: Kramer/Nobel/Waldburger, 589 ff., 592 ff.; zur Vertrauenshaftung Bucher, in: Forstmoser/Honsell/Wiegand (Hrsg.), 231 ff.

652 Vgl. Druey, 232 ff., 155, 313 ff.; zu Art. 2 ZGB als rechtsdogmatischem Ansatz eines Vertraulichkeitsschutzes Häusermann, 107 ff.; Steinauer, 165 ff. und insb. 185 ff.; Tuor/Schnyder/Schmid/Jungo, 47 ff.; zur Confidentiality Harvey, U. Pa. L. Rev. 1992, 2385 ff.

653 Illustrativ insofern der Beitrag von Fried, Yale L.J. 1968, 475 ff.; Boll, 2.

654 Grundlegend hierzu namentlich Zech, *passim*.

Miete auf der «Sachebene» meist ausgleichen, steht eine entsprechend wirksame Mechanik im Umgang mit Information gerade nicht zur Verfügung. Bereits der Volksmund bringt die informationellen Besonderheiten mit Redewendungen wie «Es bleibt immer etwas hängen» oder «Ist der Ruf mal ruiniert, lebt es sich ganz ungeniert» eingänglich zum Ausdruck.

441 Entsprechend hat das Recht seit Längerem versucht, spezifische Instrumente zu schaffen: Im Kontext des Medienrechts ist vor diesem Hintergrund die Ausübung des Rechts auf Gegendarstellung, Art. 28g ff. ZGB von Bedeutung. Das Recht auf Gegendarstellung ermöglicht es dem Betroffenen, auf Tatsachendarstellungen in periodisch erscheinenden Medien, die ihn in einem schlechten Licht dastehen lassen, zu reagieren, vorab ohne behördliche Intervention. Ziel des Instruments der Gegendarstellung ist die Verwirklichung des Prinzips der «gleich langen Spiesse» im Medienkontext. Der Gesetzgeber hat insofern ein eigenes Rechtsinstrumentarium geschaffen, um eine «faire», «korrekte» Medienberichterstattung abzusichern und das Konzept von «audiatur et altera pars» auch unter Privaten wirksam werden zu lassen. Das Rechtsinstitut ist damit von Treu und Glauben mitinspiriert. Immerhin: Mit der Geltendmachung des Gegendarstellungsrechts wird allenfalls eine unliebsame Angelegenheit erneut in Erinnerung gerufen, was nicht immer von Vorteil ist. Erfolgte Informationsflüsse lassen sich nicht beliebig rückgängig machen.

442 Treu und Glauben ist untrennbar mit *Vertrauen* verbunden: Vertrauen wiederum bildet eine Grundbedingung zwischenmenschlicher Beziehungen. Beziehungen leben zu einem wesentlichen Teil von Kommunikation und Informationsaustausch. An dieser Stelle sei an das im ersten Teil dargestellte Arztgeheimnis erinnert, wobei die traditionsreichen Geheimhaltungspflichten als die frühesten «datenschutzrechtlichen» Instrumente beschrieben wurden. Das Arztgeheimnis schützt, wenn auch nicht ausschliesslich und isoliert, das *Vertrauensverhältnis* zwischen behandelnder Ärztin und Patienten.[655]

443 Heute gelten das Reputationsrisiko und der Vertrauensverlust aufgrund einer *medialen Berichterstattung* über Compliance-Verstösse und damit ebenso Datenschutzverstösse als Kernherausforderung.[656] In digitalen Netzwerken verbreiten sich entsprechende Informationen schnell und weit. Ein datenschutzrechtskonformer Umgang ist damit nicht nur unter Berücksichtigung von drohenden behördlichen Sanktionen oder zivilrechtlichen Klagen geboten, sondern ebenso wegen potentieller Vertrauensverluste, welche eine «negative Presse» bringen können.

655 Vgl. BGE 117 Ia 341, E 6.a. sowie BGE 87 IV 105, E 2.b.

656 Hierzu Vesting, in: Ladeur (Hrsg.), 155 ff., 182; dazu, dass auch die verschärften Sanktionen gemäss DSGVO ein beträchtliches Reputationsrisiko darstellen, Räther, ZHR 2019, 94 ff., 95 f.; vertiefend dritter Teil, VII. Kapitel, A.3.

444 Der kurze Abriss redet somit dem eingangs zitierten Druey das Wort: Treu und Glauben hat in Anbetracht der Bedeutung von Information und Kommunikation für soziale Beziehungen sowie der «Eigenarten» von Information als Schutzgegenstand in seiner *präventiven Rolle im Sinne von Handlungsanleitungen an das faire, redliche, korrekte Informations- und Kommunikationsverhalten besondere Relevanz*. Die *retrospektive Korrektur* und Kompensation von Verstössen gegen Informationserwartungen bleibt hingegen gerade aufgrund der «Natur» personenbezogener Daten, die «nicht-rivalisierend» sind sowie fluid, oft unmöglich.[657] Über den Grundsatz wird damit eine Erkenntnis transportiert, wonach der Umgang mit Information ebenso auf normativer Ebene spezifischen Logiken, Erwartungen und Enttäuschungen unterliegt.

445 Bevor auf Treu und Glauben in seiner *spezifischen Bedeutung als datenschutzrechtlicher Verarbeitungsgrundsatz* eingegangen wird, dient ein kurzer Überblick über die Theorien der Generalklauseln sowie Treu und Glauben der Bereitung des Bodens.

446 Die rechtswissenschaftlichen Studien zu den Generalklauseln für das Privat- und Verfassungsrecht im Allgemeinen und zu den «Obergeneralklauseln» wie Treu und Glauben sowie den guten Sitten im Besonderen füllen Bibliotheken. Hierbei wird versucht, die unbestimmten Rechtsbegriffe zu qualifizieren und zu systematisieren, zudem werden diese anhand ihrer jeweiligen Funktionen erörtert. Die Kernbestrebungen richten sich indes auf die jeweiligen inhaltlichen Konkretisierungen der einzelnen unbestimmten Rechtsbegriffe. Eine Sichtung der Literatur zu Treu und Glauben sowie anderen Generalklauseln führt zunächst eine breit angelegte Diskussion zur *Definierung von Generalklauseln selbst* zu Tage.

447 Die *Einheitstheorien* wollen die Generalklauseln anhand *eines einzelnen Kriteriums* einfangen, wobei allerdings das einschlägige Kriterium in den verschiedenen Beiträgen variiert.[658] In den sog. *Verbindungstheorien* werden *mehrere Definitionskriterien* (Generalklauseln als wertungsbedürftiger Tatbestand, als unbestimmte, abstrakte oder allgemeine Rechtsbegriffe, als Normbildungsauftrag an die Gerichte) kombiniert.[659] Eine teilweise neue Systematisierung und Interpretation zu den Generalklauseln legt Auer vor. Sie präsentiert *drei Grundwidersprüche in der Privatrechtsordnung*: erstens den materiellen zwischen Individualismus und Kollektivismus, zweitens den formalen zwischen Rechtssicherheit und Einzelfallgerechtigkeit und drittens den institutionellen zwischen Richterbindung

657 Ähnlich sowie zur Fluidität von Daten Flückiger, AJP 2013, 837 ff., 838 f.; zur Nichtrivalität von Daten insb. Zech/Hürlimann, sui-generis 2016, 89 ff., 90.
658 Vgl. Hellwege/Soniewicka, 8.
659 Vgl. vertiefend hierzu Teubner, Direktiven, 118; Auer, Materialisierung, 127 ff.; Röthel, in: Riesenhuber (Hrsg.), 225 ff.

und Richterfreiheit.[660] Generalklauseln wirken gemäss der Autorin als *Äquilibriums-Instrument,* als Puffer resp. bewegliche Zonen im statischen Gebäude, um der Beurteilung und Austarierung ebendieser Dichotomien Raum zu verschaffen. Die Qualifizierung als Generalklausel erfolgt dann, wenn ein offener oder unbestimmter Rechtsbegriff die *Funktion des Wertungsausgleichs* innerhalb der drei Grundwidersprüche wahrnimmt.[661]

448 Eine *Metapher*, die mit Generalklauseln und damit für Treu und Glauben auftaucht, ist das *Einfallstor.*[662] Generalklauseln öffnen das Recht gegenüber ausserrechtlichen Normen und Entwicklungen; so könne beispielsweise die gute Sitte als Verweis auf tatsächlich geltende Sitten und Gebräuche, also empirisch feststellbare soziale Normen, interpretiert werden.[663] Generalklauseln gelten als Öffnungsklauseln für Anpassungen an sich wandelnde Lebensverhältnisse.[664]

449 Neben Definitionsversuchen der Generalklauseln selbst steht im Zentrum der Auseinandersetzungen mit ihnen deren *Konkretisierung*. Als Kernherausforderung und -aufgabe gilt die Rationalisierung der Methode, um griffige Inhalte sowie standardisierte Funktionen zu umschreiben. Insofern wurden mehrere Ansätze entwickelt.[665] Die *Funktionstheorie* mit Wiackers rechtstheoretischer Präzisierung zu Treu und Glauben lautet «*iuris civilis invandi, supplendi, corrigendi gratia*».[666] Es sind damit mehrere Funktionen, die Treu und Glauben wahrnimmt, namentlich die *interpretative Funktion* für Rechtsgeschäfte und Erlasse (wobei Treu und Glauben im Rahmen der Interpretation von AGB eine besondere Bedeutung erlangt hat), die *ergänzende Funktion* für Rechtsgeschäfte und Erlasse (womit sich Treu und Glauben oft in der Zone der Auslegungsfragen bewegt) sowie die *anpassende resp. korrigierende und auflösende Funktion*.[667]

450 Weiter soll «Ordnung und Rechtssicherheit» generiert werden: Konkretisierte Anwendungsfälle von Treu und Glauben resp. des Rechtsmissbrauchs werden anhand von *Fallgruppen* systematisiert.[668] Die Zuweisung gewisser Tatbestände zu Art. 2 Abs. 1 resp. zu Abs. 2 ZGB wird allerdings teilweise kontrovers disku-

660 Auer, Materialisierung, 98.
661 Dies., a. a. O., 142.
662 Vgl. BverfG, Beschluss der 2. Kammer des Ersten Senats vom 14. September 2010 – 1 BvR 1504/10, E 13.
663 Vgl. hierzu Teubner, 29 ff., 61, 65 ff.; Walter, in: Ehrenzeller/Gomez/Kotzur/Thürer/Vallender (Hrsg.), 127 ff., 133 f.; BverfG, Beschluss der 2. Kammer des Ersten Senats vom 14. September 2010 – 1 BvR 1504/10, E 13.
664 Auer, Materialisierung, 55.
665 Dies., a. a. O., 144 ff.
666 Wiacker, zit. nach Auer, Materialisierung, 163.
667 M. w. H. auf die einschlägigen Quellen Pfaffinger, KuKo-ZGB, Art. 2 N 2 und N 7.
668 Vgl. Riemer, § 5 N 13; Hürlimann-Kaup/Schmid, N 266.

tiert.[669] Als Konsequenz wird Art. 2 ZGB denn auch als Gesamtkonzept für einen *allgemeinen Vertrauensschutz* dargestellt.[670]

451 Konkretisiert formuliert Treu und Glauben – das Bundesgericht spricht von einer Grundschutznorm[671] – einen allgemeinen, übergeordneten (objektiven) Massstab,[672] wobei die *gegenseitige Rücksichtnahme* im Rahmen der Ausübung resp. Achtung gesetzlicher wie rechtsgeschäftlicher Pflichten und Rechte verlangt wird. Treu und Glauben gebietet und schützt *loyales, redliches, korrektes Verhalten, das gegenseitige Vertrauen- und Glauben-Dürfen, die Fairness im Rechtsverkehr*.[673] Seit jeher und an erster Stelle wird Treu und Glauben als *Auffangklausel* beschrieben.[674] Treu und Glauben wurde und wird dort angerufen, wo positivierte Regeln und Grundsätze einen Sachverhalt nicht oder nicht befriedigend erfassen. Hat sich alsdann eine Praxis konsolidiert, werden nicht selten die vonseiten der Praxis und Wissenschaft über die Wendung von Treu und Glauben anerkannten Ansprüche vom Gesetzgeber rezipiert und in eigenständige Normen überführt.

452 Ebendiese Konstruktionen und Charakterisierungen spielen nachfolgend eine Rolle beim Unterfangen, die *spezifisch datenschutzrechtliche Bedeutung von Treu und Glauben* zu durchdringen. Hierfür wird vorab auf die Verortung von Treu und Glauben in den datenschutzrechtlichen Texten eingegangen. Kombiniert mit einer Analyse zu den jüngsten datenschutzrechtlichen Entwicklungen lassen sich (Entwicklungs-)Linien nachzeichnen, die massgeblich von Treu und Glauben geprägt wurden. Jeglicher Kritik zum Trotz gegenüber Treu und Glauben als «Leerformel» präsentiert sich diese vielmehr als «Lehrformel» und «Einfallstor» in einem produktiven Sinne für die Weiterentwicklung des Datenschutzrechts. Den nachfolgenden Ausführungen zu «Treu und Glauben» mit Fokus auf *seine spezifische informationelle Bedeutung* ist vorauszuschicken, dass die Gültigkeit von Treu und Glauben im Datenbearbeitungskontext selbst ohne seine explizite Verankerung in Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG sowohl für den privaten als auch für den öffentlichen Datenbearbeitungssektor gewährleistet wäre. Als Generalklausel durchdringt Treu und Glauben die gesamte Schweizer Rechtsordnung, vgl. Art. 2 Abs. 1 ZGB sowie Art. 4 aBV, Art. 9 BV und Art. 5 Abs. 3 BV. Vergleichbar zum Rechtmässigkeitsprinzip rezipiert das Schweizer Datenschutzgesetz mit Art. 4 Abs. 2 erster Satzteil DSG resp. Art. 6 Abs. 2 erster Satzteil nDSG ein allgemeines und fundamentales Rechtsprinzip und importiert

669 M. w. H. Pfaffinger, KuKo-ZGB, Art. 2 N 2.
670 So Schwander, OFK-ZGB, Art. 2 N 2; vgl. zum Zusammenspiel zwischen Vertrauen und Recht Druey, Rechtswissenschaftliche Abteilung der Universität St. Gallen (Hrsg.), 525 ff.
671 BGE 125 III 261.
672 Riemer, § 5 N 2.
673 Hierzu Ders., § 5 N 2.
674 M. w. H. Ders., § 5 N 4.

es in das Datenschutzrecht. Mit dieser Einschreibung von Treu und Glauben ins Datenschutzgesetz macht sich ebenso dessen «didaktischer Wert» bemerkbar.[675] Das DSG bringt mit der «Leerformel» (und Lehrformel) von Treu und Glauben als allgemeinem Verarbeitungsgrundsatz zum Ausdruck, dass *loyales Gebaren auch im Rahmen von Datenverarbeitungen initial handlungsanleitend* ist.

453 Die «Zählebigkeit»[676] und Breitenwirkung der Generalklauseln, die selbst in die Felder und Zeiten der Digitalisierung übergreifen, hat ebenso einen «psychologischen Effekt» – Teubner hat ihn exemplarisch für die guten Sitten, mit Referenz auf Topitsch, wie folgt umschrieben: Man suggeriere zum einen Konstanz von höchsten moralisch-politischen Prinzipien, zum anderen schaffe man eine «kollektive Wertungseinheit», vereine Gefühl und Verstand, Rationalistinnen und Irrationalisten.[677] Dieser integrative und beruhigende Effekt ist *a fortiori* für ein Rechtsgebiet willkommen, das sich mit dem «rasanten technischen Fortschritt» und hierbei mit künstlicher Intelligenz, Algorithmen, Minichips, Clouds sowie hoher gesellschaftlicher Ambivalenz, Freud und Leid, Chancen und Risiken dieser neuen Technologien konfrontiert sieht.[678]

2.2. Datenschutzrechtliche Bedeutung

2.2.1. Positivierungen

454 Dem Grundsatz Treu und Glauben kommt seit jeher ein fester Platz in der Datenschutzregulierung zu.[679] In der DSGVO findet er sich in Art. 5 Abs. 1 lit. a mit den Worten:

> «Personenbezogene Daten müssen auf rechtmässige Weise und nach Treu und Glauben und in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden.»

455 In der Schweiz wurde in den 1980er Jahren intensiv über den rechten Ort des Grundsatzes im ersten eidgenössischen Datenschutzgesetz verhandelt, nicht ohne inhaltliche Zuweisungen daran zu koppeln (Stichwort «Relevanz der Systematik für die Auslegung von Gesetzen»): Im ersten Bundesratsentwurf von Art. 4 Abs. 1 ging Treu und Glauben, wie erwähnt, Hand in Hand mit dem Rechtmässigkeitsgebot:

675 Zum Begriff Meier, N 630 und N 647.
676 Teubner, 22.
677 M. w. H. Ders., a. a. O.
678 Vgl. z. B. mit Blick auf das Cloud Computing Cavoukian, digma 2009, 20 ff., 21 ff.
679 Vgl. vor den gesetzgeberischen Anpassungen, die im Zuge der DSGVO erfolgten, z. B. § 6 Abs. 1 Ziff. 1 des Österreichischen Datenschutzgesetzes sowie die französische Loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Version consolidée au 27 septembre 2016, wonach Art. 6 Abs. 1 lautete: «Les données sont collectées et traitées de manière loyale et licite».

> «Personendaten dürfen nur *mit rechtmässigen Mitteln und nicht wider Treu und Glauben* [Hervorhebung durch die Autorin] beschafft werden.»[680]

456 In Kraft gesetzt wurde am 1. Juli 1993 Art. 4 Abs. 2 DSG, der betreffs Personendaten vorschreibt:

> «Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.»

457 An Art. 4 Abs. 2 DSG selbst, welcher den Grundsatz von Treu und Glauben mit demjenigen der Verhältnismässigkeit vereint, wurde seit Inkrafttreten des DSG nichts geändert. An derselben Formulierung und Kombinierung mit dem Verhältnismässigkeitsprinzip wird abgesehen von einer minimalen sprachlichen Vereinfachung mit der Totalrevision festgehalten, vgl. Art. 6 Abs. 2 nDSG. Die Totalrevision führt indes mehrere neue Instrumente ein, deren Entwicklung in Treu und Glauben festzumachen sind. In ihrem Zentrum steht der *Ausbau spezifischer Informationsvorgaben und entsprechend der Transparenz*.[681] Ein Prozess der Ausdifferenzierung und Fortentwicklung datenschutzrechtlicher Vorgaben über Treu und Glauben lässt sich keineswegs erst im Zuge der jüngsten Entwicklungen im Zuge der Totalrevision nachzeichnen. Explizite Anerkennungen von eigenständigen *Transparenzvorgaben* gelten als Ableitungen von Treu und Glauben.[682] Vor Teilrevision des DSG 2008 und der Stärkung der Transparenzerfordernisse galt, wie erwähnt, eine *heimliche* Beschaffung von Daten oder eine solche unter Angabe einer falschen Identität oder eines falschen Zwecks als Verstoss gegen Treu und Glauben.[683]

458 Damit hat Treu und Glauben bislang im Kontext des Datenschutzes eine *Anstoss*- und damit *Rechtsfortbildungsfunktion* für die gesetzgeberische Konkretisierung, Ausdifferenzierung, Fortentwicklung und Spezifikation datenschutzgesetzlicher Rechte und Pflichten wahrgenommen. Einige der in der Schweiz (noch) über den Phraseologismus abgehandelten Vorgaben wurden in Deutschland, wo Hessen als erstes Bundesland früh ein eigenes Datenschutzgesetz verabschiedete und der Bund schon 1977 sein erstes Bundesdatenschutzgesetz erliess, bereits gesetzgeberisch spezifisch normiert. Augenfällig war allerdings, dass Treu und Glauben in seiner «abstrakten» Gestalt im Deutschen Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 nicht verankert war. Auf den ersten Blick erstaunt dies für ein Land, das als «Schrittmacher» für die

680 Vgl. BBl 1988 II 414 ff., 460 und 517.

681 Zum Ausbau der Transparenzvorgaben Botschaft DSG 2017–1084, 17.059, 6941 ff., 6972 ff.; Baeriswyl, digma 2020, 6 ff., 6.

682 Vgl. Art. 4 Abs. 4 DSG, Erkennbarkeit der Beschaffung und Erkennbarkeit des Zweckes, später Art. 7a DSG, inzwischen wieder aufgehoben; BBl 1988 II 414 ff., 449; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 8; Rosenthal, HK-DSG, Art. 4 N 14; Meier, N 649.

683 Wiederum zeigt sich an dieser Stelle die Schwierigkeit der Abgrenzung zu Art. 4 Abs. 1 DSG, zumal die Beschaffung unter falschen Angaben gleichermassen als Täuschung und damit unrechtmässige Datenbeschaffung gemäss Art. 4 Abs. 1 DSG zu beurteilen ist.

Entwicklungen und Fortschritte im Datenschutzrecht gilt, wenn Treu und Glauben als Impulsgeber für die datenschutzrechtliche Weiterentwicklung und hierbei insb. für den Ausbau von Transparenzvorgaben verstanden wird. Der Verzicht ist erklärbar: Vorab beansprucht der Grundsatz in Deutschland bereits aufgrund allgemeiner Bestimmungen ausserhalb des DSG ebenso für das Datenschutzrecht Gültigkeit. Weitere spezifische Vorgaben sind als Konkretisierungen von Treu und Glauben zu lesen, so insb. der Grundsatz der *Direkterhebung*. Im Bundesdatenschutzgesetz vom 30. Juni 2017 findet sich der Grundsatz neu ausdrücklich in § 47 Ziff. 1 BDSG verankert, womit die Vorgabe gemäss Art. 5 Abs. 1 lit. a DSGVO rezipiert wird.

459 Für die Schweiz belegt sich die explizite Voranstellung von Treu und Glauben als allgemeiner Verarbeitungsgrundsatz gerade für den privaten Sektor als sinnvoll. Erst die «treuwidrige», also die qualifizierte Datenverarbeitung, wird im privatrechtlichen Bereich mit einer «roten Flagge» versehen.[684] Seit jeher haben Treu und Glauben, vgl. auch Art. 2 Abs. 1 ZGB, und namentlich das Verbot des Rechtsmissbrauchs, vgl. Art. 2 Abs. 2 ZGB, die Funktion, an den *äussersten Rändern* «Schranken» zu setzen. Interveniert wird bei «krass stossenden Verhaltensweisen oder Ergebnissen».[685] Gerade in Bezug auf die datenschutzgesetzliche Normierung für den privaten Bereich, die vom Grundsatz der freien Verarbeitung mit Schranken ausgeht und an der qualifizierten Verarbeitungshandlung ansetzt, ist es entsprechend gesetzgeberisch angezeigt, die Datenbearbeitenden eingangs an diese «äussersten Schranken» zu erinnern. Dagegen kommt Treu und Glauben in einem Datenschutzrecht, in dem der Grundsatz des Verarbeitungsverbotes mit Erlaubnistatbeständen implementiert ist und das zudem eine längere zeitliche Konsolidierungs- und Ausdifferenzierungsphase hinter sich hat, eine andere Rolle zu.

2.2.2. Rezeption in der Schweizer Lehre und Praxis

460 Wie wird Treu und Glauben in der datenschutzrechtlichen Lehre und Praxis der Schweiz rezipiert und inwieweit spiegelt sich der dem Prinzip im Informationskontext zugewiesene gewichtige Bedeutungsgehalt? Auf die zahlreichen Unklarheiten bzgl. der Bedeutung von Treu und Glauben im Datenbearbeitungskontext wird in der Doktrin hingewiesen: Hier wird die Frage aufgeworfen, ob der Grundsatz neben dem Zweckbindungs-, Verhältnismässigkeits-, aber auch Recht-

684 Zur Verwendung dieser Metapher im Datenschutzkontext Nissenbaum, 127 ff., 148 ff.; beachte sodann Art. 13 Abs. 2 BV, der – wenn auch nicht direkt auf den privaten Bereich anwendbar – den Schutz vor missbräuchlicher Datenverarbeitung und jedenfalls im Wortlaut gerade kein (Grund-)Recht auf informationelle Selbstbestimmung verbürgt; kritisch ebenso Gächter/Werder, in: Epiney/Fasnacht/Blaser (Hrsg.), 87 ff., 91 ff.

685 Vgl. Riemer, § 5 N 14; Bger 5A_304/2010 vom 27. August 2010, E 4.5.1.

mässigkeitsprinzip überhaupt eine eigene Bedeutung habe.[686] Umgekehrt wird der Grundsatz im datenschutzrechtlichen Kontext nicht nur von Meier als mehr denn ein didaktisches Lehrstück im Sinne eines ermahnenden Fingers taxiert.[687] Die Ausführungen zum Grundsatz von Art. 4 Abs. 2 DSG sind – trotz der *in abstracto* deklarierten hervorragenden Bedeutung von Treu und Glauben im Informationskontext – dennoch *punktuell* und stark *einzelfallbezogen*. Systemisch wird der Grundsatz – abgesehen von der Stärkung des Transparenzgebotes als tragende Säule zeitgenössischer Datenschutzregulierung – nicht fruchtbar gemacht.

Die erste Wortmeldung stammt vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeamten. Der EDÖB lässt zu Treu und Glauben verlautbaren: 461

> «Personendaten dürfen nicht ohne Wissen und gegen den Willen der betroffenen Person beschafft werden. Wer die betroffene Person bei der Datenbeschaffung absichtlich täuscht – z. B. wenn er die Daten unter Angabe einer falschen Identität beschafft oder falsche Angaben über den Zweck der Bearbeitung erteilt –, verletzt das Prinzip von Treu und Glauben. Dieses verletzt er auch, wenn er Personendaten verdeckt beschafft, beispielsweise durch Belauschen eines Gesprächs oder Abhören von Kommunikationsverbindungen.»[688]

Die Passage verleitet indes selbst eine redliche Leserschaft zu einer Fehlannahme betreffend die Bedeutung der Einwilligung des Datensubjektes: Nach Schweizer Datenschutzgesetz ist eine Bearbeitung selbst gegen den Willen des Datensubjektes zulässig, vgl. Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG, sofern hierfür ein Rechtfertigungsgrund vorliegt. Zugleich illustrieren die Erwägungen des EDÖB erneute Abgrenzungsschwierigkeiten zwischen den verschiedenen Bearbeitungsgrundsätzen und Verarbeitungsvorgaben, insb. dem Grundsatz der Erkennbarkeit sowie den sukzessive national wie international ausgebauten Transparenzgeboten. 462

Darüber hinaus rücken *zwei Rechtsfälle*, die den Umgang mit Personendaten betreffen, *Treu und Glauben in das Zentrum ihrer Argumentation*: zum einen der *Spamming-Entscheid* des Bundesverwaltungsgerichts, zum anderen die *Logistep-Entscheide* des Bundesverwaltungsgerichts und des Bundesgerichts. In ersterem wurde der Generalklausel Relevanz im Rahmen der *elektronischen Massenmedien* und der Bewerbung zugemessen. In seinem *Spamming-Entscheid* weist das Bundesverwaltungsgericht in E 5.5. auf die fundamentale Bedeutung von Treu und Glauben im Rechtsverkehr hin mit den Worten: 463

686 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 8.
687 Meier, N 630 und N 647.
688 EDÖB, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/telekommunikation/telefonie/allgemeine-grundsaetze.html#886355380> (zuletzt besucht am 10. September 2021); Schlussbericht vom 1. Juni 2015 betreffend die Abklärung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

> «Dieser Grundsatz […] gebietet ein loyales und vertrauenswürdiges Verhalten im Rechtsverkehr. Im Geschäftsverkehr hat Treu und Glauben eine herausragende Bedeutung. Das Gebot von Treu und Glauben im Geschäftsverkehr, welches wie das Rechtsmissbrauchsverbot eine Ausprägung des gleichen Grundsatzes ist, gehört zum Kreis der universell anerkannten Rechtsgüter, deren Schutz der positive „Ordre public" dient (BGE 128 III 207). Von einem loyalen und vertrauenswürdigen Verhalten im Geschäftsverkehr kann jedoch keine Rede sein, wenn eine an einer Geschäftsanbahnung interessierte Partei es in Kauf nimmt, zur Gewinnung einzelner Kunden systematisch eine Vielzahl von nicht einmal ansatzweise identifizierten Adressaten wahllos mit beliebiger Streuwerbung zu bedienen. Dies gilt erst recht, wenn dieser Vielzahl von Empfängern in voraussehbarer Weise gänzlich nutzlose Auslagen und Umtriebe anfallen, wie dies vorliegend der Fall ist. Insbesondere darf nicht vermutet werden, dass eine Person ihre E-Mail-Adresse bekannt gibt, damit ihr jeder beliebige Anbieter im World Wide Web seine Angebote für die Anbahnung von Geschäftsbeziehungen unterbreiten kann. Der Grundsatz von Treu und Glauben greift schon im vorvertraglichen Bereich. Daher hat die an einer Geschäftsanbahnung interessierte Partei die Privatsphäre und die Interessen des anderen zu respektieren. Dazu gehört, dass der Geschäftswillige nicht ungefragt und systematisch massenhaft nutzlose Auslagen und Umtriebe bei Dritten verursacht. Bei wahlloser Streuwerbung an nicht identifizierte Dritte ist zu beachten, dass der Anbieter nur über vage bzw. ganz und gar zufällige Aussichten auf eine Geschäftsmöglichkeit verfügt, wenn er seine Werbung an Personen und Unternehmen adressiert, von denen er nicht einmal im Ansatz weiss, um wen es sich dabei handelt und welche Interessenlage bei diesen herrscht. Es verstösst somit gegen Treu und Glauben, wenn ein an Geschäftsanbahnung Interessierter systematisch Tausenden von Adressaten ungefragt und nutzlos beachtliche Kosten und Umtriebe für die Zustellung seiner Werbung zumutet, nur um zufällig zu einzelnen Geschäftsabschlüssen zu gelangen. Ein solches Verhalten missachtet den Willen der Personen, die ihre E-Mail-Adressen im Internet für gezielte Kontaktaufnahmen und Werbung zugänglich gemacht haben. Demzufolge liegt in der Verwendung von wahllos gesammelten, nicht identifizierten E-Mail-Adressen zum Zweck der Zustellung unverlangter Streuwerbung ein Verstoss gegen den Grundsatz von Treu und Glauben im Sinne von Art. 4 Abs. 2 DSG (ebenso, wenn auch aus wettbewerbsrechtlicher Sicht, ZR 102 Nr. 39; sic! 7/8/2003).»[689]

464 Heute ist es Art. 3 lit. o UWG, in Kraft seit 2007, der Massenwerbung in besagter Form als unlautere Praxis taxiert – ein Beispiel, inwiefern über Treu und Glauben in der Praxis eine konkretisierte Vorgabe formuliert wird, die alsdann Eingang in ein Gesetz findet.

465 Ein anderer Aspekt von Treu und Glauben als Datenbearbeitungsgrundsatz wird in den *Logistep-Entscheiden* des Bundesverwaltungsgerichts resp. Bundesgerichts reflektiert.[690] Es ging um die Aufdeckung strafrechtlicher Handlungen, genauer um Urheberrechtsverletzungen im Internet durch Private.[691] Die Logistep AG, ein

689 Spamming-Entscheid des Bundesverwaltungsgerichts, JAAC 69.106, E 5.5.

690 BVGer A-3144/2008, Urteil vom 27. Mai 2009; BGE 136 II 508; vgl. zur rechtlichen Diskussion um das Internet und das Recht, die insb. die Bereiche des Urheber- und Datenschutzrechts, die Domain- und Verschlüsselungsdebatte, die elektronische Debatte und diejenige rund um schädliche Inhalte im Internet erfasse, Burkert, in: Drossu/van Haaren/Hensche et al. (Hrsg.), 185 ff., 185 f.

691 Aufschlussreich in diesem Zusammenhang die Ausführungen zu Spyware, auch mit Blick auf den Einsatz von Urheberrechtsverletzungen Bucher, 95 ff.; grundlegend zu DRM-Systemen im Zusam-

privates Unternehmen, sammelte in P2P-Netzwerken IP-Adressen von Personen, die urheberrechtlich geschützte Werke «schwarz», d. h. ohne Entrichtung der geforderten Gebühr, herunterluden. Entsprechende Angaben übermittelte sie in der Folge den Rechteinhabern, die alsdann Strafanzeige gegen Unbekannte einreichten. Im Rahmen des strafrechtlichen Akteneinsichtsrechts konnten die Identitäten der Inhaber der Internetanschlüsse erlangt werden und diese mit einer Schadenersatzforderung konfrontiert werden. Der EDÖB hatte gegenüber der Logistep AG eine Empfehlung gestützt auf Art. 29 Abs. 3 DSG erlassen, die indes nicht befolgt wurde. Daraufhin legte der EDÖB die Angelegenheit dem Bundesverwaltungsgericht zur Entscheidung vor. Dieses beschäftigte sich, nachdem es die Anwendbarkeit des DSG auf den Sachverhalt bejaht hatte, mit der Frage, ob eine Verletzung der Bearbeitungsgrundsätze vorliege. Hierbei ging es auch auf Treu und Glauben gemäss Art. 4 Abs. 2 DSG ein:

> «Dem Prinzip von Treu und Glauben kommt gerade bei der Datenbeschaffung besondere Wichtigkeit zu. Daten sollen nicht in einer Art erhoben werden, mit der die betroffene Person nicht rechnen musste und mit der sie nicht einverstanden gewesen wäre. Wider Treu und Glauben handelt namentlich, wer Daten durch absichtliche Täuschung beschafft, weil er beispielsweise die betroffene Person über seine Identität oder den Zweck seiner Bearbeitung falsch informiert, oder wer heimlich Daten beschafft, ohne dabei eine Rechtsnorm zu verletzen (vgl. Botschaft zum DSG, BBl 1988 II, S. 449). Aus dem Grundsatz von Treu und Glauben ist auch die Anforderung abzuleiten, dass eine Datenbearbeitung transparent erfolgen muss, das heisst grundsätzlich für die betroffene Person erkennbar sein muss […]. Im Zusammenhang mit der Prüfung einer Verletzung des Grundsatzes von Treu und Glauben ist daher auch die vom Kläger gerügte Verletzung des Erkennbarkeitsprinzips zu behandeln. Der Kläger macht geltend, dieses sei verletzt, weil die von der Beklagten durchgeführte Datenbearbeitung heimlich stattfinde und weder für den Urheberrechtsverletzer noch für den Inhaber des Internetanschlusses erkennbar sei. Würden die Daten als besonders schützenswerte Personendaten im Sinne von Art. 3 Bst. c DSG qualifiziert, käme der Beklagten sogar eine gesteigerte Informationspflicht zu, wonach die Einwilligung der betroffenen Person nach angemessener Information ausdrücklich zu erfolgen habe (Art. 4 Abs. 5 DSG).»[692]

Das Bundesverwaltungsgericht beurteilte das Vorgehen der beklagten Logistep AG im Lichte des Vertrauensprinzips als «diskutabel», um sodann anzufügen: 466

> «Angesichts der Umstände, die die Beklagte erst zur Datensammlung bewegten, hält diese aber vor dem Grundsatz von Treu und Glauben stand.»[693]

Allerdings: Da die Beschaffung der Daten ohne Wissen der Betroffenen erfolgte, liege in der Regel eine Verletzung des Erkennbarkeitsprinzips und damit eine Per- 467

menhang mit dem Urheberrecht Bechthold, 1 ff.; humoristisch zur Thematik der Abschnitt bei Schaar, 211 ff. unter dem Titel «Raubkopierer sind Verbrecher».

692 Vgl. BVGer A-3144/2008, Urteil vom 27. Mai 2009, E 9.3; zu den besonders schützenswerten Personendaten vgl. auch Epiney, in: Rumo-Jungo/Pichonnaz/Hürlimann-Kaup/Fountoulakis (Hrsg.), 97 ff.

693 Vgl. BVGer A-3144/2008, Urteil vom 27. Mai 2009, E 9.3.4. und E 9.3.6.

sönlichkeitsverletzung vor. Diese wurde als nicht widerrechtlich beurteilt, weil man in der Durchsetzung des Urheberrechtes ein überwiegendes öffentliches und privates Interesse gemäss Art. 13 DSG verortete.[694] Folglich wurden die Begehren des Klägers – sprich des EDÖB – vom Bundesverwaltungsgericht abgewiesen. Er legte das Urteil des Bundesverwaltungsgerichts alsdann *dem Bundesgericht zur Beurteilung* vor. Das Bundesgericht qualifizierte IP-Adressen nicht per se als Personendaten i. S. des DSG, ging indes im vorliegenden Fall ebenso von der Anwendbarkeit des DSG aus.[695] IP-Adressen, so das Bundesgericht, seien keine besonders schützenswerten personenbezogenen Daten, weshalb es auch keiner Einwilligung des Inhabers bedürfe. Bei der Überprüfung, ob die Vorgehensweise der Logistep AG im Einklang mit den Bearbeitungsgrundsätzen stehe, ging das Bundesgericht – anders als das Bundesverwaltungsgericht – nicht auf Art. 4 Abs. 2 DSG ein. Vielmehr stützte es seine Analyse auf Art. 4 Abs. 3 und 4 DSG und nahm eine Verletzung an.[696] Es verwarf die Argumentation im Urteil des Bundesverwaltungsgerichts und verneinte das Vorliegen eines Rechtfertigungsgrundes mit den Worten:

> «Wie bereits erwähnt, dürfen zudem Rechtfertigungsgründe beim Verstoss gegen die Grundsätze von Art. 4 DSG nur mit grosser Zurückhaltung bejaht werden (E. 5.2.4 hiervor). Mithin vermag auch das Interesse an der wirksamen Bekämpfung von Urheberrechtsverletzungen die Tragweite der Persönlichkeitsverletzung und der mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen. Ein überwiegendes privates oder öffentliches Interesse ist umso mehr zu verneinen, als dieses nur zurückhaltend bejaht werden darf.»[697]

468 Bezüglich Treu und Glauben als Datenverarbeitungsgrundsatz ist aus der Schweizer Doktrin besonders auf die Erwägungen von Epiney/Nüesch einzugehen. Sie weisen Treu und Glauben im Datenschutzrecht zunächst die allgemein beschriebene *Auffangfunktion* zu. Gemäss den Autorinnen handle es sich um eine Generalklausel, die dann greifen solle, wenn die anderen Bearbeitungsgrundsätze *nicht* wirksam werden.[698] Diese Auffangfunktion wird übrigens ebenso für den Bearbeitungsgrundsatz von Treu und Glauben gemäss DSGVO in der Kommentarliteratur anerkannt.[699] Die beiden Schweizer Autorinnen plädieren darüber hinaus dafür, aus dem abstrakten Bearbeitungsgrundsatz eine *individualrechtlich ange-*

694 Vgl. BVGer A-3144/2008, Urteil vom 27. Mai 2009, E 12.3.2.; zum Urteil insb. in Bezug auf die Rechtfertigungsgründe, die Rechtmässigkeit sowie den Instanzenzug Schäfer, medialex 2011, 142 ff.

695 Nach EUGH gelten dynamische IP-Adressen nicht nur für den Provider, sondern auch für den Websitebetreiber als personenbezogene Angaben, weil der Websitebetreiber über den Provider die Identität des Betroffenen erlangen kann, vgl. m. w. H. Daten:recht, BGH i. S. Breyer, Personenbezug dynamischer IP-Adressen, <https://datenrecht.ch/bgh-i-s-breyer-vi-zr-13513-16-5-17-personenbezug-dynamischer-ip-adressen/> (zuletzt besucht am 30. April 2021); zum Begriff der Personendaten bereits Bischof/Schweizer, digma 2011, 152 ff.

696 BGE 136 II 508, E 6.3.1.

697 BGE 136 II 508, E 6.3.3.

698 Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.72.

699 M. w. H. Herbst, BeckKomm-DSGVO, Art. 5 N 15.

legte Informationspflicht abzuleiten: Demgemäss könne aus dem Grundsatz von Treu und Glauben gemäss Art. 4 Abs. 2 DSG eine allgemeine Informationspflicht gegenüber Datensubjekten («den Betroffenen») hinsichtlich Datenbearbeitungen resultieren, sofern diese angesichts der Umstände aus Loyalitätserwägungen als geboten erscheine.[700] Wann sich allerdings konkret eine solche Informationspflicht aus Loyalitätserwägungen manifestieren soll, wird nicht ausgeführt. Die Totalrevision rezipiert diese Stossrichtung, indem es die Transparenzvorgaben und insb. die Informationspflichten ausbaut, vgl. Art. 19 nDSG.[701]

In Lehre und der Rechtsprechung zu Treu und Glauben im Datenschutz lassen sich entsprechend *zwei Akzente* feststellen: 469

Erstens die Bedeutung von *Transparenzvorgaben*, wobei einige sukzessive gesetzliche Spezifizierungen im informationellen Kontext ihre Quelle in Treu und Glauben finden. Aufschlussreich insofern der Blick auf die kantonalen Erlasse: Sie verzichten regelmässig auf eine abstrakte und explizite Inklusion von Treu und Glauben in ihren Datenschutzgesetzen.[702] Stattdessen verankern sie ausdrücklich den Grundsatz der Erkennbarkeit und der Informierung.[703] Auf Bundesebene soll der Ausbau von Transparenzvorgaben mit der Totalrevision des DSG einen richtungsweisenden Entwicklungsanstoss verleihen.[704] Die Totalrevision schlägt nebst weiteren Instrumenten, welche die Transparenz erhöhen, eine allgemeinere Informationspflicht vor, womit die Transparenz erhöht wird, vgl. insb. Art. 19 nDSG mit den Ausnahmen gemäss Art. 20 nDSG. 470

Zweitens wird über Treu und Glauben als Verarbeitungsgrundsatz erneut die Relevanz der *Umstände* bzw. des *Kontextes*, in welchen Personendatenverarbeitungen eingebettet sind, sichtbar. Über den Grundsatz wird datenschutzrechtlich die Einschlägigkeit der Verarbeitungszusammenhänge anerkannt. Der Logistep-Entscheid weist auf die Umstände hin und darauf, dass Personendatenverarbeitungen *im Lichte von Treu und Glauben dann problematisch seien, wenn die betroffene Person nicht damit rechnen müsse*. Ebendies wurde in jenem Fall angenommen aufgrund der Tatsache, dass Private auf intransparente Weise Strafverfolgungsfunktionen wahrnahmen, wobei die «verdeckt ermittelnde» Logistep AG wirtschaftliche Interessen verfolgte.[705] 471

700 Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.72.
701 M. w. H. Bühlmann/Lagler, SZW 2021, 16 ff.
702 Sie widmen sich entsprechend der in der Schweiz verfassungsrechtlich vorgeschriebenen Kompetenzausscheidung dem kantonalen öffentlichen Recht.
703 Meier, N 650.
704 Vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff., 6944 und 6974.
705 Vgl. auch unter Bezugnahme auf das Erkennbarkeitsgebot BGE 136 II 508, E 4, E 5.2.6., E 6.3.3.; vgl. zu Treu und Glauben nach DSG BVGer, A-3144/2008, Urteil vom 27. Mai 2009, E 9.

472 Beide Kernelemente von Treu und Glauben im Rahmen des DSG – Transparenz und Relevanz der Umstände – finden sich auch beim EDÖB im Schlussbericht i. S. Postfinance 2015:

> «Die Bearbeitung von Personendaten muss nach Treu und Glauben erfolgen (Art. 4 Abs. 2 DSG). Daten sollen nicht in einer Art erhoben und bearbeitet werden, mit der die betroffene Person aus den Umständen heraus nicht rechnen musste und mit der sie nicht einverstanden gewesen wäre. Gegen diesen Grundsatz verstösst beispielsweise derjenige, der Daten nicht offen bearbeitet, ohne dabei gegen eine Rechtsnorm zu verstossen (Botschaft DSG BBl 1988 II 449). Demzufolge muss eine Datenbearbeitung für die betroffenen Personen transparent erfolgen. Dies bedeutet gemäss Art. 4 Abs. 4 DSG, dass für betroffene Personen die Datenbeschaffung und jede weitere Datenbearbeitung (BSK-DSG, Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 8), der Zweck jeder (weiteren) Datenbearbeitung, die Identität des Datenbearbeiters und – bei einer Datenbekanntgabe an Dritte – die Kategorien von möglichen Datenempfängern erkennbar sein müssen (Botschaft DSG BBl 2003 2125). Auch die Beschaffung von Personendaten bei Dritten muss erkennbar sein (Botschaft DSG BBl 2003 2126).»[706]

473 Vom Grundsatz von Treu und Glauben gehen folglich wichtige Impulse für die Rechtsentwicklung aus, namentlich was *Transparenzvorgaben sowie die Integration kontextueller Erwägungen* anbelangt. Zu beiden Elementen ist immerhin zu ergänzen: Die Konkretisierung und Fortbildung des Rechts durch die *rechtsanwendenden Behörden*, die über die Generalklauseln erfolgen soll, vermag sich im Datenschutzrecht gerade auch für Treu und Glauben kaum zu entfalten. Zwar kam es in den letzten Jahren in der Schweiz zum einen oder anderen nennenswerten Urteil, das sich ebenso mit Treu und Glauben sowie den weiteren generalklauselartigen Verarbeitungsgrundsätzen beschäftigte. Gleichwohl müssen Quantität und Effekt behördlicher Datenschutzentscheide in Anbetracht der faktisch «grenzenlosen» Personendatenverarbeitungen als marginal qualifiziert werden.[707] Ursächlich für die bescheidene Rechtsdurchsetzung ist zum einen die Tatsache, dass die Kompetenzen des EDÖB für den privatrechtlichen Sektor (jedenfalls vor der Totalrevision) restriktiv gestaltet sind. Zum anderen ergreifen Einzelpersonen kaum je die privatrechtlichen Instrumente des Persönlichkeitsschutzes bei Verletzungen des Datenschutzgesetzes.[708] «Der Richterkönig», ein traditionelles Angstbild im Zusammenspiel mit den Generalklauseln, bleibt im Datenschutzrecht fiktiv.[709]

706 EDÖB, Schlussbericht Postfinance, 12.

707 Vgl. zur geografischen Grenzenlosigkeit von Personendatenverarbeitungen bereits Henke, 18 ff.; vgl. sodann die Beiträge insofern in Weber/Thürer/Zäch (Hrsg.); das sukzessive Entfallen von Grenzen aufgrund der technologischen Möglichkeiten wird im Zuge dieser Arbeit vertieft dargestellt.

708 Vgl. Rosenthal, in Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.20; hierzu auch Mayer-Schönberger, Delete, 165 ff.

709 Teubner, 42, mit dem Hinweis, dass umgekehrt hierfür durch die Freirechtsschule plädiert wurde; vgl. zum durch Weber gezeichneten Gegenbild des Gerichts als Paragrafenautomaten m. w. H. Baer, 30 f.

Rosenthal legt ein methodisches Rezept im Umgang mit der datenschutzrechtlichen Orientierungslosigkeit vor. Dieses Rezept ändert nichts an der Tatsache, wonach Lehre und Rechtsprechung sich lange wenig intensiv um datenschutzrechtliche Auslegungsfragen gekümmert haben. Immerhin lässt sich in den letzten Jahren auch für die Schweiz feststellen, dass dem Datenschutzrecht im Zuge der Revisionswellen von Lehre und Behörden erhöhte Aufmerksamkeit zugemessen wird. Wie aber lautet das Rezept des Datenschutzexperten? Es geht um einen «Rückgriff auf das Bauchgefühl»[710] – ein Rezept, das Juristinnen herausfordert, *a fortiori* dort, wo es um die Konkretisierung eines Terminus geht, bei dem die *vernünftig handelnde Person als Referenzperson* eine Hauptrolle spielt.[711] 474

Entsprechend liess auch für das Datenschutzrecht die Kritik an den Generalklauseln, wie sie mit der berühmten «Flucht in die Generalklauseln» in allgemeiner Weise von Hedemann beschrieben wurde, nicht lange auf sich warten. Früh schon wurde für den Datenschutz eine Gesetzgebung kritisiert, die per Generalklauseln Antworten zu finden suche, *weil* die neuen Technologien nicht durchschaubar und durch konkretisierte Normen dingfest gemacht werden konnten.[712] Hinzu kommt, dass als Folge der ungenügenden Wirksamkeit der prozeduralen Durchsetzungsinstrumente keine stabilisierende Praxis generiert wird. Der Mechanismus, wonach Generalklauseln wie Treu und Glauben als Normbildungsauftrag an die Gerichte figurieren, erlangt damit beschränkt Griffigkeit.[713] Ein solcher Befund ist für den privaten Bereich des DSG, für welchen kein allgemeines Verarbeitungsverbot eine markante Bearbeitungsschranke setzt, kritisch. 475

Denn: Wenn Treu und Glauben sich als primordiale Verarbeitungsvorgabe an die Datenbearbeitenden richtet, die im privaten Bereich grundsätzlich frei in der Verarbeitung sind, und die generalklauselartigen Verarbeitungsgrundsätze die Hauptschranken bilden, für diese indes kaum konkretisierte Handlungsanleitungen konsolidiert werden können, verfehlt der Grundsatz weitgehend eine seiner zentralen Funktionen. Für die datenverarbeitenden Stellen als Adressaten wird der Grundsatz mangels griffiger Konkretisierungen vonseiten der Lehre und Praxis in der Tat zur «Leerformel». 476

710 Vgl. Rosenthal, in: Datenschutz-Forum Schweiz, 69 ff.

711 Insb. relevant im Rahmen der Vertragsauslegung; vgl. m. w. H. Müller, BK-OR, Art. 18, N 50 sowie zur weiteren Kommentarliteratur, insb. auch zu Art. 1 OR; BGE 105 II 1; BGE 133 III 406, E 2.2. in Bezug auf die allgemeinen obligationsrechtlichen Auslegungsregeln zwecks Interpretation eines Erbvertrages.

712 Simitis, NomosKomm.-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 20; vgl. zur schweren Verständlichkeit des Datenschutzrechts selbst für Expertinnen und Experten Hoffmann-Riem, AöR 1998, 513 ff., 516.

713 Zu den Generalklauseln als wichtigen Instrumenten der richterlichen Umbildung des Privatrechts Teubner, 9; kritisch zum Rückzug auf Generalklauseln im Datenschutzrecht unter Bezug auf das Recht auf informationelle Selbstbestimmung Simitis, NJW 1984, 394 ff., 400 f.

477 Nichtsdestotrotz greift es selbst für das Datenschutzrecht zu kurz, Treu und Glauben als inhaltsleere «Stirnschrift» zu bezeichnen. Seine Bedeutung liegt zwar weniger in konkretisierten Handlungsanleitungen gegenüber den personendatenverarbeitenden Stellen, die durch Lehre und Praxis bereitgestellt werden. Vielmehr sind dem Prinzip wichtige Impulse für den *gesetzgeberischen Ausbau* eines hoch ausdifferenzierten Instrumentariums zur Gewährleistung von «Transparenz» zuzuschreiben. Darüber hinaus haben die vorangehenden Ausführungen Elemente herausgearbeitet, die über Treu und Glauben die *Systemrelevanz und Kontextbezogenheit* des Datenschutzrechts sichtbar werden lassen. Das ist für die Weiterentwicklung des Datenschutzrechts von Interesse, zumal Treu und Glauben seit jeher die Rolle eines Motors für die Evaluation des Datenschutzrechts spielte.

2.3. Vertiefung der Entwicklungsimpulse und -linien

2.3.1. Ausbau von Transparenz-, Dokumentations- und Rechenschaftsvorgaben

478 Der Grundsatz von Treu und Glauben ist, wie gezeigt, Impulsgeber für die *Fortentwicklung* datenschutzrechtlicher Vorgaben, namentlich mit Blick auf den Ausbau und die Konkretisierung von *Transparenzvorgaben*. Treu und Glauben präsentiert sich als *Treiber für die Anerkennung von Informations- und Meldepflichten im Datenbearbeitungskontext*. Allerdings greift der Mechanismus der Rechtsfortbildung im Bereich des Datenschutzes, wie diese Studie zeigt, gerade nicht primär und effizient über die Gerichtspraxis.[714]

479 Vielmehr dient Treu und Glauben in erster Linie dem Gesetzgeber als *Vehikel zur Stärkung der Transparenz in Datenbearbeitungsprozessen*. Dass die Gewährleistung von Transparenz ein zentrales Anliegen der Datenschutzgesetzgebung ist, lässt sich als Antwort auf die «undurchsichtigen» Verarbeitungsprozesse sowie die Wahrnehmung der technologischen Prozesse als «Black-Box» lesen. Sie lösen Verunsicherung aus, zumal der Mensch von den Technologien zum Objekt degradiert werde. Verarbeitungsprozesse transparent(er) zu gestalten zielt auch darauf ab, den «Subjektstatus» der Person abzusichern.[715]

714 Vertiefend zum Vollzugsdefizit, mit welchem nicht nur die originäre (Nicht-)Einhaltung, sondern auch die ungenügende behördliche und hierbei insb. gerichtliche Durchsetzung nach Rechtsverletzungen thematisiert wird, dritter Teil, VII. Kapitel, A.2.

715 Zu diesem Zusammenhang die berühmten und viel zitierten Worte des Bundesverfassungsgerichts in seinem Volkszählungsurteil, BverfGE 65, 1, 154 – Volkszählung: «Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer

480 Untrennbar mit Treu und Glauben sowie der Garantie von Transparenz (aber auch Geheimhaltung) ist der Begriff des *Vertrauens* verbunden. Dies zu gewährleisten im Zusammenhang mit Personendatenverarbeitungsprozessen ist neuerdings zu einer wichtigen Aufgabe auch von Unternehmen geworden.[716] An dieser Stelle setzen die jüngsten rechtlichen Entwicklungen mit der Einführung neuer Konzepte und Instrumente an. Namentlich zu nennen sei das Rollenkonzept und die Einführung der Figur des «Verantwortlichen», vgl. Art. 5 lit. j nDSG. Hinzu treten weitere Instrumente wie die Datenschutz-Folgenabschätzung, das Verarbeitungsverzeichnis oder Dokumentations- und Rechenschaftspflichten, welche die Transparenz im Bereich Personendatenverarbeitung operationalisieren sollen. Die Instrumente sollen Verarbeitungsprozesse, Risiken sowie Massnahmen dokumentieren, womit die Konformität der Verarbeitungsprozesse mit den datenschutzrechtlichen Vorgaben navigiert werden soll.

481 Druey war es, der früh statuierte: Treu und Glauben habe eine hohe Relevanz im Informationsrecht – dies artikuliert sich namentlich in einer Kategorie von subjektiven Ansprüchen auf Information resp. reziprok: von Aufklärungspflichten.[717] Der Trend zur Fortentwicklung des Datenschutzrechts mittels Ausbaus von *Transparenzvorgaben,* die ihre Quelle in Treu und Glauben haben, konnte bereits im Rahmen der Teilrevision des DSG verzeichnet werden.[718] Die *Totalrevision* des DSG stärkt den Datenschutz über den Ausbau der Transparenzvorgaben in verschiedene Richtungen.[719] Die Gewährleistung von *Transparenz ist folglich als tragende Säule des Datenschutzrechts und seiner Entwicklungen auszumachen.*

482 *Transparenz* im Datenschutzrecht wird heute und insb. in Zukunft durch ein *Nebeneinander mehrerer Instrumente und Mechanismen*, materieller Rechte und Pflichten sowie prozeduraler und organisatorischer Vorgaben gewährleistet. Als klassisches Instrument gilt das *Auskunftsrecht* der Datensubjekte, vgl. Art. 8 DSG resp. Art. 25 f. nDSG. Zudem steht für das Datenschutzrecht am Anfang bekanntermassen die Anerkennung eines (abstrakten) *Erkennbarkeitsgrundsat-*

unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.»

716 M. w. H. statt mehrerer Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f.; Dies., Schweizer Bank Mai 2018, 21 f.

717 Druey, 315.

718 Meier, N 649.

719 Botschaft DSG 2017–1084, 17.059, 6941 ff., 6944; EJPD, Bericht Begleitgruppe, 3; Rosenthal, Jusletter 16. November 2020, N 92 ff.

zes, Art. 4 Abs. 4 DSG und Art. 6 Abs. 3 nDSG, der in Treu und Glauben sein *Quellrecht* hat. Mit der ersten Teilrevision kamen weiter die Vorschriften über die Anforderungen betreffend eine gültige *Einwilligung* hinzu – vgl. Art. 4 Abs. 5 DSG, der das Instrument des «informed consent» festhält, das sein Hauptanwendungsgebiet im Arzt-, Medizin- und Biomedizinrecht findet.[720] Die Einwilligungsvorgaben finden sich nach Totalrevision in Art. 6 Abs. 6 und Abs. 7 nDSG. Erhöhte Bedeutung kommt gerade auch nach dem Inkrafttreten der DSGVO, aber auch des totalrevidierten DSG den Informationspflichten zu.

483 Aus prozeduraler Sicht seien im Zusammenhang mit Treu und Glauben sowie Transparenz im Datenschutz folgende Instrumente erwähnt, um das Bild abzurunden: Mit der Teilrevision wurde dazumals eine *Registrierungspflicht* für Datensammlungen eingeführt, vgl. Art. 11a DSG. Die Totalrevision wird das Instrument für den privaten Sektor aufgeben. Ein weiteres Instrument zwecks Schaffung von Transparenz ist die *Zertifizierung* gemäss Art. 11 DSG resp. Art. 13 nDSG, ein *Selbstregulierungsansatz:* Indem datenverarbeitende Stellen ihre Bearbeitungsprozesse gegenüber einer unabhängigen Zertifizierungsstelle offenlegen und durchleuchten lassen, wird ebenso Transparenz hergestellt. Die Verleihung eines Gütesiegels, Art. 11 Abs. 2 DSG resp. 13 Abs. 2 nDSG, schafft Transparenz nach aussen.[721] Abrundend zu nennen ist die Möglichkeit von *Abklärungen im privaten Sektor durch den EDÖB*, Art. 29 DSG, wobei er gemäss Art. 30 Abs. 2 DSG seine Empfehlungen und Feststellungen unter Umständen *öffentlich machen* kann.[722]

484 Allgemein ist ein *Akzent der Neuerung* durch die Totalrevision sowie die DSGVO darin zu sehen, dass die «Verantwortlichen» selbst nachhaltig und konkret Massnahmen zu implementieren haben, die *Transparenz* über ihre Verarbeitungsprozesse generieren und diese damit hinsichtlich ihrer Konformität mit Datenschutzvorgaben überprüfbar machen.[723] Das *Paradigma der erhöhten Transparenz* ist eine Konsequenz der Undurchschaubarkeit der informationstechnologischen Verarbeitungshandlungen. Es bleibt paradox, dass der Gesetzgeber als eine Hauptstrategie die Transparenz verfolgt, wohl wissend, dass die technologisch unterstützten Personendatenverarbeitungen kaum durchschaubar sind.

720 Vgl. Körner, in: Simon/Weiss (Hrsg.), 131 ff., 134 ff.; zur Selbstbestimmung im Abtreibungsdiskurs Krähnke, 147 ff.

721 Zu diesem vgl. Belser, in: Weber/Thouvenin (Hrsg.), 143 ff., wobei der Autor einen eigentlichen Mehrwert der Zertifizierung in der Sensibilisierung im Unternehmen verortet, die im Zuge der Zertifizierungsprüfung entsteht, 151; beachte sodann die Verordnung über die Datenschutzzertifizierung vom 27. September 2007, AS 2007 5003.

722 Zu den Kompetenzen des EDÖB nach Totalrevision vgl. Art. 49 ff. nDSG.

723 Zum Paradigmenwechsel, wonach Datenschutz zu einer Aufgabe der Compliance und des Risikomanagements wird sowie zum sog. Accountability-Ansatz, vgl. dritter Teil, VIII. Kapitel, A.2.6. und A.2.7.

Gleichwohl lässt sich feststellen, dass *Treu und Glauben* im Sinne der Schaffung von Rechenschaftsvorgaben, Transparenz sowie Gewährleistung des rechtskonformen Verhaltens datenschutzrechtlich einen starken Entwicklungsanstoss gegeben hat. Der Befund bezieht sich nicht nur auf die Massnahmen zur Erhöhung von Transparenz, sondern auch auf das Ziel, den Datenschutz faktisch griffiger zu gestalten. An dieser Stelle eine *Tour d'Horizon* über die Vorgaben nach den neuen Erlassen, die auch, aber nicht nur das Ziel verfolgen, Transparenz als Element des Datenschutzes auszubauen – Redundanzen an dieser Stelle werden aufgrund der Bedeutsamkeit des Entwicklungstrends in Kauf genommen: 485

Verankert werden *aktive Informationspflichten*, Art. 12 ff. DSGVO (vgl. auch ErwG 39) und Art. 19 nDSG.[724] Mit der Totalrevision beschränkt sich die aktive Informationspflicht nicht länger auf besonders schützenswerte Daten. Gleichwohl ist der Gegenstand der Informationspflicht gemäss Art. 19 nDSG gegenüber dem Regime in der DSGVO weniger nuanciert und detailliert. Die DSGVO differenziert zwischen direkter Erhebung, Art. 13 DSGVO (Personendaten werden beispielsweise im Rahmen des Kundenmeetings direkt beim Kunden erhoben), und indirekter Erhebung, Art. 14 DSGVO (Personendaten werden aus anderen Quellen erhoben).[725] Der Katalog von Angaben, die zum Informationsgegenstand gemacht werden, ist weit gefasst. Er umfasst insb. die vollständigen Kontaktangaben des Verantwortlichen, Angaben zum Datenschutzbeauftragten (sofern eingesetzt), Quellen sowie Kategorien der Angaben, Rechtsgrundlagen für die jeweiligen Bearbeitungen und insb. die berechtigten Interessen, sofern die Bearbeitung auf diesem Legitimationsgrund beruht, alle zur Zeit der Erhebung angestrebten Zwecke in hinreichender Detailliertheit, allfällige Empfänger, ggf. das Thema Auslandstransfer, die Speicherdauer und Kriterien zur Festlegung dieser Dauer (erfordert Löschungskonzept), Hinweise auf die Betroffenenrechte, das Beschwerderecht und Widerspruchsrecht, namentlich auch das Widerrufsrecht der Einwilligung bei den einwilligungsbedürftigen Verarbeitungshandlungen (insb. bei besonders schutzwürdigen Angaben). Zudem ist eine Risikoaufklärung vorzunehmen, mit der betroffene Personen angemessen über Risiken, Vorschriften, Garantien und Rechte sowie deren Ausübung im Zusammenhang mit der Datenverarbeitung informiert werden (ErwG 39). Weiter sind die erforderlichen Angaben bei automatisierten Einzelfallentscheidungen zu erteilen. Die Informierung muss gemäss Art. 13 Abs. 1 DSGVO vor oder bei der Erhebung der Personenda- 486

724 Zu den Neuerungen auch im Zusammenhang mit den Informationspflichten gemäss Totalrevision DSG vgl. Rosenthal, Jusletter vom 16. November 2020, N 92 ff.; Bühlmann/Lagler, SZW 2021, 16 ff.; nach DSGVO Passadelis/Roth, Jusletter vom 4. April 2016, N 6, N 24 ff., N 63 ff.; zur Totalrevision und insb. zur Dokumentation auch Sury, SJZ 2021, 458 ff.; Frei, Jusletter vom 17. September 2018; mit einer Gegenüberstellung von DSGVO und totalrevidiertem DSG Baeriswyl, SZW 2021, 8 ff.

725 Beachte insofern die einschlägige Kommentarliteratur.

ten erfolgen. Eine Ausnahme mit Blick auf den Informierungszeitpunkt gilt für die Direkterhebung, sofern die betroffene Person bereits über die Information verfügt, Art. 13 Abs. 4 DSGVO. Einzuhalten ist zudem eine Pflicht zur Nachinformation gemäss Art. 13 Abs. 3 DSGVO, beispielsweise bei Zweckänderungen. Sodann ist zu beachten, dass die Anforderungen an die Wirksamkeit der Einwilligung, die nach DSGVO ein Erlaubnistatbestand ist, hoch sind, vgl. Art. 6 Abs. 1 lit. a DSGVO. Einwilligungserklärungen müssen verständlich und in klarer sowie einfacher Sprache abgefasst sein, wobei es in der EU etablierte Praxis ist, eigenständige Datenschutzerklärungen in spezifischen Dokumenten vorzusehen. Datenschutzerklärungen im Kleindruck genügen den strengen Vorgaben der DSGVO nicht mehr.[726]

487 Neu sind zudem *umfassende Dokumentations- und Rechenschaftspflichten*, welche den Personendatenverarbeitenden auferlegt werden, vgl. insb. auch Art. 24 DSGVO. Sie zielen nicht nur auf erhöhte Transparenz hinsichtlich der Einhaltung der Datenschutzvorgaben ab, sondern auch darauf, das Datenschutzrecht seiner «formellen» Existenz zu entheben und in der Praxis griffig zu machen («Operationalisierung des Datenschutzrechts»).[727] Herzstück sowohl der *DSGVO* als auch der *Totalrevision des DSG* ist die Pflicht zur Erstellung eines *Verarbeitungsverzeichnisses*, vgl. Art. 30 DSGVO und Art. 12 nDSG. Die Erfassung und Abbildung der Landschaft von Datenverarbeitungsprozessen ist Dreh- und Angelpunkt für die Einhaltung der datenschutzrechtlichen Vorgaben und deren Überprüfung. Das Inventar ist Basisinstrument zur Verwirklichung des breiten Fächers an Instrumenten und Vorgaben, die der Schaffung von Transparenz mit Blick auf Personendatenverarbeitungen dienen. Allgemein verlangt die DSGVO gemäss Art. 24, dass *jederzeit Rechenschaft* über die *Datenschutzkonformität der Verarbeitungstätigkeiten* abgelegt werden können muss, womit auch umfassende Dokumentationspflichten einhergehen. Gesprochen wird vom sog. *Accountability-Ansatz*.[728] Es sind die datenverarbeitenden Stellen, die jederzeit in der Lage sein müssen, darzulegen, dass ihre Verarbeitungstätigkeiten datenschutzrechtlich regelkonform sind. Die Totalrevision des DSG sieht nicht ausdrücklich ein Pendant vor. Allerdings ist davon auszugehen, dass sich auch in der Schweiz ein entsprechender Ansatz als Element der Data Governance durchsetzen wird.

488 *Rechenschaftspflichten* wurden bisher ausserhalb des Datenschutzrechts insb. für Konstellationen vorgesehen, in denen jemand ein Geschäft für einen anderen erledigt.[729] Die Person, die das Geschäft für einen anderen besorgt, kennt sich

726 Vgl. Passadelis/Roth, Jusletter vom 4. April 2016, N 22.
727 Hierzu Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f.; vertiefend dritter Teil, VIII. Kapitel, A.2.5.
728 Vgl. Art. 24 DSGVO; Hartung, BeckKomm-DSGVO, Art. 24 N 20; vgl. zum Accountability-Ansatz und zum Data Mapping Schröder, digma 2020, 16 ff.; Sury, SJZ 2021, 458 ff., 462 f.
729 Die folgenden Ausführungen basieren auf Druey, 230.

in aller Regel in der Sache besser aus, verfügt über eine spezifische Expertise und kennt die Usanzen der Branche. Rechenschaftspflichten überbrücken eine Distanz, in der die Geschäftsherrin zu ihrer Angelegenheit infolge unzureichender Ressourcen (Expertise, Zeit, Nähe) steht. Die geschäftsführende Person legt zudem gegenüber der beauftragenden Person wie auch gegenüber sich selbst Rechenschaft darüber ab, dass sie sich bewusst ist, mit der Besorgung eines fremden Geschäftes resp. der Verwaltung eines fremden Gutes betraut zu sein. Weiter beinhaltet die Rechenschaft eine bewertende Überprüfung, ob die Handlungen in Einklang mit den normativen Erwartungen und Vorgaben stehen. Zugleich gelten Rechenschaftspflichten als *Entlastungsstrategie*:[730] Die Geschäftsherrin ersucht darum, den Eindruck zu erlangen, dass ihre Angelegenheit in guten Händen, der Geschäftsgang regelmässig ist. Sie tut dies im Sinne eines Appells an das erwiesene *Vertrauen*. Die geschäftsführende Person liefert mit der Rechenschaft ggf. auch den Beleg, sich des Vertrauens würdig zu erweisen. Verweigerte, ausweichende, lückenhafte, widersprüchliche Rechenschaftsauskünfte gelten als Hinweise, wonach ein Prozess oder Vorgehen nicht regelkonform ist. Sie geben Anlass, allfällige Defizite aufzudecken. Die regelmässige Rechenschaft ermöglicht es, Zeitpunkt, Inhalt, Ort und Ansatz defizitärer Entwicklungen zu lokalisieren. Bestätigen sich Fehlentwicklungen, wird in der Regel nicht nur das Vertrauen, sondern auch das Geschäft entzogen. Rechenschaftspflichten und -rechte sind folglich hocheffiziente und zugleich niederschwellige *Kontrollinstrumente*. Sie verzichten (vorab) auf eine rigide, engmaschige, interventionistische Kontrolle, die eine effiziente Geschäftsführung im Ergebnis behindern. Vielmehr geht das Konzept der Rechenschaft davon aus, was sowohl Treu und Glauben als auch die Expertise des Geschäftsführenden nahelegen: Ausgangspunkt ist die Annahme eines *redlichen Verhaltens*, eines vertrauensvollen Umgangs im Allgemeinen; reflektiert wird die Vertrauenswürdigkeit mit Blick auf Kenntnisse, Ernsthaftigkeit und Umsicht eines Experten oder einer Expertin. Als Garanten für die Expertise kommen sodann nicht zuletzt Ausbildung, Diplome, Standesregeln usf. zum Einsatz.[731]

Entsprechende Ideen werden jüngst datenschutzrechtlich rezipiert, sind es doch 489
an *erster Stelle* die Verarbeitenden, die dafür sorgen können und müssen, dass ihre Personendatenverarbeitungen den datenschutzrechtlichen Vorgaben entsprechen. Die DSGVO verankert unter dem Titel «*Verantwortung des für die Verarbeitung Verantwortlichen*» in Art. 24 DSGVO einen eigentlichen Generalauftrag des Verantwortlichen zur Gewährleistung der Datenschutz-Compliance.[732] Den Verantwortlichen obliegt es, dokumentieren zu können, dass ihr Handeln im Ein-

730 Druey, a. a. O.
731 Teubner, in: Brüggemeier (Hrsg.), 303 ff., 318 ff.
732 Raschauer, NomosKomm-DSGVO, Art. 24 N 10.

klang mit den datenschutzrechtlichen Vorgaben steht. Mit den jüngsten datenschutzrechtlichen Neuerungen werden folglich an erster Stelle die *Personendatenverarbeitenden* in die Pflicht genommen, wobei diese in Bezug auf die Einhaltung der datenschutzrechtlichen Vorgaben und die getroffenen Massnahmen dokumentations- und rechenschaftspflichtig sind.[733]

490 Dieser *neue Accountability-Ansatz* steht in einem engen Zusammenhang zu Treu und Glauben. Datenschutzrechtlich betrachtet lässt sich damit weiter feststellen: Zum einen lässt sich der Accountability-Ansatz in einer individualrechtlichen Richtung sehen, indem die entsprechenden Dokumentationen auch der Umsetzung und Gewährleistung der Betroffenenrechte dienen. Zum anderen wird sichtbar, dass der Datenschutz mit diesem Ansatz zu einer Aufgabe im Interesse der Good Governance der jeweiligen Unternehmen, Organisationen resp. Institutionen wird.

491 Im Rahmen der Relevanz von Treu und Glauben, der erhöhten Transparenz sowie der Aufgabe, die Datenschutz-Compliance und Data Governance zu installieren, ist auf das Instrument der *Datenschutz-Folgenabschätzung* hinzuweisen: Dort, wo Datenbearbeitungen mit einem erhöhten Risiko für Persönlichkeitsverletzungen einhergehen, muss eine entsprechende Analyse erstellt werden, die auf Verlangen der Datenschutzaufsichtsbehörde resp. dem EDÖB vorgelegt werden soll, vgl. Art. 35 DSGVO und Art. 22 nDSG.

492 Ein jüngeres spezifisches Aktivitätsfeld von Treu und Glauben lässt sich im *Umgang mit sog. Datensicherheitsvorfällen mit ihren entsprechenden Notifikationspflichten* verorten, vgl. Art. 33 f. DSGVO und Art. 24 nDSG.[734] Bis zum Inkrafttreten der Totalrevision wurde eine sinngemässe Informationspflicht aus Art. 4 Abs. 2 erster Satzteil DSG abgeleitet, womit sich die rechtsfortbildende Kraft von Treu und Glauben im Datenschutzrecht bestätigt. Der Hauptimpuls für die Integration einer ausdrücklichen gesetzlichen Notifikationspflicht nach totalrevidiertem DSG scheint indes von der DSGVO auszugehen: Die DSGVO statuiert eine entsprechende Meldepflicht gemäss Art. 33 f. Hierbei legt Art. 33 DSGVO die Notifikation an die Behörden nieder, Art. 34 DSGVO darüber hinausgehend die

733 Ein Beispiel soll das Erörterte datenschutzrechtlich umreissen: Die DSGVO verankert einen extraterritorialen Ansatz, vgl. Art. 3 Abs. 2 lit. a und lit. b DSGVO, womit auch Unternehmen in der Schweiz in ihren Anwendungsbereich fallen können. Viele Fragen sind derzeit mit Blick auf die Tatbestandselemente des Anwendungsbereiches unklar. Indes erscheint es geboten, für Schweizer Unternehmen mit EU-Ausrichtung eine Basisanalyse vorzunehmen, in welcher die Frage erörtert wird, ob und inwiefern man in den Anwendungsbereich der DSGVO fällt. Wird die Anwendbarkeit der DSGVO aufgrund einer entsprechenden Analyse verneint und kommt indes eine Europäische Behörde zu einem anderen Ergebnis, wird die Verantwortlichkeit des Verantwortlichen anders beurteilt werden als diejenige eines Verarbeitenden, der keine entsprechende Analyse vorgenommen hat; vgl. Pfaffinger, in: Emmenegger (Hrsg.), 17 ff.; zur Accountability resp. Ablegung von Rechenschaft auch Cichocki, Jusletter IT vom 21. Mai 2015, N 49 ff.

734 Vgl. Rosenthal, HK-DSG, Art. 4 N 16; Meier, N 657.

Benachrichtigung an die Datensubjekte, sofern ein qualifiziertes Risiko mit der Verletzung des Schutzes von Personendaten einhergeht.

493 Mehrere weitere Transparenzinstrumente vervollständigen die Landschaft: Im Zusammenhang mit der Totalrevision sind die Vorgaben im Zusammenhang mit den automatisierten Einzelfallentscheidungen zu nennen, vgl. z. B. Art. 21 nDSG. Auch Zertifizierungen zielen darauf ab, die Transparenz von Datenverarbeitungen zu verbessern sowie die Einhaltung der datenschutzrechtlichen Vorgaben zu erhöhen.[735] Im Rahmen des Zertifizierungsverfahrens wird sachkundig die Konformität der Datenverarbeitungen der sich ihm freiwillig unterwerfenden Verantwortlichen überprüft und ggf. Verbesserungspotential aufgezeigt. Erfolgt der Nachweis der Rechtskonformität, wird ein Zertifikat ausgestellt, das als Gütesiegel nach aussen den Datensubjekten und Konsumentinnen, Klientinnen, Versicherten usf. das erfolgreich durchlaufene Prüfungsverfahren ausweist. Im Ergebnis vermittelt man damit auch den Datensubjekten, die den datenverarbeitenden und zertifizierten Unternehmen in verschiedenen Rollen begegnen, die Information und daraus folgend das Vertrauen, dass das Unternehmen den Datenschutz ernst nimmt und sich datenschutzkonform aufstellt. Die Datensubjekte, denen weiterhin Individualrechte inklusive Haftungsansprüche infolge von Datenschutzverstössen zukommen, erlangen mit dem Zertifikat resp. dessen Fehlen eine bedeutsame Entscheidungsgrundlage für die Gestaltung ihrer Geschäftsbeziehungen. Das Instrument ist in anderen Bereichen, z. B. in der Lebensmittel- oder Textilbranche, gut etabliert. Es dient nicht nur der Qualitätssicherung; vielmehr dient es auch dazu, Konsumentinnen und Konsumenten die Informationen zu vermitteln, um informierte und verantwortungsvolle Entscheidungen zu treffen.

494 *Zusammenfassend* lässt sich feststellen, dass *Treu und Glauben eine treibende Kraft im Zusammenhang mit der Rechtsfortbildung ist,* namentlich in Bezug auf die Anerkennung und den Ausbau von Transparenzvorgaben. Das Prinzip der Transparenz, das untrennbar mit dem Gebot von Treu und Glauben in Verbindung steht, wird namentlich im Zuge der DSGVO, aber auch der Totalrevision des DSG mit einem dichten Netz *unterschiedlicher Instrumente* ausgebaut: mittels aktiver Informationspflichten, Meldepflichten, ggf. Register, Auskunftsrechten, Dokumentations- und Rechenschaftspflichten, aber auch Zertifizierungsverfahren. Der *Trend*, im Rahmen des Datenschutzes über Treu und Glauben *Transparenzerfordernisse* und Rechenschaftsinstrumente, verknüpft mit prozeduralen und organisatorischen Massnahmen auszubauen, *entspricht den Erwartungen einer Wissens- und Informationsgesellschaft*.[736] Wenn im Zuge der

735 Vgl. Raschauer, NomosKomm-DSGVO, Art. 42 N 1.

736 Vgl. zum Trend im Familienrecht, Informationsrechte sukzessive auszubauen, Pfaffinger, FamPra.ch 2014, 604 ff.; vgl. mit Blick auf Informationspflichten in einem spezifischen Kontext, dem

jüngsten Neuerungen die Transparenz- und Rechenschaftsvorgaben durch mehrere neue Instrumente, die sich als «Umsetzungsinstrumente» beschreiben lassen, gesetzlich ausgebaut werden, dann darf zugleich angenommen werden, dass Treu und Glauben als allgemeiner und abstrakter Verarbeitungsgrundsatz und Auffangtatbestand an Bedeutung verlieren wird.

2.3.2. Integration kontextueller Erwägungen

495 Neben der Bedeutung von Treu und Glauben im Kontext der *Gewährleistung von Transparenz* ist ein *weiterer Aspekt von diesem Grundsatz* mitgeprägt. Der Zugriff auf diesen zweiten Aspekt erfolgt seinerseits über die soeben beleuchtete Transparenz- und Informationsthematik im Zusammenhang mit Treu und Glauben. Der Ausbau der Informationspflichten und damit der Transparenz ist, wie dargelegt, ein Kernanliegen der Totalrevision.[737]

496 Bislang wurde in der Schweizer Lehre im Rahmen des noch geltenden Datenschutzgesetzes aus dem Bearbeitungsgrundsatz von Treu und Glauben ein Informationsrecht resp. eine Informationspflicht wie folgt abgeleitet: Aus dem Grundsatz von Treu und Glauben gemäss Art. 4 Abs. 2 DSG könne eine *Informationspflicht gegenüber Datensubjekten* («den Betroffenen») hinsichtlich Datenbearbeitungen resultieren, sofern diese *angesichts der konkreten Umstände aus Loyalitätserwägungen geboten erscheine*.[738]

497 An dieser Stelle soll die Bedeutung und Einschlägigkeit von «vernünftigen Erwartungen», die eng mit Treu und Glauben verbunden sind, im Lichte der Umstände von Personendatenverarbeitungen angesprochen werden. Der Aspekt hat in der Datenschutzdebatte der Schweiz bislang keine besondere Aufmerksamkeit gefunden.

498 Ganz anders präsentiert sich die Situation in den USA, wo die Doktrin der *«reasonable expectations of privacy»* Gegenstand zahlreicher Gerichtsentscheide bildet.[739] Sie wird als Instrumentarium eingesetzt, um Privacy-Herausforderungen, die sich infolge des Einsatzes neuer Technologien ergeben, zu bewältigen. Die Rechtsfigur findet über die Rechtsprechung des EGMR zu Art. 8 EMRK auch im europäischen Rechtsraum Einsatz.[740] Aber auch im Zusammenhang mit der

---

Bankenbereich, und zu Informationspflichten des Bankiers, abgeleitet aus Art. 2 ZGB, Emmenegger, in: Chappuis/Winiger, 67 ff., 70.

737 Vgl. BBl 2017–1084, 17.059, 6941 ff., 6944 und 6972 ff.

738 Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.72.

739 Mit Hinweisen auf das Urteil Katz v. United States und das Votum von Justice Harlan Nissenbaum, 241.

740 Hierzu vertiefend dritter Teil, IX. Kapitel; dazu, dass in Grossbritannien Prominente lange quasi Freiwild waren für die Regenbogenpresse, diese Situation sich allerdings mit dem Entscheid Campbell v. Mirror Ltd. änderte, wobei das Gericht seine Argumentation auf die *«reasonable expectations of privacy»* stützte, Hoppe, ZUM 2005, 41 ff., 43.

DSGVO findet die Konstruktion Erwähnung. Eine vertiefende Auseinandersetzung mit diesem Ansatz wird im dritten Teil dieser Arbeit erfolgen.[741]

Zu vermerken ist, dass sich die *«reasonable expectations of privacy»* nicht auf eine individuelle, subjektive Sicht und Einschätzung des adressierten Individuums beschränken. Vielmehr wird über die Figur eine objektive sowie gesellschaftliche Komponente integriert. Die *Vernünftigkeit der Erwartung* wird ihrerseits anhand der jeweiligen *spezifischen gesellschaftlichen Kontexte* mit den sie mitstrukturierenden Erwartungen eruiert. Es ist somit die Verletzung von kontextrelativen Normen, die als Verstoss gegen vernünftige Privacy-Erwartungen taxiert wird.[742] 499

In Europa zeigt sich der Einfluss kontextueller Erwägungen über die Figur der vernünftigen Privatheitserwartungen in einem Dokument der WP 29 zur DSGVO, der «Opinion 2/2017 on data processing at work». Das Dokument befasst sich bereichsspezifisch mit Fragen des Datenschutzes und der Datenschutz-Grundverordnung im Arbeitskontext: 500

> «This opinion makes a new assessment of the balance between legitimate interests of employers and the reasonable privacy expectations of employees by outlining the risks posed by new technologies and undertaking a proportionality assessment of a number of scenarios in which they could be deployed.»[743]

Über die Figur wird darauf abgezielt, im Vorfeld vom konkret betroffenen Datensubjekt in seiner Rolle als Arbeitnehmer zu abstrahieren und zugleich bereichsspezifisch anhand von Szenarien die Auswirkungen bestimmter Personendatenverarbeitungsprozesse zu evaluieren. Treu und Glauben und die daran ankoppelbaren «vernünftigen Erwartungen» des Datensubjektes lassen sich somit als Einfallstor bezeichnen, über welches die *Relevanz des Verarbeitungszusammenhanges und -kontextes* in die datenschutzrechtlichen Erwägungen integriert wird.[744] 501

Wenn aus dem Verarbeitungsgrundsatz von Treu und Glauben Informationspflichten angesichts der Umstände aus Loyalitätserwägungen abgeleitet wurden, schliesst das die Anerkennung ein, wonach *kontextrelative Erwägungen für das Datenschutzrecht* einschlägig sind. Die vernünftigen Erwartungen des Datensubjektes sind indes im Rahmen von Personendatenverarbeitungen differenziert, die vernünftige Person keine einheitliche Figur.[745] Vielmehr hängen sie vom *Verarbeitungszusammenhang* ab, vom jeweiligen gesellschaftlichen Kontext, in welchen 502

741 Vgl. auch Paefgen, 33 ff.; vertiefend dritter Teil, IX. Kapitel.
742 Nissenbaum, 233.
743 Vgl. <ec.europa.eu/newsroom/document.cfm?doc_id=45631, 3> (zuletzt besucht am 30. April 2021).
744 Auf die Bedeutung des Verarbeitungszusammenhanges und der Relationen, in denen Informationsverarbeitungen stattfinden, wies früh bereits Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 30, hin, wobei sich sein Fokus gleichwohl auf die Person als Subjekt richtet.
745 Zum vernünftigen Menschen als (hypothetische) Figur des Obligationenrechts vgl. Gauch, in: Steinauer (Hrsg.), 177 ff., 179 auch zu verschiedenen Rollen.

die Personendatenverarbeitungen eingebettet sind, und von den Rollen, in denen agiert wird.[746]

503 Die Korrelation zwischen Treu und Glauben und der Beachtlichkeit kontextueller Bezüge von Personendatenverarbeitungen deutet sich im Logistep-Fall an. Es waren der EDÖB und das Bundesverwaltungsgericht, nicht aber das Bundesgericht, die Treu und Glauben sowie die Umstände zur Beurteilung beizogen. Wie bereits dargestellt, handelte es sich um einen Konflikt zwischen Privaten. Hierbei wurde die Logistep AG vertraglich damit beauftragt, Personen resp. deren Surfverhalten auszuspionieren, um damit Urheberrechtsverletzungen aufzudecken. Im Ergebnis nahmen Private eine Aufgabe wahr, die der Strafverfolgung der öffentlichen Hand vorbehalten sein soll. Das Vorgehen wurde, wie dargetan, als Verstoss gegen datenschutzgesetzliche Vorgaben taxiert. Das Bundesverwaltungsgericht hielt fest, dass Personendaten nicht in einer Art erhoben werden dürfen, mit der die betroffene Person nicht rechnen musste. Mit anderen Worten: Geheime Ausforschungen eines privaten Lebensbereiches aus ökonomischen Interessen und zwecks Strafverfolgung durch Private wurden als Verstoss gegen den Verarbeitungsgrundsatz von Treu und Glauben taxiert, weil die betroffenen Personen damit nicht rechnen mussten. Die Konstellation des Logistep-Falles ist übrigens der bei den Versicherungsbetrugsfällen und den dort erfolgenden Observationen ähnlich.[747] Der letzte Teil dieser Arbeit wird sich zwecks Entwicklung eines Vorschlages zur Rekonfiguration eines Datenschutzrechts der Zukunft vertieft damit befassen.

504 Die getätigte Analyse führt vor Augen, dass bereits unter geltendem Recht, namentlich auch über «Treu und Glauben», die *vernünftigen Erwartungen* der von Personendatenverarbeitungen betroffenen Personen adressiert werden. Als Verarbeitungsgrundsatz und Handlungsanleitung an die personendatenverarbeitenden Stellen allerdings bleibt Treu und Glauben wenig ergiebig, namentlich, weil weder über die Praxis noch Lehre konkrete Konsolidierungen des sehr abstrakten Grundsatzes generiert werden. Treu und Glauben beschränkt sich insofern für das Datenschutzrecht auf eine flankierende Rolle an den äussersten Rändern, wie es Treu und Glauben, namentlich aber dessen Spiegelbild, dem Rechtsmissbrauchsverbot, entspricht.

505 Es ist nunmehr auf den zweiten in Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG niedergelegten Verarbeitungsgrundsatz, das Verhältnismässigkeitsprinzip, einzugehen. Auch zu diesem gibt es markige Einschätzungen:

746 Hierzu vertiefend Nissenbaum, 129 ff.; Simitis, in: Schlemmer (Hrsg.), 67 ff., 74 f.

747 Blick, Aargauer Justizdirektor ist gegen das Schnüffler-Gesetz, Zürich 2018, <https://www.blick.ch/politik/unterstuetzung-fuer-sybille-berg-und-co-aargauer-justizdirektor-ist-gegen-das-schnueffler-gesetz-id8247397.html> (zuletzt besucht am 30. April 2021).

«Der Grundsatz der Verhältnismässigkeit scheint heute in der Welt des Rechts omnipräsent zu sein.»[748]

Fest steht: Für das duale Regime des DSG ist die Voranstellung eines Verhältnismässigkeitsprinzips, das ebenso für Personendatenverarbeitungen im privaten Bereich gilt, erklärungsbedürftig. 506

3. Das Verhältnismässigkeitsprinzip

3.1. Aspekte und kontextualisierte Analyse

> «Der Grundsatz der Verhältnismässigkeit hat eine spektakuläre Erfolgs- und Rezeptionsgeschichte hinter sich. Von seinen eher diffusen verwaltungsrechtlichen Ursprüngen hat er sich unter dem Grundgesetz zu einem der zentralen Elemente der Grundrechtsdogmatik emanzipiert und greift auch in andere Bereiche, nicht nur des Verfassungsrechts, aus.»[749]

Im DSG ist das Verhältnismässigkeitsprinzip als «gemeinsamer» Verarbeitungsgrundsatz gleichermassen für den öffentlichen wie den privaten Sektor zusammen mit Treu und Glauben in Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG niedergelegt.[750] Rosenthal weist dem Prinzip eine Art «Scharnierposition» zu, wonach dieses nicht nur eng mit dem Zweckbindungsgrundsatz verknüpft sei, sondern sich stattdessen ebenso mit weiteren Grundsätzen überschneiden könne.[751] 507

In der Lehre wird dem Grundsatz hohe praktische Relevanz zugewiesen. Gleichwohl gilt er als der am häufigsten verletzte Grundsatz.[752] Die Sichtung der vorhandenen (rudimentären) Gerichts- und Verwaltungspraxis sowie der Wissenschaft zeigt, dass das Verhältnismässigkeitsprinzip als datenschutzrechtlicher Verarbeitungsgrundsatz für den öffentlichen wie den privaten Sektor *identisch interpretiert wird*. Die Botschaft von 1988 gab bereits eine eindeutige Anweisung: 508

> «Mit dem in diesem Absatz statuierten Verhältnismässigkeitsgebot wird das im öffentlich-rechtlichen Bereich ohnehin geltende Verhältnismässigkeitsprinzip auch für den privaten Bereich als anwendbar erklärt. Der Datenbearbeiter ist demnach gehalten, nur diejenigen Daten zu erheben und weiter zu bearbeiten, die für einen bestimmten Zweck geeignet sind und die er tatsächlich benötigt. Wer z. B. Autos vermietet, darf zwar die Personalien des Mieters erheben; übermässig wäre es aber, wenn der Mieter zusätzlich Auskünfte über seine Familienverhältnisse oder seine Beziehungen zu weiteren Drittper-

748 Jestaedt/Lepsius (Hrsg.), Vorwort, VII.
749 Von Arnauld, in: Jestaedt/Lepsius (Hrsg.), 261 ff., 276.
750 Vgl. zum Grundsatz der «Datenminimierung» auch Art. 5 Abs. 1 lit. c DSGVO; jüngst erwähnt in BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 3; zu den Erwägungen des Gerichts in Bezug auf die verschiedenen Vorgaben gemäss DSG Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f. und zur Empfehlung des EDÖB Dies., digma 2018, 154 ff.; Vasella/Ziegler, digma 2019, 80 ff.; Pärli, SZS 2018, 107 ff. kritisch zur verordneten Selbstverantwortung.
751 Rosenthal, HK-DSG, Art. 4 N 26.
752 Ders., HK-DSG, Art. 4 N 19 und N 27; Meier, N 669.

> sonen verlangt. Bei Kreditauskünften wiederum können neben Angaben über Vermögensverhältnisse und Zahlungsmoral auch die Familienverhältnisse wesentlich sein; übermässig wären aber Auskünfte über die Religionszugehörigkeit oder politische Auffassungen der überprüften Person. Des Weiteren muss aber auch zwischen dem Bearbeitungszweck und der mit Blick darauf nötigen Persönlichkeitsbeeinträchtigung ein vernünftiges Verhältnis bestehen. So ist es etwa unzulässig, im Hinblick auf einen Wahlkampf das Privatleben eines politischen Gegners umfassend und systematisch auszuforschen.»[753]

509 Das Verhältnismässigkeitsprinzip kann entsprechend als «Import» vom öffentlichen Recht in das Privatrecht bezeichnet werden. Personendatenverarbeitungen durch öffentliche Stellen des Bundes wie durch Private müssen *geeignet* sein, einen fixierten Zweck zu erreichen, und insofern *erforderlich* sowie *verhältnismässig im engeren Sinne*.[754] Die Trias der Verhältnismässigkeit, wie sie für das öffentliche Recht entwickelt wurde, gilt im Datenschutzrecht für den privaten Bereich gleichermassen: Demnach muss im privaten Sektor die Art und Weise jeder Personendatenverarbeitung zur Verwirklichung eines bestimmten Zwecks objektiv geeignet und notwendig sein; zudem soll der angestrebte Zweck in einem vernünftigen Verhältnis zu den Beeinträchtigungen stehen.[755]

510 Die *datenschutzrechtliche Verhältnismässigkeit* wird vorab *generisch als prinzipielle Verhältnismässigkeit* umrissen: Angeführt werden hierbei die Gebote der Datensparsamkeit und -minimierung sowie das Verbot der Vorratsdatensammlung, vorbehältlich seiner Durchbrechung mittels ermächtigender gesetzlicher Grundlage.[756]

511 Meier beschreibt als ein *Unterprinzip* des allgemeinen Verhältnismässigkeitsgebots die *materielle Verhältnismässigkeit*. Unter dem Begriff thematisiert er die Art der Verarbeitungsmethode und die Ausbreitung der gesammelten Personendaten über verschiedene Felder hinweg, im Sinne des Zugriffes von einem Kontext auf einen anderen.[757]

512 Als weiteres *Unterprinzip* wird die *temporelle Verhältnismässigkeit* genannt. Hierbei wird allem voran danach gefragt, wie lange Datenbestände gespeichert werden dürfen resp. wann eine Löschung oder Anonymisierung angezeigt ist.[758] Die Löschung von Personendaten ist folglich nicht nur und nicht erst aufgrund der Geltendmachung des entsprechenden Betroffenenrechts vorzunehmen, son-

753 BBl 1988 II 414 ff., 450.
754 Hierzu namentlich Maurer-Lambrou/Steiner, Art. 4 N 11; Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.78 ff.; Rampini, BK-DSG, Art. 12 N 4.
755 Vgl. Pedrazzini, in: Schweizer (Hrsg.), 19 ff., 27; Steinauer, in: Schweizer (Hrsg.), 43 ff., 45; zum Verhältnismässigkeitsprinzip sodann BBl 1988 II 414 ff., 450 und BBl 2017–1084, 17.059, 6941 ff., 7026 f.
756 Vgl. Meier, N 633 und N 661 ff.; Bolliger/Féraud/Epiney/Hänni, 12; Rosenthal, HK-DSG, Art. 4 N 19 ff.; vgl. zudem Bereits, 132 ff.
757 Meier, N 676 ff.
758 Hierzu neben Ders., N 679 f. weiter auch Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.79; ein Verfallsdatum für Daten schlägt Mayer-Schönberger, Delete, 201 ff. vor.

dern stets dann, wenn die Verhältnismässigkeit entfällt. In diesem Zusammenhang sind Vorgaben aus anderen Rechtsbereichen zu beachten, namentlich Archivierungspflichten, wie sie für verschiedenste Bereiche anerkannt sind.[759] Die Totalrevision des DSG greift diesen temporellen Aspekt ausdrücklich mit Art. 6 Abs. 4 nDSG auf. Entsprechend ist nach Totalrevision das Verhältnismässigkeitsprinzip an zweierlei Stellen, Art. 6 Abs. 2 und Art. 6 Abs. 4 nDSG, verankert.[760]

513 Die griffigste Konkretisierung zum datenschutzrechtlichen Verhältnismässigkeitsprinzip findet sich bei Rosenthal: Der Grundsatz setze vorab, gemeinsam mit dem Zweckbindungsgrundsatz, das datenschutzrechtliche *Prinzip der Datensparsamkeit* resp. das *Need-to-know-Prinzip* um.[761] So verbietet das Kriterium der Erforderlichkeit das Sammeln von Daten, das in sachlicher, zeitlicher, räumlicher oder persönlicher Hinsicht objektiv über das zur Zweckerreichung Notwendige hinausgeht.[762] Vorratsspeicherungen sind also nicht verhältnismässig, da diese Verarbeitungshandlungen gerade keinen bestimmten Zweck verfolgen. Zudem verlangt der Grundsatz eine wiederholte Überprüfung der Personendatenbestände.[763]

514 Ursprünglich wurde der Verhältnismässigkeitsgrundsatz, wie eingangs zitiert, im öffentlichen Recht installiert. In der Schweiz gilt der Grundsatz allgemein aufgrund von Art. 5 Abs. 2 BV, sodann Art. 36 Abs. 3 BV. Das Prinzip zielt darauf ab, staatliche Macht gegenüber den Bürgerinnen und Bürgern zu regulieren; das *Verhältnis Bürger – Staat ist ein asymmetrisches*. Das Verhältnismässigkeitsprinzip spielt seit jeher eine Schlüssel- oder Hauptrolle im öffentlichen Recht.

515 Anders kommt ihm im Privatrecht eine *Nebenrolle* zu. Im Aufsatz von Kähler mit dem humoristischen Titel «Raum für Masslosigkeit. Zu den Grenzen des Verhältnismässigkeitsgrundsatzes im Privatrecht» ist zu lesen:

> «So triumphal der Siegeszug des Verhältnismässigkeitsprinzips im öffentlichen Recht verlaufen ist, so klar sind ihm im Privatrecht Grenzen gesetzt.»[764]

516 Die Bedeutung des Verhältnismässigkeitsprinzips im nicht-öffentlichen Bereich ist folglich keineswegs trivial. Ein *funktionales Äquivalent* findet das Verhältnismässigkeitsprinzip im Privatrecht in erster Linie im *Rechtsmissbrauchsverbot gemäss Art. 2 Abs. 2 ZGB*. Allerdings formuliert der privatrechtliche Rechtsmissbrauch die *Grenzen deutlich weiter aussen*, als es das öffentlich-rechtliche Verhältnismässigkeitsgebot tut: Nach Art. 2 Abs. 2 ZGB ist es das «krass stossende Verhal-

759 Zum Datenschutzrecht, seinen Grundprinzipien und den Herausforderungen der Archivierung vgl. Husi-Stämpfli/Gisler, in: Epiney/Nüesch (Hrsg.), 103 ff., insb. 110 ff.
760 Hierzu Rosenthal, Jusletter vom 16. November 2020, N 33 f. und N 51.
761 Vgl. Ders., HK-DSG, Art. 4 N 19 ff.; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 11.
762 Rampini, BSK-DSG, Art. 4 N 11; zum Ganzen Rosenthal, HK-DSG, Art. 4 N 20 ff.
763 Peter, 134.
764 Kähler, in: Jestaedt/Lepsius (Hrsg.), 210 ff., 233.

ten», das untersagt wird.[765] Zur Konkretisierung von Art. 2 Abs. 2 ZGB wurden verschiedene Fallgruppen strukturiert.[766]

517 Die Verhältnismässigkeit ist für das Privatrecht im Zusammenhang mit dem Grundsatz der Privatautonomie zu sehen: Dem Grundsatz der Privatautonomie mit seinen verschiedenen Aspekten (z. B. Vertragsfreiheit) setzt der Privatrechtsgesetzgeber in erster Linie mittels *zwingenden Rechts Schranken*. Solche Schranken qua zwingendem Recht finden sich namentlich im sog. sozialen Privatrecht und hierbei im privatrechtlichen Arbeitsrecht oder Mietrecht, zudem im Konsumentenschutzrecht.

518 Weiter ist zur Erfassung der Bedeutung des Verhältnismässigkeitsprinzips mit privatrechtlichen Bezügen in Feldern wie dem Kindes- und Erwachsenenschutz[767] oder im Kartell- und Wettbewerbsrecht anzusiedeln.[768] – Rechtsgebiete, welche vor Augen führen, dass die Idee einer scharfen Trennung zwischen öffentlichem und privatem Recht rein theoretischer Natur ist.

519 Erwägungen zur *Verhältnismässigkeit* fliessen folglich m. E. in Konstellationen *struktureller Ungleichgewichte und Asymmetrien in gesellschaftlichen Beziehungen* in das Privatrecht ein.

520 Dies ist der Hintergrund, vor dem sich der Verhältnismässigkeitsgrundsatz als gemeinsames Verarbeitungsprinzip für den privaten und öffentlichen Bereich gemäss Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 und Abs. 4 nDSG verstehen lässt. Aufgrund der in Personendatenverarbeitungszusammenhängen, unterstützt durch neue Technologien, verorteten *Machtasymmetrien* zwischen Verarbeitenden – ungeachtet der Frage, ob es öffentliche Stellen oder private Personen sind – liegt die Begründung für den Transfer des Verhältnismässigkeitsprinzips vom öffentlichen Bereich in den privaten Bereich. Der Grundsatz wird datenschutzrechtlich konsequent ebenso für den Bereich der privaten Datenbearbeitung analog der öffentlich-rechtlichen Struktur – Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne – interpretiert.[769] Insofern liesse sich von einer *monistischen Interpretation* sprechen. Ob der Verhältnismässigkeitsgrundsatz im *Lichte des Dualismus* für die beiden Bereiche gemäss DSG und nDSG datenschutzrechtlich *unter-*

765 Vgl. Riemer, § 5 N 14; vgl. BGE 125 II 275, E 2.c., wonach «der formalen Rechtsordnung eine ethisch materielle Schranke» gesetzt wird, wo «durch die Betätigung eines behaupteten Rechts offenbares Unrecht geschaffen würde», vgl. BBl 1904 IV 14.

766 Insofern sei auf die zivilrechtliche Kommentarliteratur und die einschlägige Rechtsprechung verwiesen.

767 Beschränkungen des persönlichen Verkehrs beispielsweise haben verhältnismässig in dem Sinne zu sein, dass sie geeignet und erforderlich sind, um das Kindeswohl zu schützen, Art. 273 ZGB; Michel, KuKo-ZGB, Art. 273 N 19; allgemein Cottier, KuKo-ZGB, Vor Art. 307–317, N 7.

768 Vgl. Urteil des EuGH, C-441/07 P, Urteil vom 29. Juni 2019 – Alrosa.

769 Vgl. BBl 1988 II 414 ff., 450; Rosenthal, HK-DSG, Art. 4 N 19 ff.; Rampini, BSK-DSG, Art. 4 N 9, mit Hinweis in N 10 auf die Partikularität der Übernahme dieses öffentlich-rechtlichen Grundsatzes im Bundeszivilrecht.

schiedlich zu interpretieren sei, wurde bislang nicht grundlegend diskutiert.[770] Die Ansicht, wonach der Inhalt des Verhältnismässigkeitsprinzips in seiner gemeinsamen Verankerung in Treu und Glauben für den privaten Bereich im Sinne des Rechtsmissbrauchs zu lesen wäre, wird – soweit ersichtlich – nicht vertreten. Vielmehr wird das Verhältnismässigkeitsprinzip identisch für den privaten Bereich wie für den öffentlichen Bereich interpretiert, und zwar, wie gezeigt, im Sinne des öffentlich-rechtlichen Prinzips. Damit trägt das DSG – trotz seines Dualismus – dem Aspekt der *Beziehungsasymmetrie im Kontext der Personendatenverarbeitung Rechnung*. Indem auch für Datenverarbeitungen durch Private verlangt wird, dass ihre Handlungen geeignet sein müssen, um den vordefinierten Verarbeitungszweck zu erreichen, trägt man der *Machtasymmetrie* zwischen datenverarbeitenden Unternehmen und privaten Datensubjekten Rechnung.[771]

Ein Machtungleichgewicht zwischen den personendatenverarbeitenden Verant- 521
wortlichen und den Datensubjekten im privaten Bereich dürfte heute kaum mehr ernsthaft bestritten werden. Nichtsdestotrotz *variieren* die aus einem solchen Befund gezogenen rechtlichen *Schlussfolgerungen*.

Für die *Schweiz* wurden diese namentlich bereits im IV. Kapitel dieses zweiten 522
Teils, der den Dualismus des eidgenössischen Datenschutzgesetzes darstellt, herausgearbeitet. Mit der Totalrevision wird an dem Dualismus festgehalten. Gleichwohl ist eine Vereinheitlichung dergestalt zu verzeichnen, dass die gemeinsam für beide Bereiche geltenden Anforderungen und neuen Instrumente ausgebaut werden.

Anders lautet die Antwort vonseiten der *EU mit der DSGVO*: Der Machtasym- 523
metrie, der das Datensubjekt sowohl in seiner Beziehung zu privaten als auch zu öffentlichen Verarbeitenden ausgesetzt ist, wird mit der Implementierung eines monistischen Ansatzes entgegengetreten. Dieser Monismus sieht identische Regeln für Personendatenverarbeitungen durch Private und öffentliche Stellen vor. Der Übergang zu einem monistischen Modell, den die DSGVO vollzieht, markiert einen datenschutzrechtlichen *Paradigmenwechsel*.[772] In Deutschland wurde der Ansatz bereits einige Jahre zuvor debattiert.[773] Im Zusammenhang mit dem *Verhältnismässigkeitsgrundsatz* ist nicht nur das für beide Bereiche geltende grundsätzliche Verarbeitungsverbot gemäss Art. 6 DSGVO relevant. Einschlägig ist zudem der sog. Grundsatz der Datenminimierung gemäss Art. 5 lit. c DSGVO.

770 Für eine Ausdifferenzierung im Einzelfall tritt Epiney, in: Belser/Epiney/Waldmann (Hrsg.), 530, ein.

771 Vgl. insofern Buchner, 26 ff., insb. 28; zur Problematik der Machtasymmetrie im Vertragsrecht und den Reaktionen vonseiten des Rechts und der Rechtsprechung Derleder, in: Jestaedt/Lepsius (Hrsg.), 234 ff., 236 f.

772 Hierzu Pfaffinger, Vortrag vom 31. Januar 2019, Deloitte Zürich. Die Schweiz weicht im Zuge der Totalrevision des DSG nicht von ihrem dualistischen System ab.

773 Vgl. Buchner, 26 ff.

Ein *prinzipielles Verarbeitungsverbot* ist *das einflussreichste Instrument*, um die Datenminimierung zu implementieren. Gleichwohl wurde eine *Vereinheitlichung datenschutzrechtlicher Vorgaben* wegen einer parallel für den privaten und öffentlichen Bereich gedachten Beziehungsasymmetrie bereits vor der Ära der DSGVO selbst in Deutschland namentlich von Vesting und Buchner kritisch beleuchtet: Vesting legt die Ausrichtung und Orientierung einer vereinheitlichenden Datenschutzgesetzgebung an einem staatszentrierten Leitbild frei, in welchem er das Datenschutzrecht tief verhaftet sieht. Er weist auf die Schwächen des Vergleichs sowie des Transfers von Leitbildern vom öffentlich-rechtlichen in den privatrechtlichen Kontext hin. Ebendieser Transferprozess wurde gerade auch von der Rechtsprechung des Bundesverfassungsgerichts angeleitet.[774] Ähnlich kommt Buchner zu dem Schluss, dass sich die *Gefährdungslagen nicht* vergleichen lassen, zumal der Staat auf einen Zwangsapparat zur Durchsetzung seiner Ansprüche zurückgreifen kann.[775] Er plädiert für ein konsequent dem *privaten Interessenausgleich verpflichtetes Datenschutzrecht* für den privaten Sektor, dessen Ausgangspunkt ein Recht auf informationelle Selbstbestimmung sei.

524 Für die *Schweiz* nun lässt sich im Rahmen einer Analyse des Verhältnismässigkeitsprinzips und der Vorgabe der Datenminimierung im DSG eine bemerkenswerte Differenziertheit attestieren. Mit dem Dualismus und dem Ausgangspunkt der Verarbeitungsfreiheit mit Schranken für den privaten Bereich wird ausgedrückt, dass datenschutzrechtlich die Beziehung zwischen Datensubjekt und verarbeitenden öffentlichen Stellen gegenüber jener zwischen Privaten unter dem Aspekt der Machtasymmetrie *nicht identisch* gedacht wird. Gleichwohl wird die *Machtasymmetrie* auch in den gesellschaftlichen Beziehungen anerkannt, indem das Prinzip der Verhältnismässigkeit mit seinem im öffentlichen Recht geprägten Inhalt importiert wird. Ein solcher Transport eines Prinzips, das seinen Ursprung im öffentlichen Recht hat, in den privaten Sektor ist im Zusammenhang der Personendatenverarbeitung durchaus *sachgerecht*. Im *öffentlichen Bereich* erfolgt die Datenminimierung *doppelstufig: erstens* über das allgemeine Verarbeitungsverbot mit Ausnahmen gemäss Art. 17 DSG resp. Art. 33 nDSG und *zweitens* über das Verhältnismässigkeitsprinzip gemäss Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG in seiner öffentlich-rechtlichen Tradition und Trias. Für den *privaten Bereich* wird die Datenminimierung *einstufig* implementiert: Das Verhältnismässigkeitsprinzip mit seiner Trias der Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne setzt der prinzipiellen Verarbeitungsfreiheit im privaten Bereich eine recht konkrete und einschneidende Schranke. Der Verarbeitungsgrundsatz der Verhältnismässigkeit formuliert gegenüber privaten Verantwortlichen *präzise Handlungsanleitungen*. Die Datenverarbeitenden werden in

774 Vesting, in: Ladeur (Hrsg.), 155 ff.
775 Vgl. Buchner, 64 ff., 80 ff.

die Pflicht genommen, ihre Personendatenverarbeitungen auf ihre Eignung und Erforderlichkeit hin zu überprüfen. In dieser Zweck-Mittel-Relation markiert der Grundsatz der Verhältnismässigkeit die Grenze zwischen zulässiger und unzulässiger Datenverarbeitung.

525 In die Kritik, wonach das Verhältnismässigkeitsprinzip der grosse «Gleich- und Weichmacher» ist, der zur Auflösung des «sicheren Rechts in ein allgemeines Werten und Wägen führt»,[776] sollte im datenschutzrechtlichen Zusammenhang nicht eingestimmt werden. Mit diesem über das Verhältnismässigkeitsprinzip in der Schweiz weiter ausdifferenzierten Mechanismus wird die Dichotomie von öffentlich und privat aufgeweicht, aber keineswegs aufgegeben. Denn für den öffentlichen Bereich ist vorgeschaltet das Legalitätsprinzip zu beachten, vgl. datenschutzgesetzlich Art. 17 DSG resp. Art. 33 nDSG. Entsprechend ist es der Gesetz- oder Verordnungsgeber, der das zu verfolgende öffentliche Interesse, an das die Bearbeitungszwecke gekoppelt sind, *vordefiniert*.

526 Ein zusätzlicher Differenzierungsaspekt findet sich im DSG wie folgt: Unverhältnismässige Datenbearbeitungen im privaten Sektor können gerechtfertigt werden, nicht aber im öffentlichen Bereich.[777] Zur Rechtfertigung eines Verstosses gegen das Verhältnismässigkeitsprinzip kommen im privaten Bereich namentlich Gesetz und Einwilligung in Frage.[778] Die Koordinierung des Verarbeitungsgrundsatzes der Verhältnismässigkeit i. S. v. Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG mit dem Rechtfertigungsgrund des überwiegenden privaten oder öffentlichen Interesses, vgl. Art. 13 Abs. 1 und Abs. 2 DSG resp. Art. 31 Abs. 1 und Abs. 2 nDSG, fällt schwer. Insofern wird die Meinung vertreten, dass die Abwägungen von Art. 4 Abs. 2 und Art. 13 Abs. 1, Abs. 2 DSG zusammenfallen: Ist eine Datenbearbeitung unverhältnismässig, könne sie nicht durch ein überwiegendes Interesse nach Art. 13 DSG gerechtfertigt werden. Eine unverhältnismässige Datenbearbeitung i. S. v. Art. 4 Abs. 2 DSG sei widerrechtlich, es sei denn, es läge eine Einwilligung oder gesetzliche Grundlage vor.[779] In dieser Interpretation fallen Tatbestandsmässigkeit und (Nicht-)Rechtfertigung, was das Thema der Interessenabwägungen anbelangt, punktuell zusammen.

527 Ebendieser Auslegungsvorschlag vermag nicht zu überzeugen. Vielmehr verfolgt der Verhältnismässigkeitsgrundsatz gemäss Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2

776 Von Arnauld, in: Jestaedt/Lepsius (Hrsg.), 276 ff., 277; insofern auch Ladeur, Kritik.

777 Rosenthal, HK-DSG, Art. 4 N 19, der unter N 28 f. für die Rechtfertigungsmöglichkeit des verletzten Verhältnismässigkeitsgrundsatzes eintritt. Er begründet dies ebenso mit unterschiedlichen Funktionen des Grundsatzes sowie der Rechtfertigungsgründe.

778 Immerhin ist darauf hinzuweisen, dass die Einwilligungsmöglichkeit eingeschränkt werden kann, was namentlich über Art. 328b OR von Relevanz ist. Aufgrund der spezifischen Machtasymmetrie gilt die Einwilligung im arbeitsrechtlichen Kontext als kritisch.

779 So Epiney/Civitella/Zbinden, 24; strenger vertritt Peter, 134, dass eine Einwilligung in eine unverhältnismässige Personendatenverarbeitung nicht möglich sein soll.

nDSG als Verarbeitungsgrundsatz eine andere Stossrichtung, als sie die Interessenabwägung im Rahmen der Rechtfertigung aufweist. Die Verletzung des Verhältnismässigkeitsprinzips markiert für den privaten Bereich einen Tatbestand der Persönlichkeitsverletzung, vgl. Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Die Rechtfertigung gemäss Art. 13 Abs. 1 und Abs. 2 DSG resp. Art. 31 Abs. 1 und Abs. 2 nDSG infolge überwiegender Interessen hat eine andere Ausrichtung. Während es bei der Verhältnismässigkeit als Verarbeitungsgrundsatz um die Relation zwischen Verarbeitungszweck und Verarbeitungshandlung geht, geht es bei den überwiegenden Interessen im Rahmen der Rechtfertigungsgründe um die Interessenabwägung zwischen den Parteien, den Datenverarbeitenden («Verantwortliche») und den Datensubjekten.[780] Man stellt mithin die ggf. gegenläufigen Interessen von Datenbearbeitenden und Datensubjekten einander abwägend gegenüber. Es mag richtig sein, dass bei einer Verletzung der «Mittel-Zweck-Relation» solche überwiegenden Interessen nur ganz selten angenommen werden können. Das mit dem Verhältnismässigkeitsprinzip unweigerlich assoziierte Abwägungsparadigma bleibt damit bestehen; allerdings wird es aufgrund der vorangehenden Eignungs- und Erforderlichkeitsprüfung in einen engen Rahmen verwiesen.[781]

528 *Zusammenfassend:* Die Vorgabe, wonach Personendatenverarbeitungen geeignet und erforderlich für die Zweckerreichung sowie verhältnismässig im engeren Sinne sein müssen, bildet *für den privaten Bereich* die konkreteste und engste Schranke der prinzipiellen Verarbeitungsfreiheit. Mit dem Import eines im öffentlich-rechtlichen Verständnis definierten Verhältnismässigkeitsprinzips wird dem Befund Rechnung getragen, wonach auch in gesellschaftlichen Beziehungen im Umgang mit Personendaten *Machtasymmetrien* zwischen Datensubjekten und Verarbeitenden bestehen. Insofern wird die Vorstellung von der «Reinheit» des privaten Bereiches und des im ersten Kapitel beschriebenen Dualismus relativiert. Die für beide Bereiche im Kontext der Personendatenverarbeitung anerkannte Machtasymmetrie wird nach schweizerischem DSG indes nicht synchron gedacht: Für den öffentlichen Bereich wird das grundsätzliche Verarbeitungsverbot vorgeschaltet, was ein klares Gebot der Minimierung von Personendatenverarbeitungen markiert; ebendieses wird alsdann in einem zweiten Schritt durch den Verarbeitungsgrundsatz der Verhältnismässigkeit weiter umgesetzt. Die hier etablierte *Trias* von Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne soll gleichermassen für den öffentlichen wie den privaten Bereich gelten. Nimmt man für den Bereich der privaten Datenverarbeitung die Verhält-

780 Ausdrücklich hierzu Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.76; ähnlicher Ansicht wohl auch Rosenthal, HK-DSG, Art. 4 DSG N 28.

781 Von Arnauld, in: Jestaedt/Lepsius (Hrsg.), 276 ff., 277; zum Verhältnismässigkeitsprinzip im Rahmen der Bearbeitung von Personendaten auch Glass, 55 ff.

nismässigkeit im Sinne der Eignungs- und Erforderlichkeitsprüfung ernst, dann wird dem beklagten Risiko «willkürlicher, irrationaler» Entscheidungen viel von seiner Sprengkraft genommen.[782] Wenn sich die Verhältnismässigkeit als gemeinsamer Verarbeitungsgrundsatz auf die Mittel-Zweck-Relation konzentriert, dann gewinnen die jeweiligen Verarbeitungszusammenhänge beträchtliche Bedeutung. Im Verhältnismässigkeitsprinzip zeigt sich erneut mit Deutlichkeit die Relevanz, ob und inwiefern das Datenschutzrecht für die Personendatenverarbeitung durch Private resp. öffentliche Stellen identisch, vereinheitlichend oder ausdifferenziert gestaltet werden soll. Das DSG sieht hierbei, wie dargelegt, auch wenn es die Verhältnismässigkeit als Verarbeitungsprinzip für beide Bereiche in seiner öffentlichrechtlichen Gestalt vorsieht, ein beachtliches Mass an Differenzierung vor. Wie relevant die Berücksichtigung des Verarbeitungskontextes für die datenschutzrechtliche Normierung ist, zeigt sich in markanter Weise in dem Grundsatz. Das DSG zeigt eindrücklich, dass die Machtasymmetrie der Beziehung, wie sie für beide Bereiche gesehen wird, durch den Transport des Verhältnismässigkeitsprinzips in den privaten Bereich anerkannt wird. Sogleich aber werden die Spezifika der Bereiche, wie sie sich auch im Dualismus ausdrücken, via die Gewährleistung anderer, ausdifferenzierender Mechanismen geschützt. Der Argumentationsfaden ist: Machtasymmetrie in beiden Bereichen ja, Legitimation der Gültigkeit des Verhältnismässigkeitsprinzips in seiner öffentlichen Trias-Konzeption ja, gleichwohl weitere Anerkennung der Differenzierungswürdigkeit, selbst über Instrumente, die mit dem Verhältnismässigkeitsprinzip im Zusammenhang stehen.

529 Die datenschutzrechtliche Relevanz des Verarbeitungskontextes wird sodann über die «Gegenspieler» von den untrennbar mit dem Verhältnismässigkeitsprinzip verbundenen Löschungspflichten und -ansprüchen, vgl. neu auch Art. 6 Abs. 4 nDSG sowie spezialgesetzliche Aufbewahrungs- und Archivierungspflichten, sichtbar. Die Relevanz kontextueller Bezüge für das Datenschutzrecht, mit der eine Abwägung individueller Interessen für den Einzelfall in den Hintergrund rückt, wird vertiefend im Rahmen der zweckgebundenen Verarbeitungsgrundsätze analysiert.

3.2. Faktische Herausforderungen und rechtliche Entwicklungen

530 Das Verhältnismässigkeitsprinzip wird insb. vom Phänomen «Big Data» auf eine harte Probe gestellt. Auch in der Schweiz ist Big Data weder aus der öffentlichen Verwaltung noch aus dem privaten Sektor wegzudenken. Den unter diesem

782 Von Arnauld, in: Jestaedt/Lepsius (Hrsg.), 276 ff., 279.

Schlagwort eingefangenen Praktiken kommt nicht nur in der Praxis, sondern auch im Schrifttum grosse Aufmerksamkeit zu.[783]

531 Der Einsatz von Big-Data-Analysen gilt z. B. als wirksames Instrument zur Bekämpfung von Staus im Strassenverkehr. Staus verursachen enorme Kosten. Der wohl häufigste Einsatz von Big-Data-Analysen findet bei der Verkehrsplanung und -steuerung durch staatliche Behörden statt. So nutzt das Bundesamt für Strassen (Astra) Big Data, um Stauprognosen und dem Verkehrsfluss angepasste Tempo-Limits zu generieren. Hierfür kommen Videosensoren und eine Datenbasis der Swisscom mit (anonymisierten) Positionsdaten der Mobiltelefone von Swisscom-Kunden zum Einsatz. Darauf basierend lässt sich eruieren, wo der Strassenverkehr mit welcher Geschwindigkeit fliesst. Auf diesem Weg werden Staus und Stautendenzen frühzeitig erkannt; Navigationssysteme können Daten nutzen, um die Nutzerinnen und Nutzer auf Alternativrouten aufmerksam zu machen. Die Stauregulierung und -prävention ist nicht nur aus umweltschützerischen Gründen, sondern auch aus wirtschaftlichen Erwägungen interessant: Volkswirtschaftlich verursachen Staus nach Berechnungen des Bundesamts für Raumentwicklung und des Bundesamts für Strassen jährlich Kosten in der Höhe von gegen zwei Milliarden Franken.[784]

532 Ein weiteres Einsatzfeld findet Big Data im Bereich «öffentliche Sicherheit». Ein Beispiel wird in der NZZ vom 22. Dezember 2015 unter dem Titel «Kommissar Kristallkugel» dargestellt.[785] Wie kaum ein Verbrechen hat der Vierfachmord von Rupperswil am 21. Dezember 2015 die Schweiz erschüttert. Erst im Juni 2016 konnte der Zugriff auf den Täter erfolgen, wobei neben dem Fingerabdruck und der DNA-Analyse das Schlüsselinstrument zur Aufklärung der Tat die akribische Auswertung von Handydaten war. So wurden die Registrierungen über die Antennen in unmittelbarer Umgebung zum Tatort untersucht: Jedes eingeschaltete Handy loggt sich, sobald dessen Träger sich in der Nähe der entsprechenden Antenne befindet, in diese ein. Anschliessend konnte anhand einer riesigen Menge von Handydaten, die über die Antenne gesammelt wurden, ermittelt werden, wer zum relevanten Zeitpunkt in der Umgebung des Tatortes war. Die Auswertung

783 Culik/Döpke, ZD 2017, 226 ff.; Hoeren, Int. J. Law Inf. Technol. 2017, 26 ff.; Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff.; sodann die Beiträge in Kalyvas/Michael (ed.); Weber/Thouvenin (Hrsg.) und Fasel/Meier (Hrsg.); Epiney, Jusletter IT vom 21. Mai 2015; unlängst hierzu auch Heuberger, N 31 ff.; zu Big Data Analytics Baeriswyl, in: Weber/Thouvenin (Hrsg.), 45 ff.; Mayer-Schönberger/Cukier, *passim*; eine kursorische Analyse führt Prieur, AJP 2015, 1643 ff. zu dem Schluss, dass sich Big-Data-Unternehmen, die im Internet und über soziale Plattformen Personendaten zusammentragen und auswerten, um das Datenschutzrecht foutieren; vgl. zu den datenschutzrechtlichen Herausforderungen am Beispiel von Big Data Burkert, in: Epiney/Fasnacht/Blaser (Hrsg.), 1 ff.; de Werra, RSDA 2020, 365 ff.

784 Vgl. Tagesanzeiger, So viel kosten Staus auf Schweizer Strassen, Zürich 2018, <https://www.tagesanzeiger.ch/schweiz/standard/so-viel-kosten-staus-auf-schweizer-strassen/story/21144070> (zuletzt besucht am 30. April 2021).

785 Przybilla, NZZ vom 22. Dezember 2015.

wurde polizeilich nach einem Gesuch der Staatsanwaltschaft an die Swisscom vorgenommen.[786]

In Zürich setzt die Stadtpolizei seit November 2013 auf die Prognosesoftware Precobs (Precrime Observation System).[787] In das Programm werden ermittlungstechnische Daten von bereits begangenen Einbrüchen wie der Tatort, die Tatzeit, Beute und Vorgehensweise eingegeben. In der Folge macht sich die Software eine Erkenntnis aus der Kriminologie zunutze: Auch professionelle Einbrecher haben ihre jeweils eigene Handschrift, die Delikte werden nach bestimmten Mustern begangen. Darauf basierend erstellt ein Software-Programm Prognosen hinsichtlich unmittelbar zu erwartender Folgeeinbrüche. Entsprechend lässt sich z. B. eine Erhöhung der Polizeipräsenz planen. 533

Big-Data-Analysen kommen sodann im Versicherungswesen zur Anwendung: Unfall- und Krankenversicherungen müssen pro Jahr Millionen von Arzt- und Spitalrechnungen kontrollieren, was eine finanzielle und bürokratische Herausforderung darstellt.[788] Um diese Arbeit zu bewältigen, setzen Schweizer Versicherer wie die Suva bereits heute auf Big Data.[789] Millionen von Rechnungsdaten können mithilfe einer Software kontrolliert werden. Die Software kann feststellen, ob eine Konsultation richtig verrechnet oder ob der Ansatz für Schmerzmittel eingehalten wurde. Der Einzelfall wird durch das Programm mit tausenden ähnlich gelagerten Fällen verglichen, wobei beispielsweise Medikamente als auffällig eingestuft werden, die in einem solchen Fall für gewöhnlich nicht verschrieben werden. Durch die Nutzung von Big Data kann allein die Suva jährlich CHF 200'000'000.00 einsparen. 534

Die Einsatzmöglichkeiten von Big Data erscheinen alle sehr nützlich – Staus umfahren, Verbrechen bekämpfen, Unfälle verhindern, vor Versicherungsbetrug und Kreditkartenmissbrauch schützen, effizientere Markt- und Konsumbeziehungen aufbauen sowie pflegen. Die Einsatzbereiche von Big-Data-Analysen erstrecken sich damit über weite Felder.[790] 535

786 In diesem Zusammenhang ist das neue BÜPF zu erwähnen, vgl. <https://www.ejpd.admin.ch/ejpd/de/home/aktuell/meldungen/2017/vuepf-faq.html> (zuletzt besucht am 30. April 2021).

787 Vgl. Institut für musterbasierte Prognosetechnik Verwaltungs-GmbH, Pre-crime observation system, Bern 2016, <https://www.swisspoliceict.ch/getattachment/04e4ca1a-cf03-4c89-973d-a822cb7e7539/.aspx> (zuletzt besucht am 30. April 2021); zum Predictive Policing in der Schweiz und Precobs Camavdic, Jusletter IT vom 26. September 2019, N 1 ff., insb. N 4; zur rechtsstaatlichen Verarbeitung von Personendaten im Bereich der Polizei Glass, 244 ff.

788 Eindrücklich mit Blick auf Personendatenflüsse, wie sie innerhalb von Spitälern, aber auch nach aussen zwecks Forschung, Abwicklung von Sozialversicherungsleistungen oder zu Bundesbehörden erfolgen, Gogniat, Jusletter vom 20. Juni 2016, N 35 ff.

789 Vgl. hierzu NZZ vom 8. März 2016 – Suva schöpft Kraft aus Big Data, abrufbar unter: <https://www.nzz.ch/wirtschaft/suva-schoepft-kraft-aus-big-data-1.18708611?reduced=true> (zuletzt besucht am 30. April 2021).

790 Bereits an der Jahrtausendwende wurden Personendaten in unzähligen Bereichen gesammelt; vgl. hierzu den Überblick bei Eckhardt/Fattebert/Keel/Meyer, 17 ff.; vgl. zu den Anwendungsberei-

536 Was aber ist Big Data? So vielfältig die Beispiele daherkommen, so vielfältig sind auch die vorgeschlagenen Definitionen.[791] Regelmässig wird Big Data anhand von vier resp. fünf Charakteristika definiert. Varianten finden sich auch hier. Als definitionsrelevant gelten die sog. «vier resp. fünf Vs»: *Volume*, *Velocity*, *Variety*, *Veracity* und *Value*.[792]

537 Zunächst beschreibt Big Data enorme Datenmengen – *Volume* –, die durch den technischen Fortschritt mit höchster Geschwindigkeit – *Velocity* – verarbeitet werden (Echtzeitsammlung).[793] Vielfältig ist die Beschaffenheit der Daten sowie der Quellen – *Variety* –, wobei an Audio- oder Videodateien, Tweets, Dokumente, Fotos zu denken ist, um nur einige Beispiele zu nennen, aber eben auch an Datenbestände, die in unterschiedlichen Systemen oder Kontexten gesammelt wurden. Mit *Veracity* wird die Korrektheit der Daten eingefangen. *Value* ist das Merkmal des (ökonomischen) Mehrwerts, der durch die Verarbeitung und Verknüpfung von Daten geschaffen wird.[794]

538 Durch die weiträumige Analyse von Einkaufsgewohnheiten von Konsumierenden kann beispielsweise Werbung individualisiert auf den Einzelnen zugeschnitten werden.[795] Damit einher geht die Monetarisierung von Daten, wobei die Kundschaft den Rohstoff selbst liefert. An dieser Stelle gewinnt die Dimension von Value – gerade auch für die Privatwirtschaft – einen besonderen Wert.[796]

539 Bei Banken kamen früher personenbezogene Daten der Klientel in erster Linie zur Kontoführung und – rudimentärer – zur Pflege der Kundenbeziehung zum Einsatz. Heute bieten die Banken Tools zur Erfassung von Auslagen an, die deren Einordnung nach Sport, Familie usf. ermöglichen. Das kann dazu dienen, spezifische Angebote, ggf. auch in Kooperation mit anderen Unternehmen, zu unterbreiten. Ein weiteres Beispiel zu Value ist die Registrierung von Kreditkartenbezügen: Mit der exakten Erfassung entsteht ein Bild über Kaufverhalten und

chen von Big-Data-Analysen auch Epiney, Jusletter IT vom 21. Mai 2015; zu Big Data mit den Risiken spezifisch für den Arbeitskontext Nebel, ZD 2018, 520 ff.

791 Vgl. auch Prieur, AJP 2015, 1644 ff.

792 Vgl. m. w. H. (ohne Value als Definitionselement) Wespi, in: Weber/Thouvenin (Hrsg.), 3 ff., 4 f.; zu den fünf Vs Meier, in: Meier/Fasel (Hrsg.), 5 ff.; vgl. zu Definitionen von Big Data auch Wenhold, 32 ff.; zur Korrelation von Volume sowie Value Odlyzko, Int. J. Commun. 2012, 920 ff.; zum Value, gerade von Daten im Internet, auch Cavoukian/Chibba/Williams/Ferguso, Jusletter IT vom 21. Mai 2015, N 7; zu den Begriffen von Big Data und Data Mining Cichocki, Jusletter IT vom 21. Mai 2015, N 4 ff.; vgl. auch die Beschreibung des Soziologen Coll, in: Epiney/Nüesch (Hrsg.), Separatum, 1 ff., 2 f.; als charakteristisch gilt insb. die Verknüpfung von Daten aus diversen Quellen; vgl. Epiney, Jusletter IT vom 21. Mai 2015, N 6; vgl. Fasel/Meier, in: Fasel/Meier (Hrsg.), 3 ff., 5 ff.

793 Hierzu m. w. H. auch Beranek Zanon, in: Thouvenin/Weber (Hrsg.), 86 ff., 87; Mayer-Schönberger/Cukier, 11 f.

794 Meier, in: Meier/Fasel (Hrsg.), 37.

795 Zur personalisierten Werbung Auf der Mauer/Fehr-Bossard, in: Thouvenin/Weber (Hrsg.), ITSL 2017, 23 ff.

796 Vertiefend hierzu dritter Teil, VII. Kapitel, B.2.

Lokalität der Inhaberin. Verzeichnet das Kreditkartenunternehmen den Einsatz an einem überraschenden Ort oder deckt sich ein Konsumverhalten ganz und gar nicht mit den bisherigen Verhaltensweisen des Karteninhabers, geht man der Angelegenheit nach und interveniert. So können Kartenbetrüge verhindert oder rascher unter Kontrolle gebracht werden.

Der Begriff «Big Data» wird als «Phänomen» beschrieben.[797] Ein Phänomen, das mit Schlagworten von «Big Brother» über «Big is beautiful» bis zum «neuen Goldrausch» besetzt ist.[798] Realitätsnäher erfasst steht der Terminus eher für ein Paradigma denn eine Technologie, Methode oder Praxis.[799] 540

Big Data fordert das Datenschutzrecht und präziser die datenschutzrechtlichen Verarbeitungsgrundsätze heraus. Augenfällig ist dies nicht nur mit Blick auf das Verhältnismässigkeitsprinzip, verstanden als Datensparsamkeit. Big-Data-Analysen streben nach maximalen Datenbeständen. Der Analyseerfolg wird in Abhängigkeit von der Grösse der Datenmengen beurteilt.[800] Dies steht in einem scharfen Kontrast zum Verhältnismässigkeitsgrundsatz. Zugleich ist ein neuralgischer Punkt in der Mittel-Zweck-Relation sowie der Zweckbindung zu verorten. Denn der Pool von Personendaten für Big-Data-Analysen wird regelmässig aus diversen Quellen gespeist. Damit einher gehen meist auch Zweckänderungen.[801] Die Personendaten stammen oft aus diversen Quellen, wobei mit ihnen zahlreiche Zwecke verfolgt werden, die im Vorfeld meist nicht definiert sind. Werden sie potentiell an einen unbestimmt offenen Empfängerkreis weitergeleitet, stehen über das Verhältnismässigkeitsprinzip und das Verbot der Vorratsdatenspeicherung hinaus auch die Einhaltung von Transparenzvorgaben auf dem Spiel.[802] 541

An dieser Stelle geht es weniger darum, die Kollision von Big Data im Hinblick auf die datenschutzrechtlichen Vorgaben *de lege lata* abzuhandeln.[803] Dargestellt werden vielmehr die jüngsten rechtlichen Entwicklungen und die Weiterentwicklung von datenschutzrechtlichen Vorgaben. 542

Auf die zugleich produktiven wie auch disruptiven Folgen von Big-Data-Analysen bezog sich der Europarat mit «Guidelines on the protection of individuals 543

797 So Epiney, Jusletter IT vom 21. Mai 2015.
798 Cichocki, Jusletter IT vom 21. Mai 2015, N 1.
799 Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 44 und 46.
800 Nissenbaum, 41 ff.
801 Hierzu Helbing, K&R 2015, 145 ff.
802 Vgl. Passadelis, Vortrag vom 13. April 2016, Universität Luzern.
803 Zu den Datenschutzrisiken von Big Data z. B. Beranek Zanon, in: Thouvenin/Weber (Hrsg.), 86 ff., 92 ff. und insb. 106 ff.; dazu, dass das aktuelle Datenschutzrecht den Herausforderungen von Big Data nicht gewachsen ist, Cavoukian/Chibba/Williams/Ferguso, Jusletter IT vom 21. Mai 2015; als «contradiction manifeste» mit den datenschutzgesetzlichen Prinzipien wird Big Data beschrieben von Coll, in: Epiney/Nüesch (Hrsg.), Separatum, 1 ff., 9; Epiney, Jusletter IT vom 21. Mai 2015, N 9 ff.; eine kursorische rechtliche Reflexion von Big Data im Lichte des DSG findet sich auch bei Prieur, AJP 2015, 1644 ff., 1647 ff.

with regard to the processing of personal data in a world of Big Data».[804] Es handelt sich um Empfehlungen, welche die Bedeutung der *Zweckbindung* betonen. Sie halten fest, dass entsprechende Verfahren nicht zu einer Personendatenverarbeitung führen sollen, die für die Datensubjekte *unerwartet* ist sowie zu diversifizierten Risiken führt.[805] Die Empfehlungen weisen auf die Bedeutung *präventiver Massnahmen* hin. Dazu gehören die Risiko-Analysen sowie der Privacy-by-design-Ansatz.[806] Zudem wird das Instrument der Anonymisierung und die Notwendigkeit der Integration der Datensubjekte im Rahmen von automatisierten Entscheidungen aufgeführt.[807]

544 Entsprechende Instrumente finden sich ebenso in der DSGVO sowie in der Totalrevision des DSG: Anonymisierungsvorgaben, Anforderungen an die informierte Einwilligung sowie solche im Rahmen der automatisierten Entscheidungen, das Instrument der Datenschutz-Folgenabschätzung sowie «privacy by design and default» gelten gemäss dieser Rechtstexte.[808] Es handelt sich hierbei um Vorgaben und Instrumente, die auch, aber nicht nur, der Verwirklichung des Grundsatzes der Verhältnismässigkeit dienen.

545 Spezifisch für den Verhältnismässigkeitsgrundsatz hält die Totalrevision an der nicht überzeugenden Systematik fest, wonach die Verhältnismässigkeit mit Treu und Glauben in einem Absatz verankert wird, vgl. Art. 6 Abs. 2 nDSG. Er entspricht dem bisherigen Art. 4 Abs. 2 DSG. Allerdings finden sich Konkretisierungen mit Art. 6 Abs. 3 und Abs. 4 nDSG, welche die Korrelation zwischen dem Verhältnismässigkeitsprinzip und dem Verarbeitungszweck verdeutlichen. Abs. 4 konkretisiert die *zeitliche* Dimension der Verhältnismässigkeit, wonach Daten nicht beliebig lange mit ihrem Personenbezug gespeichert werden dürfen.[809] Neu lauten die Absätze:

> «[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.»
>
> «[4] Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.»

546 Die gesetzgeberischen Anpassungen verdeutlichen, dass der Grundsatz der *Verhältnismässigkeit* dazu dient, die Eignung und Erforderlichkeit von Personenda-

804 Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data vom 23. Januar 2017, abrufbar unter: <https://rm.coe.int/16806ebe7a> (zuletzt besucht am 30. April 2021).
805 Vgl. Council of Europe, Guidelines, Ziff. 3.1.
806 Vgl. Council of Europe, Guidelines, Ziff. 2. und 4.
807 Vgl. Council of Europe, Guidelines, Ziff. 6. f.
808 Siehe Art. 4 Nr. 3–5, Art. 12., Art. 25 und Art. 35 f. DSGVO.
809 Vgl. zum Niedergang des Vergessens im Zuge der Digitalisierung und seiner Problematik Mayer-Schönberger, Delete, 64 ff.

tenverarbeitungen zu den damit anvisierten Zwecken zu gewährleisten. Offensichtlich weist der Verarbeitungsgrundsatz der Verhältnismässigkeit damit eine nähere Verbindung zu den *Zweckvorgaben* als zu Treu und Glauben auf. Neu wird zudem namentlich das zeitliche Element des Verhältnismässigkeitsprinzips ausgearbeitet, indem eine *Anonymisierung* resp. *Vernichtung resp. Löschung* verlangt wird, sobald die Erforderlichkeit nicht mehr gegeben ist. Betreffend die Vorgaben zur Löschung resp. Vernichtung ist auf das Recht der Betroffenen auf Löschung hinzuweisen, vgl. Art. 32 Abs. 2 lit. c nDSG, wobei dieses Betroffenenrecht nicht an Verhältnismässigkeitsvorgaben gebunden ist.

Auch die DSGVO widmet den *Löschungsvorgaben* und damit der zeitlichen Di- 547
mension von Personendatenverarbeitungen, namentlich der Speicherung, erhöhte Aufmerksamkeit: Den Betroffenen kommt gemäss Art. 17 DSGVO ein Recht auf Löschung zu, das unter dem Recht auf Vergessen in das kollektive Bewusstsein eingeht.[810] Die EU-Aufsichtsbehörden können den Anspruch autoritativ durchsetzen, vgl. Art. 58 lit. g DSGVO. Zudem geht die DSGVO vom grundsätzlichen Verbot der Personendatenverarbeitung und der Erforderlichkeit eines Rechtfertigungsgrundes für die Datenverarbeitung gemäss Art. 6 DSGVO aus, womit Personendatenverarbeitungen generell beschränkt und auf ein gerechtfertigtes Mass reduziert werden. Alsdann verankert Art. 5 lit. c DSGVO den Grundsatz der Datenminimierung, wonach Datenverarbeitungen in Korrelation zum verfolgten Zweck relevant, angemessen und auf das notwendige Mass beschränkt sein müssen. Ergänzend statuiert Art. 5 lit. e DSGVO eine Speicherbegrenzung dahingehend, dass Personendaten nur so lange in einer Form, welche die Identifizierung einer Person ermöglicht, gespeichert werden dürfen, wie dies zur Zweckerreichung erforderlich ist. Ist der Verarbeitungszweck erreicht worden und stehen keine Archivierungs- und Aufbewahrungspflichten entgegen, sind die Daten entweder zu löschen oder endgültig zu anonymisieren. Im Lichte der Vorgaben der DSGVO und namentlich von Art. 24 DSGVO empfiehlt es sich, ein eigentliches Löschkonzept zu entwickeln und entsprechende Vorgänge zu dokumentieren. Im

810 Löschungsvorgaben werden in der Schweiz durch weitere Bestimmungen umgesetzt werden, vgl. auch Art. 32 Abs. 2 lit. c nDSG; hierzu vertiefend Hunziker, 15 ff., auch kritisch zur Frage einer Utopie des Löschens und des dahinterstehenden Idealbildes der Kontrolle, 213 ff.; das Bild der Kontrolle ist auch im Konzept informationeller Selbstbestimmung mächtig, trifft indes auch ebenda auf Grenzen im Lichte digitaler Technologien; vgl. illustrativ hierzu z. B. Cavoukian, digma 2009, 20 ff., 20; zum Recht auf Speicherbegrenzung, zur Löschungspflicht resp. zum Recht auf Löschung gemäss DSGVO und zu den Begrifflichkeiten auch nach Schweizer DSG Rosenthal, digma 2019, 290 ff., 291 ff.; vgl. zur Bedeutung des Vergessens resp. Löschens im digitalen Zeitalter grundlegend Mayer-Schönberger, Delete, 10 ff., mit dem einleitenden Illustrationsbeispiel der betrunkenen Piratin: Einer jungen Frau, die Lehrerin werden wollte und sämtliche Prüfungen erfolgreich bestanden hatte, wurde der Zugang zum Beruf verweigert. Da sie im Internet ein Foto von sich selbst mit einem Piratenhütchen, einem Plastikbecher sowie den Worten «Drunken Pirate» hochgeladen hatte, wurde sie als nicht geeignet für den Lehrerinnenberuf beurteilt.

Rahmen der Löschungs- und Anonymisierungsprozesse kommt automatisierten und technischen Massnahmen eine wichtige Rolle zu.[811]

548 Die Umsetzung der Löschungs- aber auch Anonymisierungsvorgaben stellt die Verantwortlichen in der Praxis oftmals vor beträchtliche, auch technisch bedingte Schwierigkeiten.[812] Um den entsprechenden rechtlichen Anforderungen nachkommen zu können, bedarf es an erster Stelle der Kenntnis der Personendatenverarbeitungsprozesse in der Organisation mit ihren jeweiligen Zwecken. Basisinstrument ist bezüglich der Vorgaben gemäss Verhältnismässigkeitsprinzip, aber auch der Gewährleistung der Betroffenenrechte, das Inventar (sog. Verarbeitungsverzeichnis, vgl. Art. 30 DSGVO und Art. 12 nDSG). Hinsichtlich der Löschungsvorgaben und der Anonymisierung ist ein kritischer Hinweis angezeigt: Die Anonymisierung eliminiert ein Element für die Anwendbarkeit der Datenschutzgesetzgebung, den Personenbezug.[813] Folglich erscheint sie als eine attraktive Lösung für Big-Data-Analysen. Allerdings wurden Schwächen des Konzeptes freigelegt: Die Anonymisierung ist kaum je unangreifbar resp. so robust, dass der Personenbezug nicht wieder herstellbar wäre. Zudem eliminiert die «Anonymität» nicht die «Erreichbarkeit» der Subjekte, den «Zugriff» auf diese und in der Folge beispielsweise die Manipulierbarkeit.[814]

3.3. Resümee

549 Der Verarbeitungsgrundsatz der Verhältnismässigkeit wird in der Schweiz gemeinsam mit Treu und Glauben verbürgt, vgl. Art. 4 Abs. 2 resp. Art. 6 Abs. 2 nDSG. Neu widmet sich auch ein Art. 6 Abs. 4 nDSG dem zeitlichen Aspekt der Verhältnismässigkeit ausdrücklich.

550 Das Verhältnismässigkeitsprinzip wird für den privaten Bereich mit dem Inhalt der Eignung sowie Erforderlichkeit mit Blick auf den angestrebten Zweck sowie die Verhältnismässigkeit im engeren Sinne angewandt. Wird das Verhältnismässigkeitsprinzip als allgemeiner Datenverarbeitungsgrundsatz eingebettet betrachtet, zeigt sich, wie ausdifferenziert das datenschutzgesetzliche System der Schweiz ist.

551 Mit dem prinzipiellen Verarbeitungsverbot für den öffentlichen Bereich anerkennt es die Machtasymmetrie im Verhältnis Bürger und Staat. Dadurch wird auf einer ersten Stufe eine *Minimierung der Personendatenverarbeitung* erzielt.

811 Vgl. Art. 25 DSGVO; zum Verhältnis zwischen Regulierung und Technologie insb. auch Nissenbaum, Berkeley Tech. L.J. 2011, 1367 ff.; vgl. zur technischen Umsetzung von Löschungsvorgaben Hunziker, 118 ff.; vgl. Waidner/Karjoth, digma 2004, 18 ff., 19 f.

812 Zur Herausforderung der Datenlöschung mit Praxisbezügen Pisà, RR-COMP 2019, 8 ff.; Rosenthal, digma 2019, 290 ff., 290.

813 Vgl. Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 49 und 56 f.

814 Dies., in: Dies. (ed.), a. a. O.; m. w. H. Heuberger, N 77 ff.

Im Sinne einer zweiten Stufe greift im öffentlichen Bereich sodann das Verhältnismässigkeitsgebot als allgemeiner Verarbeitungsgrundsatz.

552 Der Aspekt der Machtasymmetrie im Zusammenhang von Personendatenverarbeitungen wird ebenso im *privaten Bereich* anerkannt, allerdings *einstufig:* Das Verhältnismässigkeitsprinzip wird nicht in Gestalt einer Rechtsmissbrauchsschranke interpretiert (was aufgrund der vereinten Regelung mit Treu und Glauben gefolgert werden könnte), stattdessen mit seinem «engen» öffentlich-rechtlichen Inhalt, der die Trias der Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne gleichermassen für den privaten Bereich verlangt. Das setzt der prinzipiellen Verarbeitungsfreiheit eine enge und griffige Schranke. Entsprechend kommt dem Verhältnismässigkeitsprinzip im privaten Bereich eine bedeutsame Rolle zu, Personendatenverarbeitungen zu limitieren.

553 Indem das DSG zwar einen Dualismus vorsieht, zugleich aber das Verhältnismässigkeitsprinzip für den privaten Bereich mit dem für den öffentlichen Bereich geltenden analogen Gehalt gilt, wird eine machtasymmetrische Beziehung im Kontext der Personendatenverarbeitung im privaten Bereich anerkannt. Diese Machtasymmetrie wird indes aufgrund des Dualismus für den privaten Bereich anders gedacht als für das Verhältnis zwischen Bürger und Staat. Damit hat sich gezeigt, dass der im IV. Kapitel beschriebene Dualismus nicht rein verwirklicht ist, sondern durch den Verhältnismässigkeitsgrundsatz punktuell korrigiert wird.

554 Die vorangehenden Ausführungen haben zudem sichtbar gemacht, dass mit den jüngsten datenschutzrechtlichen Entwicklungen durch mehrere Instrumente der Einhaltung des Verhältnismässigkeitsgrundsatzes in der Praxis Nachachtung verschafft werden soll. Zudem wird der Grundsatz selbst mit der Totalrevision weiter konkretisiert. Von zentraler Bedeutung ist die Korrelation zwischen Verhältnismässigkeit und Verarbeitungszweck, wobei auch die zeitliche Dimension ausdrücklicher adressiert wird, Art. 6 Abs. 3 und Abs. 4 nDSG. Werden Personendaten zur Erfüllung eines bestimmten Zweckes nicht mehr gebraucht, sind diese zu löschen oder zu anonymisieren. Löschungsvorgaben ist folglich nicht erst und nur bei Ausübung eines entsprechenden Betroffenenrechts nachzukommen. Vielmehr haben die Verantwortlichen Prozesse und Massnahmen zur Löschung und Anonymisierung im Rahmen der Datenschutz-Compliance zu implementieren. Hierbei ist allfälligen Archivierungs- und Aufbewahrungspflichten Rechnung zu tragen.[815]

555 Nachdem im Rahmen der Analyse zum Verhältnismässigkeitsprinzip die Bedeutung des Verarbeitungszweckes sichtbar wurde, ist nunmehr auf die datenschutzrechtlichen Zweckvorgaben einzugehen. Die Bedeutung des Verarbeitungszweckes zeigte sich in einer ersten Facette im Rahmen des Verhältnismässigkeitsprin-

815 Insofern empfiehlt sich für Unternehmen auch, entsprechende Retention-Policies zu erlassen.

zips: In der Schweiz wird dieses durch die Zweck-Mittel-Relation ebenso für den privaten Bereich anerkannt. Personendatenverarbeitungen müssen zur Erreichung des Zweckes geeignet und erforderlich sowie verhältnismässig im engeren Sinne sein. Trotz seiner gemeinschaftlichen Regelung in einem Absatz mit Treu und Glauben steht das Verhältnismässigkeitsprinzip somit in einem engen Konnex zum Verarbeitungszweck. Darin erschöpft sich aber seine Relevanz für die Datenschutznormierung nicht, wie die nachfolgenden Erörterungen zeigen.

4. Die Zweckvorgaben

4.1. Vorbemerkungen

4.1.1. Hypothese – Schlüssel zu den datenschutzrechtlichen Schutzzwecken

556 Die Zweckvorgaben spielen in verschiedener Hinsicht eine Schlüsselrolle im zeitgenössischen Datenschutzrecht. Sie sind zwischen den generalklauselartigen Verarbeitungsgrundsätzen, namentlich der Verhältnismässigkeit, und konkretisierten Bearbeitungsvorgaben angesiedelt, vgl. Art. 4 Abs. 3 DSG und Art. 6 Abs. 3 nDSG. Anhand der *Gebote im Zusammenhang mit dem Verarbeitungszweck* lässt sich zunächst die sukzessive Ausdifferenzierung nachzeichnen. Der Zweckbindungsgrundsatz ist weiter dazu geeignet, eine datenschutzrechtliche *Grundsatzfrage aufzuwerfen: Die Frage nach dem Zweck der Datenschutzregulierung*. Ansätze für die Antwort lassen sich in erster Linie anhand einer Analyse des Volkszählungsurteils des Bundesverfassungsgerichts mit seinen Erwägungen zur Zweckbindung generieren.

557 Den datenschutzgesetzlichen Zweckvorgaben kommt, wie zu zeigen sein wird, sowohl aus einer *materiellrechtlichen als auch aus einer prozeduralen und organisatorischen Perspektive* herausragende Bedeutung für den Datenschutz zu. Der Befund lässt sich neuerdings anhand der DSGVO und der Totalrevision des DSG bestätigen.

558 Unter dem Titel der Zweckvorgaben werden nachfolgend zuerst *seine anerkannten Teilgehalte* behandelt. Dazu gehören die initiale Zweckdefinierung resp. -fixierung, die Zwecktransparenz sowie die Zweckbindung. Anhand einer Analyse des Verarbeitungsgrundsatzes der Zweckbindung sollen die inhaltliche Bedeutung und die hohe Relevanz der Zweckvorgaben für das Datenschutzrecht freigelegt werden. Im Zentrum steht hierbei eine Auseinandersetzung mit dem mittlerweile in die Jahre gekommenen *Volkszählungsurteil des Bundesverfassungsgerichts*, dessen Argumentation gleichwohl nichts an seiner Aktualität eingebüsst

hat.[816] Bis heute geht die Nennung des Volkszählungsurteils untrennbar mit der ebenda erfolgten Anerkennung des Rechts auf informationelle Selbstbestimmung einher. Mit der informationellen Selbstbestimmung wird ein subjektives Recht assoziiert, wobei die Einwilligung des Datensubjektes eine zentrale Rolle spielt. Dieser Tage gelten Einwilligungskonstruktionen stärker denn je als «Patentrezept» zur Lösung datenschutzrechtlicher Herausforderungen.[817]

559 Die Aufmerksamkeit der anschliessenden Ausführungen allerdings richtet sich gerade nicht auf das *subjektive Recht auf informationelle Selbstbestimmung*, für dessen Anerkennung besagtes Urteil in die Rechtsgeschichte einging. Vielmehr soll eine *systemische Schutzdimension des Datenschutzrechts herausgearbeitet werden,* die im Urteil angelegt ist. Sie lässt sich anhand einer Analyse der bahnbrechenden Erwägungen zu den Zweckvorgaben erschliessen. Ebendiese *systemische Dimension des Urteils* blieb bislang – im Gegensatz zur stark beleuchteten *subjektiven Dimension des Rechts auf informationelle Selbstbestimmung* – weitgehend unterbeleuchtet. Eine Auseinandersetzung mit den Erwägungen des Bundesverfassungsgerichts zum Zweckbindungsgrundsatz erhellt indes, dass das Datenschutzrecht seit jeher als Instrument des Schutzes nicht nur von Individuen, sondern auch von Systemen und Kontexten gesehen wird.[818]

560 Die herausragende Bedeutung der *Zweckbindung* im und für das Datenschutzrecht wurde somit *gerichtlich vom Deutschen Bundesverfassungsgericht* in seinem berühmten Volkszählungsurteil aus dem Jahr 1983 herausgearbeitet. Es ist die *Fixierung des Verarbeitungszweckes auf die Statistik,* das Statistikgeheimnis, welche den Angelpunkt der Argumentation bildet. Das Statistikgeheimnis implementiert ein Verbot, die zum Zweck der Volkszählung erhobenen Personendaten dem *weiteren Verwaltungsvollzug* dienlich zu machen.[819]

561 Vonseiten der Wissenschaft wurde die Relevanz der Zweckbindung früh von Simitis mit den folgenden Worten anerkannt:

> «[D]ie unmissverständliche Forderung nach einer klaren Zweckbindung schränkt den Verarbeitungsradius von vornherein nachhaltig ein […].»[820]

816 Vgl. BverfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983.

817 Zum Recht auf Kontrolle der eigenen Personendaten vgl. Buchner, 207 und 230 f.; m. w. H. und kritisch Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 26; kritisch ebenso zu der dominanten Vorstellung, wonach ein Kontrollrecht an eigenen Daten die Lösung sei, Solove, Stan. L. Rev. 2001, 1393 ff., 1445 ff.; zum Recht an eigenen Daten vertiefend dritter Teil, VIII. Kapitel, B.

818 Richtungweisend hierzu Nissenbaum, *passim;* auf die Relevanz des Verarbeitungszusammenhanges hingewiesen hat früh Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 18, N 20; Ders., in: Schlemmer (Hrsg.), 67 ff., 74 f.; vgl. auch Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 29.

819 Vgl. BverfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 178. ff. und E 222. ff.

820 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 38.

562 In der schweizerischen Lehre und Rechtsprechung wird dem *Zweckbindungsgrundsatz* zumindest punktuell hohe Relevanz zugemessen.[821] Im Logistep-Urteil richtete das Bundesgericht den Fokus auf die (fehlende) *Transparenz des Bearbeitungszwecks*.[822] Die nachfolgenden Ausführungen beschreiben – nach einer Übersicht über die datenschutzrechtliche Positivierung – die rechtlich anerkannten Teilgehalte der zweckorientierten Datenschutzbestimmungen. Anschliessend wird vertiefend der Frage nach dem Schutzzweck des Datenschutzrechts nachgegangen.

4.1.2. Übersicht über die Positivierung

563 Die Kategorie des Verarbeitungszweckes zeigte sich bereits in seinem Zusammenspiel mit dem datenschutzrechtlichen Verarbeitungsgrundsatz der *Verhältnismässigkeit*. Die Vorgaben der Verhältnismässigkeit mit der Trias Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne richten sich am Verarbeitungszweck aus. Darüber hinaus sind in Bezug auf den Verarbeitungszweck *Transparenzvorgaben*, die sich auch, aber nicht nur auf diesen beziehen, einschlägig. Innerhalb der zweckbasierten Verarbeitungsvorgaben ist an vorab der *Grundsatz der Zweckbindung* relevant. Die Gebote der Zwecktransparenz wie Zweckbindung sind fester Bestandteil gesetzgeberischer Positivierungen und gerichtlicher Entscheidungen.

564 Vorgaben, die sich am Verarbeitungszweck orientieren – neben der Zweck-Mittel-Relation sind dies die Zwecktransparenz sowie die Zweckfixierung und -bindung –, sind frühe Elemente der Datenschutzregulierung. Sie bilden einen festen Bestandteil des Datenschutzrechts und finden sich im geltenden nationalen, europäischen, aber auch US-amerikanischen Datenschutzrecht.

565 In den USA wurde der Grundsatz bereits im Privacy Act von 1974 aufgenommen, der allerdings einzig Agenturen der Bundesregierung adressierte.[823] Zudem implementieren sektorielle Erlasse im privaten Bereich Vorgaben zu den Verarbeitungszwecken, so beispielhaft der Fair *Credit Reporting Act* und dessen § 604.

566 Die DSGVO statuiert Vorgaben im Zusammenhang mit dem Verarbeitungszweck innerhalb der allgemeinen Verarbeitungsgrundsätze, vgl. Art. 5 Abs. 1 lit. b–e DSGVO. Auch die Erlaubnistatbestände gemäss Art. 6 DSGVO, die festlegen, aufgrund welcher Tatbestände eine Verarbeitung von Personendaten rechtmässig ist, orientieren sich in massgeblicher Weise an Verarbeitungszwecken: So sind

821 Vgl. BGE 136 II 508, E 6.3.1.; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 13.

822 Gemäss derzeit noch in Kraft stehendem DSG genügt die Zweckerkennbarkeit, wobei allerdings mit den jüngsten Entwicklungen und im Zuge der DSGVO sowie der Totalrevision die Transparenzvorgaben markant angehoben werden.

823 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 38.

Personendatenverarbeitungen zwecks Vertragserfüllung nach Art. 6 Abs. 1 lit. b DSGVO oder zwecks Erfüllung rechtlicher Pflichten nach Art. 6 Abs. 1 lit. c DSGVO (beispielsweise zur Verhinderung von Geldwäscherei) rechtmässig.

Im geltenden schweizerischen Datenschutzgesetz kommt die Bedeutung, die dem Zweck als Instrument datenschutzrechtlicher Regulierung beigemessen wird, nicht zuletzt in dessen *dreifacher Thematisierung* zum Ausdruck: Neben seiner Relevanz im Rahmen des Verhältnismässigkeitsprinzips werden Vorgaben an den Verarbeitungszweck im DSG in Gestalt des Zweckbindungsgrundsatzes («Zweckidentität») in Art. 4 Abs. 3 DSG geregelt sowie an ein Transparenzgebot («Zweckerkennbarkeit») in Art. 4 Abs. 3, 4 DSG geknüpft. 567

Art. 4 Abs. 3 DSG lautet in seiner heute noch in Kraft stehenden Version: 568

> «Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.»

In Abs. 4 schliesst Art. 4 DSG die Vorgabe an: 569

> «Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein.»

In diesen noch geltenden Fassungen enthalten Art. 4 Abs. 3 und 4 DSG mehrere *Teilgehalte*, wobei Meier in Abs. 3 einen *Dualismus* verortet: Der Absatz beinhalte den Grundsatz der *Zweckbestimmung* (an sich) sowie den Grundsatz der Unabänderlichkeit dieses zuvor festgelegten Zwecks der Datenbearbeitung, was ebenso mit dem Begriff der Zweckbindung resp. -fixierung erfasst wird.[824] Den engen Zusammenhang von Art. 4 Abs. 3 und Abs. 4 DSG betont Rosenthal, der die Erkennbarkeit des Zweckes weitestgehend und in überzeugender Weise unter Abs. 3 abhandelt, unter Abs. 4 indessen auf die *Erkennbarkeit der Beschaffung* fokussiert.[825] 570

Zwei Anmerkungen zur nicht geglückten Gesetzesredaktion, die mit der Totalrevision und insb. Art. 6 Abs. 3 nDSG ausgemerzt wird: 571

Erstens: Wird der hinreichend konkretisierte Verarbeitungszweck gegenüber dem Datensubjekt transparent gemacht, geht damit in aller Regel zugleich Transparenz hinsichtlich der Datenbeschaffung einher. Das separate Transparenzerfordernis betreffend die Datenbeschaffung verdeutlicht gleichwohl, dass dem Moment der Erhebung als «neuralgischem» Augenblick im Zyklus der Personendatenverarbeitung besondere Aufmerksamkeit zugemessen wird: Mit der Erhebung werden Personendaten in kaum mehr kontrollierbare Netze von Datenverarbeitungsflüssen eingespeist.[826] Sodann ist zwischen Art. 4 Abs. 3 und Abs. 4 DSG eine 572

824 Meier, N 722.

825 Zur Abgrenzung der beiden Absätze Rosenthal, HK-DSG, Art. 4 N 64.

826 Für Deutschland in den Worten von Scholz/Sokol, NomosKomm-BDSG, § 13 N 5: «In dem Moment, da Daten erhoben sind, hat das Datensubjekt weitgehend die Herrschaft über seine Daten ver-

Überlappung des Regelungsinhaltes hinsichtlich der Forderung festzustellen, wonach der Bearbeitungszweck im Zeitpunkt der Datenbeschaffung transparent zu machen ist.

573 Zweitens scheint der Gesetzgeber in Bezug auf den Zweck «interne resp. externe Pflichten» zu unterscheiden. Überzeugender allerdings wäre eine chronologische Systematisierung entlang des Verarbeitungszyklus: Zweckdefinierung nach innen, Transparenzmachung des bzw. der Verarbeitungszwecke nach aussen gegenüber dem Datensubjekt, Bindung der Verarbeitungshandlungen an diesen transparent gemachten Zwecken (nach innen, als eine Art Selbstverpflichtung). Die besagten zweckbasierten Vorgaben werden in Art. 4 Abs. 3 und Art. 4 DSG geregelt, wozu das allgemeine Transparenzgebot betreffend Datenbeschaffung tritt.

574 Im Einzelnen lassen sich nach DSG vor Totalrevision demnach *vier Inhalte aus Art. 4 Abs. 3 und Abs. 4 DSG* destillieren, die alle als Pflichten der datenverarbeitenden Verantwortlichen gestaltet sind: erstens die interne *Festlegung resp. Definierung* des Bearbeitungszwecks (Abs. 3). Sie ist Vorbedingung für die zweite Vorgabe, die *Zweckerkennbarkeit* resp. *Transparentmachung* des definierten Bearbeitungszwecks nach aussen (Abs. 3, *aber auch* Abs. 4). Drittens die *Bindung resp. Fixierung* an die definierten und transparent gemachten Verarbeitungszwecke im Rahmen der Datenverarbeitungen nach innen (Abs. 3), und viertens die Gewährleistung der Erkennbarkeit der Datenbeschaffung an sich (Abs. 4). Bei Zweckänderungen sind zudem Nachinformierungen erforderlich.

575 Die Totalrevision schafft eine systematische Bereinigung in Bezug auf die Regelungen der Zweckvorgaben. Diese werden in Art. 6 Abs. 3 nDSG gebündelt. Weiter sind Art. 6 Abs. 2 sowie Abs. 4 nDSG zu beachten.[827] Die Zweckvorgaben gemäss Art. 6 Abs. 3 und Abs. 4 nDSG lauten mit der Totalrevision des DSG wie folgt:

> «[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.»
>
> «[4] Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.»

loren.» Ebendem Rechnung tragend verbürgte das Deutsche Datenschutzgesetz in seiner Version i. K. bis zum 25. Mai 2018 den Grundsatz der Direkterhebung gem. in § 4 Abs. 2 BDSG, § 6 Abs. 1 lit. b BDSG – ein solcher Grundsatz war dem Eidgenössischen Datenschutzgesetz stets fremd.

827 EJPD, Erläuternder Bericht, 46.

4.2. Die zweckbasierten Verarbeitungsvorgaben – Teilgehalte

4.2.1. Zweckdefinierung resp. -fixierung

576 Der Verarbeitungszweck resp. die Verarbeitungszwecke müssen im Zeitpunkt der Verarbeitung und damit insb. auch der Beschaffung hinreichend konkret bestimmt sein, vgl. unmissverständlich Art. 6 Abs. 3 nDSG.

577 Unter noch geltendem DSG wird in an dieser Stelle das Verbot der *Vorratsdatenspeicherung* akzentuiert.[828] Die Vorratsdatenspeicherung ist prinzipiell unzulässig. Sie wird unter dem hier gewählten Untertitel resp. -begriff der Zweckfixierung (sowie dem Grundsatz der Verhältnismässigkeit) thematisiert: Nach dieser ist es unzulässig, Personendaten *ohne einen im Vorfeld bestimmten resp. definierten und fixierten Zweck* zu erheben. Eine «Blanko-Erhebung», eben auf Vorrat hin, um gesammelte Personendaten erst später zu jeweils ad hoc festgelegten Zwecken zu bearbeiten, ist nicht rechtens.[829] Der Verhinderung der sog. Vorratsdatenspeicherung dienen weiter die Transparenzvorgaben betreffend den Verarbeitungszweck. Bereits im Zeitpunkt der Beschaffung von Personendaten muss der Zweck, zu dem die Personendaten verarbeitet werden sollen, hinreichend präzis fixiert sein, um alsdann gegenüber dem Datensubjekt transparent gemacht zu werden, vgl. neben Art. 6 Abs. 3 nDSG auch Art. 19 Abs. 2 lit. b nDSG.

578 In Bezug auf eine dergestalt initiale Zweckfixierung ist auf Art. 5 Abs. 1 lit. b DSGVO hinzuweisen. Die Bestimmung verlangt, dass Personendatenverarbeitungen zu einem *vorab festgelegten*, für das Datensubjekt überschaubaren Zweck erfolgen müssen. Diese Anbindung muss für die Aufsichtsbehörde kontrollierbar sein.[830] Die «interne» Zweckfixierung hat hinreichend granular zu erfolgen, damit die Rechtmässigkeit der Verarbeitungshandlung überprüfbar wird. Bezüglich der Zweckfixierung sind keine Formerfordernisse vorgesehen. Immerhin müssen die Verarbeitungszwecke im Verarbeitungsverzeichnis, vgl. Art. 30 Abs. 1 lit. b DSGVO und Art. 12 Abs. 2 lit. b nDSG, aufgeführt werden. Zudem bildet der Verarbeitungszweck ein Element einer allfälligen Datenschutz-Folgenabschätzung, vgl. Art. 35 Abs. 7 lit. a DSGVO und Art. 22 Abs. 2 nDSG.

828 Vgl. Rosenthal, HK-DSG, Art. 4 N 31.
829 Vgl. Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.85; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 14.
830 Herbst, BeckKomm-DSGVO, Art. 5 N 22.

4.2.2. Zwecktransparenz

4.2.2.1. Gesetzliche Anforderungen

579 Die vorgängige «interne» Festlegung des Zweckes der Personendatenverarbeitung für bestimmte Personendaten ist sodann gegenüber den Datensubjekten *transparent* zu machen. Die von Personendatenverarbeitungen betroffenen Personen sollen wissen, wofür ihre Personendaten erhoben und verarbeitet werden.[831]

580 Das noch geltende *Erkennbarkeitsgebot* gemäss Art. 4 Abs. 4 DSG, das auch spezialgesetzlich verankert ist (vgl. für den Bereich der Privatversicherungen Art. 3 Abs. 1 lit. g und Art. 3a VVG) hat einen *doppelten Bezug*. Es verlangt erstens, dass die Beschaffung von Personendaten an sich erkennbar ist, und zweitens, dass der Bearbeitungszweck erkennbar ist. Ratio legis von Art. 4 Abs. 4 DSG ist die Erhöhung der Transparenz.[832] Mit der Totalrevision ist die Zwecktransparenz in Art. 6 Abs. 3 nDSG niedergelegt. In Art. 19 Abs. 2 lit. b nDSG findet sich eine explizite Informationspflicht über den Verarbeitungszweck bei der Beschaffung von Personendaten. Die Erkennbarkeit genügt nicht mehr, womit sich ebenso in diesem Punkt das mit der Totalrevision verfolgte Ziel der erhöhten Transparenz niederschlägt.

581 Das Transparenzgebot betreffend den Verarbeitungszweck beanspruchte bereits vor dessen ausdrücklicher Fixierung in Art. 4 Abs. 4 DSG Gültigkeit. Das Gebot der Erkennbarkeit von Beschaffung wie Bearbeitungszweck wurde – wie gezeigt – auch aus Treu und Glauben resp. – in der Terminologie der Europaratskonvention 108 oder derjenigen der EG-Richtlinie 95/46 – aus dem Loyalitätsgebot abgeleitet.[833] Der Ausbau der Transparenzvorgaben als Instrument datenschutzrechtlicher Regulierung lässt sich spezifisch mit Blick auf den Bearbeitungszweck nachzeichnen. In den ausgebauten Transparenzvorgaben hinsichtlich des Bearbeitungszwecks werden zwei Kernelemente zeitgemässer Datenschutzregulierung fusioniert: die Transparenz und der Zweck. Die *Transparenz hinsichtlich des Verarbeitungszweckes* bildet ein Kernanliegen des Datenschutzes.[834]

582 Anzugeben ist ein *korrekter* Zweck. Der Versuch, unter Vorspiegelung falscher Zielsetzungen an Daten zu gelangen, ist unzulässig.[835] Zudem müssen Bearbeitungszwecke hinreichend konkret umschrieben werden, um dem Transparenzge-

831 Peter, 126 f.; BBl 1988 II 414 ff., 451; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 13; vgl. Abschnitt 4.1.3. zur Zwecktransparenz.
832 Botschaft DSG 2003, 2101 ff., 2124.
833 Vgl. Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 8; zum Ausbau von Transparenzvorgaben namentlich über Treu und Glauben vgl. zweiter Teil, V. Kapitel, B.2., insb. B.2.3.
834 Hannich/Jenni/Beerli/Mandl, in: ZHAW (Hrsg.), 45; zur Wichtigkeit dieses Grundsatzes BGE 136 II 508, E 6.3.1.
835 Vgl. Buchner m. w. H., 148.

bot zu genügen.[836] Mehrere Zwecke sind möglich, sofern jeder einzelne jeweils genügend granular umrissen wird.[837]

583 Gemäss Art. 4 Abs. 3 und Abs. 4 DSG muss die Beschaffung von Personendaten sowie der Verarbeitungszweck *erkennbar* sein. Nicht verlangt wird damit von Gesetzes wegen eine aktive oder schriftliche Informierung. Allerdings wird eine solche aus Beweisgründen regelmässig vorgenommen.[838] In Art. 4 Abs. 3 und Abs. 4 DSG werden unterschiedliche Wendungen eingesetzt, die folglich zu harmonisieren sind: Der bei der Datenbeschaffung erkennbare Zweck muss dem bei der Datenbearbeitung verfolgte Zweck entsprechen.[839] Immerhin: Mit der expliziten und separaten Vorgabe in Art. 4 Abs. 4 DSG, wonach der Zweck der Datenbearbeitung im Zeitpunkt der *Erhebung* erkennbar sein muss, symbolisiert der Gesetzgeber die Relevanz des Zeitpunktes der Datenerhebung und der insofern notwendigen Transparenz. Ebendies hat namentlich für den privaten Bereich Bedeutung, der gerade nicht von einem grundsätzlichen Verarbeitungsverbot ausgeht. Sobald personenbezogene Daten erhoben worden sind, verlieren Subjekte – Datenschutzgesetz und *behauptetem* Recht auf informationelle Selbstbestimmung zum Trotz[840] – weitgehend die Kontrolle über die sie betreffenden Angaben.[841]

584 Wenn das in Kraft stehende DSG zumindest für den privaten Bereich auf eine aktive Informationspflicht dem Grundsatz nach verzichtet, ist zweierlei hervorzuheben:

585 Erstens ist in Bezug auf das duale System und den öffentlichen Bereich die Gesetzesänderung aus dem Jahr 2010 in Erinnerung zu rufen. Mit dem BGG vom 19. März 2010 über die Umsetzung des Rahmenbeschlusses 2008/977/JI über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen wurden die Art. 18a und 18b ins DSG eingefügt. Art. 18a DSG verlangt, dass Bundesbehörden die betroffenen Personen über die Beschaffung und den Zweck der Verarbeitung der personenbezogenen Daten *zu*

836 Für eine normative Betrachtung tritt ein Rosenthal, HK-DSG, Art. 4 N 34; vgl. hierzu Art. 5 Abs. 1 lit. b DSGVO, wonach personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden müssen; zur hinreichenden Bestimmtheit vgl. Art. 29 Datenschutzgruppe WP 203, 16 mit Beispielen.

837 Vgl. implizit Rosenthal, HK-DSG, Art. 4 N 25; nach DSGVO Herbst, BeckKomm-DSGVO, Art. 5 N 36.

838 Vgl. auch Rosenthal, HK-DSG, Art. 4 N 36.

839 Was das Transparenzerfordernis bezüglich des Zwecks im Zeitpunkt der Datenbeschaffung anbelangt, geht Art. 4 Abs. 4 in Abs. 3 DSG auf. Zur synonymen Verwendung von *aus den Umständen* ersichtlich i. S. v. Abs. 3 und erkennbar i. S. v. Abs. 4 auch Rosenthal, HK-DSG, Art. 4 N 34. Die Datenbeschaffung ist bereits eine Datenbearbeitung. Der bei der Datenbeschaffung erkennbare Zweck von Art. 4 Abs. 4 DSG wird über Art. 4 Abs. 3 DSG perpetuiert. Eine Änderung des bei der Beschaffung erkennbar gemachten Zweckes ist grundsätzlich nicht zulässig.

840 EJPD, Bericht Bundesrat, 38 f.; BGE 140 I 2, E 9.1.

841 Vertiefend hierzu zweiter Teil, VI. Kapitel.

informieren haben. Ebendiese Pflicht gilt auch, wenn Daten bei Dritten beschafft werden. Sie beschränkt sich keineswegs auf die Verarbeitung personenbezogener Daten im Kontext der polizeilichen oder justiziellen Zusammenarbeit.[842] Immerhin kann die Informationspflicht gemäss Art. 18a Abs. 4 sowie Art. 18b DSG entfallen oder eingeschränkt sein. Denn Art. 18a DSG sieht gemäss der im Nachvollzug erfolgten Novellierung des Datenschutzgesetzes von 2010 dem Grundsatz nach für den öffentlichen Sektor eine Informationspflicht unabhängig von der Datenart vor.[843] Der Erkennbarkeitsgrundsatz gemäss Art. 4 Abs. 3 und Abs. 4 DSG ist somit im öffentlichen Bereich zur Ausnahme geworden, die Ausnahme zum Grundsatz.

586 Zweitens gilt für den privaten Bereich eine aktive Informationspflicht über den Verarbeitungszweck gemäss Art. 14 Abs. 2 lit. b DSG bei der Beschaffung *besonders schützenswerter Daten oder Persönlichkeitsprofile*, vgl. Art. 3 lit. c und lit. d DSG. Eine Verletzung der Informationspflicht kann gemäss Art. 34 Abs. 1 lit. a DSG strafrechtlich mit einer Busse in Höhe von bis zu CHF 10‘000.00 sanktioniert werden.

587 Folglich greift im noch geltenden DSG eine graduelle Abstufung der Transparenzvorgaben hinsichtlich den Verarbeitungszweck: Je umfassender, komplexer und längerfristiger die Bearbeitung, je sensibler die Daten, desto höher die Anforderungen an die Erkennbarkeit. Zu berücksichtigen sind weiter die Möglichkeiten des Datenbearbeiters und die Gepflogenheiten einer Branche.[844] Für eine eigentliche Informationspflicht wird im Anwendungsgebiet des Customer Relationship Management (CRM) plädiert:

> «Die Transparenz der Datenbearbeitung stellt ein fundamentales Prinzip des Datenschutzes dar. Aus datenschutzrechtlicher Sicht ist die Verwendung der Personendaten zu Werbe- und Direktmarketingzwecken insofern problematisch, als sie für die betroffenen Kunden zum Zeitpunkt, an dem deren Daten gesammelt werden, nicht ohne weiteres ersichtlich ist. Die Kunden müssten zum Datenschaffungszeitpunkt somit insofern informiert werden.»[845]

588 Folglich wird für Situationen, in denen Beschaffung und Zweck nicht resp. nicht eindeutig erkennbar sind, eine aktive Informationspflicht selbst ausserhalb von Art. 14 Abs. 2 lit. b DSG eingefordert.[846]

842 Taormina, BSK-DSG, Art. 18a N 1.
843 Zum Ganzen auch Meier, N 692 ff.
844 Ders., N 708.
845 Vgl. Passadelis, ZHAW (Hrsg.), 51; früh zu Marketing und Datenschutz die wirtschaftswissenschaftliche Dissertation von Schineis, *passim*.
846 Vgl. Rosenthal, HK-DSG, Art. 4 N 51 m. w. H. auf Erläuterungen des EDÖB; die Transparenz wird im Rahmen von Kundenbindungssystemen neben der individuellen Ansprache als Interesse der Kundinnen und Kunden ebenso beschrieben von Eckhardt/Fattebert/Keel/Meyer, 4 ff.

589 Das *abgestufte Transparenzsystem des noch geltenden DSG* – in Bezug auf den Verarbeitungszweck für den privaten Sektor – bildet konzeptionelle eine Orientierung an den Auswirkungen ab, die Personendatenverarbeitungen auf die *Persönlichkeitsrechte* zugemessen werden.[847]

590 Das Transparenzgebot will der Vorstellung zum Durchbruch verhelfen, wonach der Mensch als Subjekt und die Persönlichkeit ebenso im Rahmen der Datenbearbeitungsprozesse zu schützen ist. Transparenzvorgaben werden als Garant wahrgenommen, den Menschen nicht zum blossen Objekt der Datenbearbeitung verkommen zu lassen.[848] Das Transparenzgebot (und dessen Parameter) gemäss Art. 4 Abs. 4 DSG geben dem Individuum die Möglichkeit, Ansprüche nach Art. 12 Abs. 2 lit. b oder Art. 8 DSG geltend zu machen.[849] Sodann werden die Anforderungen an die Transparenz mit der Schwere der Persönlichkeitsbeeinträchtigung zu korrelieren gesucht. Hierbei orientiert man sich an einer dichotomisch gedachten Struktur: Bei «gewöhnlichen Personendaten» müssen die Beschaffung sowie der Zweck gemäss Art. 4 Abs. 4 DSG bloss erkennbar sein.[850] Nur bei besonders schutzwürdigen Personendaten und Persönlichkeitsprofilen greifen *de lege lata* qualifizierte Transparenzerfordernisse. Im Ergebnis beschränkt sich Art. 4 Abs. 4 DSG damit in seiner Anwendbarkeit auf Personendatenverarbeitungen durch Private, welche keine sensiblen Daten sammeln oder Persönlichkeitsprofile bearbeiten.[851] *De lege lata* wird somit hinsichtlich der Transparenzvorgaben auch betreffend den Verarbeitungszweck ein höheres Schutzniveau für den öffentlichen gegenüber dem privaten Bereich vorgesehen.[852]

591 Wie aber wird unter dem DSG vor seiner Totalrevision rechtsgenügend Transparenz bezüglich den Verarbeitungszweck geleistet? Für den öffentlichen Sektor spielt insofern das Legalitätsprinzip eine Rolle, über welches eine gewisse Transparenz, Rechtssicherheit sowie Normenkonkretheit geschaffen wird. Die Frage, *wann* eine Datenbearbeitung und deren Zweck als erkennbar gelten können, ist dennoch und gerade für den privaten Bereich nicht geklärt.[853] Die Entwicklung einer kohärenten Praxis, die justiziable Kriterien für das Erkennbarkeitserfordernis herausbildet, wird durch die Forderung, dass dieses für jeden Einzelfall zu prüfen sei,[854] durchkreuzt. Im Logistep-Urteil hatte das Bundesgericht einen

847 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 8; Meier, N 708.
848 BBl 2003, 2126.
849 Vgl. Rosenthal, HK-DSG, Art. 4 N 57; ablehnend Meier, N 697.
850 Bereits früh trat der Datenschutzbeauftragte für die Einführung einer allgemeinen Informationspflicht auch im Lichte der internationalen Regelungen ein, was indes von der Arbeitsgruppe abgelehnt wurde. Die Erkennbarkeit solle bei «normalen Daten genügen, eine Informationspflicht wäre eine unverhältnismässige Belastung für die Datenbearbeiter», Botschaft DSG 2003, 2101 ff., 2124 f.
851 Meier, N 694.
852 Mit der Totalrevision wird für beide Bereiche eine aktive Informationspflicht auch mit Blick auf den Verarbeitungszweck eingeführt, Art. 19 Abs. 2 lit. b nDSG.
853 Botschaft DSG 2003, 2101 ff., 2125.
854 Vgl. Epiney/Civitella/Zbinden, 27.

Grundsatzverstoss moniert, ohne die Anforderungen an das Erkennbarkeitsgebot zu umreissen.[855]

592 Aspekte der Datenbeschaffung, die erkennbar sein müssen, sollen gemäss Botschaft zum ersten DSG nach den Grundsätzen der Verhältnismässigkeit sowie von Treu und Glauben definiert werden.[856] Hinsichtlich die Zweckerkennbarkeit wird Unterschiedliches vertreten. Eine Meinung geht dahin, dass der Zweck aus den Umständen ersichtlich sei, wenn die betroffene – am Schicksal ihrer Daten interessierte, aufmerksame – Person bei der Bearbeitung in guten Treuen von einem bestimmten Zweck ausgehen musste –, selbst wenn sie nicht explizit über den Zweck informiert worden war oder keine Kenntnis davon genommen hatte.[857] So sollen beispielsweise beim Antrag für eine Kundenkarte die Kontaktangaben zur Abwicklung des Vertrags, zur Buchführung und allenfalls auch zur Durchsetzung von Ansprüchen auf dem Rechtsweg verwendet werden können.[858] Trotz Fehlens eines Hinweises müsse wohl auch mit der Verwendung zu Werbe- und Marketingzwecken durch das betreffende Unternehmen gerechnet werden.[859]

593 Anders der EDÖB, nach welchem verdeckte kommerzielle Datenerhebungen, bei welchen Werbezwecke nicht klar ersichtlich werden, unzulässig sind.[860] Im Übrigen ist es nicht die Aufgabe des Betroffenen, danach zu «suchen»[861]; vielmehr ist das Transparenzgebot eine Pflicht der Verantwortlichen. Dem Betroffenen werden von Gesetzes wegen – ausser aus Treu und Glauben – keine Aufgaben zugewiesen; es ist allein der Datenbearbeiter, der potentiell in die Persönlichkeit des Betroffenen eingreift, weshalb auch er derjenige ist, der für die Erkennbarkeit gemäss Art. 4 Abs. 4 DSG zu sorgen hat. Ist Zweck des Datenschutzgesetzes der Schutz der Persönlichkeit, entspricht eine solche Auslegung der ratio legis.

594 An die Datensubjekte dürfen als Folge davon keine zu hohen Erwartungen gestellt werden, auch nicht über eine Standardformulierung, wonach eine Person vorausgesetzt wird, welche «eine gewisse Aufmerksamkeit und ein Interesse am Schicksal ihrer Daten aufweisen muss».[862]

595 Datenschutzrechtliche Transparenzvorgaben werden in der Praxis meistens standardisiert gewährleistet. Das DSG vor seiner Totalrevision äussert sich *nicht zu Modalitäten oder Formen*, beispielsweise, wie die Erkennbarkeit zu gewähr-

855 BGE 136 II 508, E 6.3.1.
856 Botschaft DSG 2003, 2101 ff., 2125.
857 Rosenthal, HK-DSG, Art. 4 N 34 ff.; Botschaft DSG 2003, 2101 ff., 2124.
858 Botschaft DSG 2003, 2101 ff., 2125; vgl. Rosenthal, HK-DSG, Art. 4 N 35.
859 Rosenthal, HK-DSG, Art. 4 N 35 und 47; Botschaft DSG 2003, 2101 ff., 2125; a. M. Althaus Stämpfli, 95.
860 EDÖB, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/merkblaetter/erhebung-von-personendaten-fuer-marketingzwecke.html> (zuletzt besucht am 30. April 2021) mit vielen Hinweisen zum Marketing.
861 Zum Ausdruck Rosenthal, HK-DSG, Art. 4 DSG N 36.
862 Ders., a. a. O., Art. 4 N 34 ff.; Botschaft DSG 2003, 2101 ff., 2124.

leisten oder einer Informationspflicht nachzukommen ist. Unter der Ära des DSG vor Totalrevision kommt allgemeinen Geschäftsbedingungen eine zentrale Rolle zu. Es gilt als zulässig, die Erkennbarkeit auch des Zecks mittels AGB zu gewährleisten, sofern diese zugänglich sind. Die Erkennbarkeit gelte selbst dann als gegeben, wenn die betroffene Person diese nicht gelesen habe.[863] Gleichwohl liess sich ebenso in der Schweiz die Etablierung einer Praxis beobachten, wonach datenschutzrechtliche Transparenzvorgaben und Einwilligungstatbestände aus allgemeinen Geschäftsbedingungen ausgelagert und in separate, spezifische Datenschutzerklärungen integriert werden.

596 Betreffend Gestaltung und Granularität, gerade auch der Zwecktransparenz, finden sich mit Blick auf das geltende DSG viele Unklarheiten: Umstritten ist, inwieweit ein ungewöhnlicher Zweck speziell hervorzuheben ist.[864] Es scheint zulässig, mehrere Bearbeitungszwecke (in einer einzigen Klausel) anzuführen, es sei denn, es resultiere ein eigentlicher Zwang für das Datensubjekt infolge einer monopolartigen Machtstellung der datenverarbeitenden Stelle. Für den Fall, dass Bearbeitungszwecke nicht abschliessend aufgeführt werden (was m. E. allerdings bereits unter geltendem Recht problematisch ist), habe eine Interpretation nach Treu und Glauben zu erfolgen.[865] Innerhalb der Auslegungsfragen wird für die Anwendbarkeit der Interpretationsregel «in dubio contra stipulatorem» eingetreten. Eine Klausel «Bearbeitung zu Werbezwecken» wäre dementsprechend wohl als «Bearbeitung zu eigenen und nicht auch zu fremden Werbezwecken» zu verstehen.

597 Mit der Totalrevision verlangt Art. 19 Abs. 2 lit. b nDSG eine *Informierung über den Zweck*. Die Gewährleistung der Erkennbarkeit wird mit dem Inkrafttreten der neuen Fassung (trotz Art. 6 Abs. 3 nDSG) nicht mehr genügen, um den Transparenzvorgaben betreffend den Verarbeitungszweck zu genügen. Unbestritten dürfte sein, dass die Erkennbarkeit gemäss Art. 6 Abs. 3 nDSG in Bezug auf den Verarbeitungszweck durch Art. 19 Abs. 2 lit. b nDSG und die ebenda niedergelegte Informationspflicht übersteuert wird. Neu wird somit über den Verarbeitungszweck im Zeitpunkt der Beschaffung zu informieren sein.

598 Nach DSGVO erstreckt sich die aktive Informationspflicht auf alle im Zeitpunkt der Erhebung angestrebten Zwecke, wobei diese in hinreichender Granularität aufgeführt werden müssen. So formulieren die Art. 5 Abs. 1 lit. a DSGVO und Art. 12 ff. DSGVO, insofern insb. Art. 13 Abs. 2 und Art. 14 DSGVO weit- und tiefgreifende Informationspflichten.[866] Der resp. die Verarbeitungszwecke sind nicht nur in den Datenschutzerklärungen, sondern auch in allfällig erforderlichen

863 Meier, N 712.
864 Befürwortend Rosenthal, HK-DSG, Art. 4 N 37; ablehnend wohl Meier, N 712.
865 Meier, N 707.
866 DSGVO ErwG 39.

Einwilligungserklärungen, dem Verarbeitungsverzeichnis und den Datenschutz-Folgenabschätzungen aufzuführen.[867] Sodann bildet der Verarbeitungszweck den Inhalt der Antwort auf ein Auskunftsbegehren gemäss Art. 15 Abs. 1 lit. a DSGVO; er ist einschlägig im Rahmen des Löschungsbegehrens, Art. 17 Abs. 1 lit. a DSGVO, sowie des Berichtigungsbegehrens, Art. 16 DSGVO.[868] Damit lässt sich festhalten, dass im Zuge der jüngsten rechtlichen Entwicklungen und namentlich der DSGVO die Transparenzmachung, die Dokumentations- und Rechenschaftspflicht auch in Bezug auf den Verarbeitungszweck eine beachtliche Aufwertung erfahren haben. Zum einen muss das Datensubjekt in hinreichender Differenziertheit über die Verarbeitungszwecke informiert werden. Zum anderen werden die Definierung und Festlegung des Verarbeitungszweckes im Rahmen von Verarbeitungsverzeichnissen, Datenschutz-Folgenabschätzungen, aber auch von Löschungskonzepten usf. zu einem eigentlichen Instrument der Rechenschaft: Datenverarbeitende haben sich stets den einmal festgelegten Verarbeitungszweck vor Augen zu halten und sind entsprechend in ihren Verarbeitungsmöglichkeiten an diesen gebunden. Die Transparentmachung des Verarbeitungszweckes im Verarbeitungsverzeichnis dient dazu, die Rechtmässigkeit der Personendatenverarbeitung zu überprüfen.

4.2.2.2. Transparenz betreffend unmittelbare und mittelbare Verarbeitungszwecke

599 Eine Kernherausforderung der *Zwecktransparenz* – ungeachtet ihrer Ausgestaltung als Erkennbarkeitsforderung oder einer Informationspflicht – liegt in den pluralen Verarbeitungszwecken. Verarbeitungszwecke sind regelmässig nicht «monistisch», stattdessen facettenreich. Es geht hier nicht darum, die rechtsgenügliche Informierung resp. Transparenz in Bezug auf mehrere, nebeneinanderstehende Verarbeitungszwecke und die Umsetzung in der Praxis präziser zu beleuchten.

600 Vielmehr interessiert der Befund, wonach Verarbeitungshandlungen in der Regel nicht nur einem *unmittelbaren, sondern darüber hinaus einem mittelbaren Zweck dienen*, namentlich ökonomischen Interessen der datenverarbeitenden Unternehmen. Der Logistep-Entscheid illustrierte den Befund: Die Beklagte machte geltend, dass der Zweck der Datenerhebung und -bearbeitung die Aufdeckung von Urheberrechtsverletzungen sei; das private Unternehmen, das mit der Verarbeitung beauftragt worden war und die notwendige Software anbot, handelte aus rein wirtschaftlichem Interesse.[869]

867 DSGVO ErwG 32 und ErwG 42.
868 DSGVO ErwG 65.
869 BGE 136 II 508.

Längst sind Wendungen wie «Ihre Daten sind Gold wert» oder «Kommerzialisierung der Persönlichkeit resp. von Personendaten» zum Topos des allgemeinen resp. juristischen Jargons geworden. Sie artikulieren, dass ein Endzweck von Datenverarbeitungen oft die Generierung von Geld für die verarbeitenden Unternehmen ist. Für die *Datensubjekte* allerdings sind Zusammenhänge zwischen Personendatenverarbeitungen und deren mittel- wie unmittelbaren Zwecken oftmals undurchsichtig. Was ist damit gemeint: 601

Mark Zuckerberg von Facebook hat stets betont, dass er die Welt verbessern wolle, indem er die Menschen vernetze, diesen eine Plattform biete, damit sie ihre Beziehungen pflegen könnten.[870] Die *Nutzung des Dienstes, der sozialen Plattform*, kostet kein Geld. Dennoch erfolgt sie nicht unentgeltlich: Personendaten sind die Währung.[871] Die Tatsache, dass Personendatenverarbeitungen in aller Regel für die Verarbeitenden neben einem unmittelbaren Zweck einen mittelbaren Zweck erfüllen, und zwar die Generierung von wirtschaftlichen Gewinnen, ist für die Datensubjekte bei den im *Internet* angebotenen und genutzten Diensten bis heute nicht offensichtlich. 602

Auch im Bereich des Marketings finden sich mit Blick auf die datenschutzrechtliche Zwecktransparenz kritische Praktiken,[872] wobei sich diese für die Schweiz anhand der weit verbreiteten und wohl bekannten Supercard von Coop resp. Cumulus-Karte der Migros illustrieren lassen. Zu letzterer war auf der Homepage der Migros viele Jahre – mittlerweile allerdings angepasst – zu lesen: 603

> «Cumulus ist das kostenlose Bonusprogramm der Migros. Das Cumulus-Bonusprogramm – unsere Art, uns für Ihre Treue zu bedanken».

Eine dergestaltige Formulierung erweckt *erstens* den Eindruck, dass ein «Bonus» für die *Treue* entrichtet wird, und *zweitens*, dass dieser «Bonus» ein Geschenk (eine Zuwendung resp. Leistung ohne Gegenleistung) ist. Die elektronische Erfassung des Einkaufsverhaltens wird präsentiert, als ob sie zum Zwecke der Evaluierung der «Treue» erfolge, also primär darauf ausgerichtet sei, das *Einkaufsvolumen* zu ermitteln. Dies ist in doppelter Hinsicht missverständlich: Denn mit der Cumulus-Karte wird keineswegs primär oder gar ausschliesslich Kundentreue belohnt. Das lässt sich dadurch belegen, dass sowohl Coop wie Migros klassische Treueprogramme wie *papierne Markensysteme* kennen. Die elektronische Kundenkarte hingegen ist gerade auch darauf ausgerichtet, personen- 604

870 NZZ am Sonntag, Die Naivität Zuckerbergs ist eine Gefahr für die Demokratie, November 2017, <https://nzzas.nzz.ch/notizen/naivitaet-zuckerbergs-ist-eine-gefahr-fuer-demokratie-ld.1326328> (zuletzt besucht am 30. April 2021).

871 Zu Daten als Entgelt statt vieler Weber/Henseler, SZW 2019, 335 ff.

872 Hierzu Buchner, 147 ff.; vertiefend zu Marketing, Datenschutz und Internet Sachs, *passim*.

bezogene Daten zu generieren und damit u. a. Direktmarketing zu betreiben.[873] Das Cumulus-Kundenprogramm ist somit keineswegs «kostenlos», weshalb eine entsprechende Formulierung auf der Eingangsseite aus datenschutzrechtlicher Perspektive problematisch ist.[874] Seit September 2016 findet man unter einem der zahlreichen Links zum Programm jeweils eine aktuelle, ausführliche Datenschutzerklärung.[875] Um die Zustimmung zu diesem mehrseitigen Dokument bittet die Migros ausdrücklich. Sie wählt damit den Weg, aus Vorsicht und Respekt «vor der Selbstbestimmung» systematisch die Einwilligung einzuholen, selbst wenn diese nicht verlangt wäre von Gesetzes wegen.[876]

605 Das Illustrationsexempel fördert mehrere Herausforderungen zu Tage: Vorab wurde auf der Eingangsseite ein falscher Eindruck erweckt hinsichtlich der Ziele resp. Zwecke sowie Entgeltlichkeit des «Treueprogramms»; die Erhebung von Personendaten erfolgt, wie erwähnt, keineswegs primär und exklusiv zum Zweck, die Treue der Kundschaft zu bewerten und zu verdanken. Sodann erscheint der Weg, Datenbearbeitungen über die Einwilligung zu legitimieren, zumindest theoretisch nachvollziehbar. Er kann in einer Gesellschaft, welche die Selbstbestimmung akzentuiert, als Erfüllung einer sozialen Erwartung qualifiziert werden. In der Realität jedoch laufen solche Einwilligungserklärungen gewissermassen ins Leere: Kaum jemand studiert so detaillierte Dokumente; tut man es doch, so verliert man in aller Regel den Überblick, wer welche Personendaten zu welchem Zweck verarbeitet. Es erstaunt damit auch nicht, dass das Instrument der informierten Einwilligung gerade im Bereich des Online-Tracking und Advertising als illusorisch resp. Fiktion bezeichnet wird.[877] Zudem konterkarieren solche Einwilligungserklärungen m. E. das datenschutzrechtliche Transparenzgebot: Dort, wo Datenschutzeinwilligungen eingeholt werden, obschon gesetzlich nicht verlangt, wird dem Datensubjekt gegenüber eine Rechtsposition suggeriert, die es de facto/ex lege nicht hat. Es wird Intransparenz geschaffen.

873 Vertiefend zu Daten als Leistung, um im Austausch gegen Personendaten Rabatte, Boni usf. zu erlangen, rechtsvergleichend und auch mit Blick auf die Strukturen des Deutschen, Österreichischen und Schweizer Datenschutzrechts Langhanke, 26 ff.

874 In eine solche Richtung auch Buchner, 148.

875 Vgl. Migros, Cumulus Datenschutz, Zürich 2021, <https://www.migros.ch/de/cumulus/ueber-cumulus/datenschutz.html> (zuletzt besucht am 30. April 2021).

876 Vgl. zu diesem Thema Meier, N 714.

877 Vgl. die Beiträge von Barocas/Nissenbaum; kritisch auch Radlanski, 16; m. w. H. Heuberger, N 285 ff.; die Problematik wird im Rahmen der Darstellung der Wirksamkeit datenschutzrechtlicher Regulierungen genauer beleuchtet, vgl. hierzu dritter Teil, VIII. Kapitel, B.2.2.; vgl. zum Firefox-Browser das Add-on «TrackMeNot», das privacy bei Internetsuchen gewährleisten will, Howe/Nissenbaum, in: Kerr/Steeves/Lucock (Hrsg.), 417 ff., 417; kritisch zur faktischen Effektivität des «consent» im Datenschutzrecht Schermer/Custers/van der Hof, Ethics Inf. Technol., 117 ff.; früh auf die Untauglichkeit der Zustimmung sowie die Unredlichkeit, sich hinter der Freiwilligkeit einer Informationserteilung zu verschanzen, hingewiesen hat Simitis, in: Schlemmer (Hrsg.), 67 ff., 77.

4.2.3. Die Zweckbindung im engeren Sinne

606 Mit der Zweckbindung im engeren Sinne ist die Vorgabe angesprochen, wonach *Personendatenverarbeitungen nur zu jenem Zweck verarbeitet werden dürfen, wie er vorab fixiert und transparent gemacht wurde*. Anders gewendet: Die zu einem bestimmten Zweck erhobenen Personendaten sollen nicht «zweckentfremdet» werden.[878] Die Zweckbindung i. e. S. wird in Art. 4 Abs. 3 DSG resp. Art. 6 Abs. 3 nDSG, letzter Satz niedergelegt («sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist»).

607 Die Kommentarliteratur zur DSGVO umschreibt den Inhalt des Zweckbindungsgrundsatzes, wie er in Art. 5 Abs. 1 lit. b DSGVO niedergelegt ist, als «Perpetuierung» des ursprünglich festgelegten und legitimen Verarbeitungszweckes. Allerdings gilt nicht jede Verarbeitung zu einem anderen Zweck als Verstoss gegen das entsprechende Gebot von Art. 5 lit. b DSGVO. Vielmehr soll nur die Weiterverarbeitung zu einem anderen Zweck, der mit dem ursprünglichen Zweck nicht kompatibel ist, verboten sein. Wie indes die Grenzlinie der «Vereinbarkeit» resp. «Unvereinbarkeit» eines ursprünglichen Verarbeitungszweckes mit einem neuen Verarbeitungszweck zu definieren ist, bleibt unklar.[879] Der Verarbeitungsgrundsatz der Zweckbindung soll die Zweckbindung auf je konkrete Konstellationen beziehen.[880]

608 Zentrales Thema im Rahmen der Zweckbindung ist somit die sog. *Zweckänderung*. Sie gilt als Verstoss gegen den Zweckbindungsgrundsatz gemäss Art. 4 Abs. 3 DSG.[881] Nach Art. 13 Abs. 3 DSGVO muss der Verantwortliche bei einer Zweckänderung eine *Nachinformation* vornehmen und, sofern geboten, eine entsprechende Einwilligung einholen. Auch nach DSG gilt, dass eine Modifikation der Bearbeitungszwecke transparent zu machen ist und ggf. eine Nachinformation zu erfolgen hat resp. eine Einwilligung hierfür einzuholen ist.[882]

609 Zudem werden aus dem Zweckbindungsgebot, wie erwähnt, *Löschungspflichten* abgeleitet: So sind beispielsweise Aufnahmen von Videokameras in öffentlichen Räumen zu löschen, sobald ihnen keine Aktualität mehr hinsichtlich Aufklärung und Verhinderung von Störungen des öffentlichen Friedens oder von Straftaten zukommt.

878 Vgl. Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.81 f.
879 Hierzu Reimer, NomosKomm-DSGVO, Art. 5 N 24 f.
880 Vgl. Herbst, BeckKomm-DSGVO, Art. 5 N 22.
881 Rampini, BSK-DSG, Art. 12 N 9.
882 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 14 mit zahlreichen Beispielen für Persönlichkeitsverletzungen durch Zweckänderungen; zur Einwilligung als Rechtfertigungsgrund: Rampini, BSK-DSG, Art. 13 DSG N 3 ff.

610 Die DSGVO flankiert das Zweckbindungsgebot mit weiteren Bestimmungen, namentlich dem Grundsatz der Datenminimierung und Speicherbegrenzung, Art. 5 Abs. 1 lit. c und lit. e DSGVO. Hieran anknüpfend verlangt Art. 5 Abs. 1 lit. e DSGVO, dass Personendaten, sobald sie zur Erfüllung des vordefinierten Verarbeitungszweckes nicht mehr erforderlich sind (und kein anderweitiger Legitimationsgrund für die weitere Verarbeitung vorliegt, wie beispielsweise gesetzliche Aufbewahrungspflichten, aber auch die Weiterverarbeitung zu sog. sekundären Zwecken wie Archiv-, Forschungs- und Statistikzwecken), endgültig *gelöscht* oder *anonymisiert* werden müssen.[883] Mit der Totalrevision werden entsprechende Pflichten explizit in Art. 6 Abs. 4 nDSG normiert. Löschungs- und Anonymisierungspflichten dienen folglich der Umsetzung des Zweckbindungsgrundsatzes sowie des Verhältnismässigkeitsprinzips. Sichtbar wird an dieser Stelle die Korrelation zwischen datenschutzrechtlichem Verhältnismässigkeitsprinzip und Zweckbindungsgrundsatz.

611 Besagte Grundsätze resp. Vorgaben werden ihrerseits durch zusätzliche Instrumente abgesichert und implementiert, namentlich durch «privacy by design», vgl. Art. 25 Abs. 1 DSGVO und für die Schweiz nach Totalrevision Art. 7 Abs. 3 nDSG. Löschungskonzepte sowie Retentions- sowie Lösch-Policies, welche Fristen wie auch Verfahren definieren, sind geboten. Mit der Totalrevision baut die Schweiz die Anforderungen zur Gewährleistung der Zweckbindung aus, wobei viele der geplanten Bestimmungen als Parallelbestimmungen zur DSGVO bezeichnet werden können.

612 Auch der Zweckbindungsgrundsatz im engeren Sinne lässt sich auf das in dieser Studie als erstes Strukturmerkmal bezeichnete Merkmal des Monismus resp. Dualismus für den öffentlichen resp. privaten Bereich beziehen: In einem Regime des prinzipiellen Verarbeitungsverbotes, wie es die DSGVO vorsieht, weisen die gesetzlich vorgesehenen Erlaubnistatbestände eine zweckbasierte Orientierung auf. Der Gesetzgeber definiert zulässige Verarbeitungsziele und -zwecke resp. -grundlagen, die das prinzipielle Verarbeitungsverbot durchbrechen.[884] Auf diesem Weg werden vom Gesetz beispielsweise die «Wahrung lebenswichtiger Interessen» in Art. 6 Abs. 1 lit. d DSGVO oder die «Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen» in Art. 6 Abs. 1 lit. c DSGVO auf der allgemein-abstrakten Ebene als Verarbeitungszwecke anerkannt, die einen Erlaubnistatbestand für eine Personendatenverarbeitung liefern können. Im Sinne einer Anknüpfung an das konkrete Gebot gemäss Art. 5 Abs. 1 lit. b DSGVO ist auf

883 Vgl. Art. 6 Abs. 4 nDSG; kritisch zum Instrument der Anonymisierung, das gewissermassen verspricht, den «Personenbezug» zu kappen, allerdings nicht geeignet ist, die Adressierung bestimmter Personen, wenn auch nicht identifizierbar, zu erreichen Barocas/Nissenbaum, 1 ff., 4; vgl. im Zusammenhang mit Personendaten von Bankkundinnen und -kunden Hirsch/Jacot-Guillarmod, RSDA 2020, 151 ff., 159 ff.

884 Vgl. insb. Art. 6 DSGVO.

Art. 6 Abs. 4 DSGVO hinzuweisen, der sich mit dem Verhältnis eines ursprünglich fixierten Verarbeitungszweckes, des Primärzweckes, zu einem Sekundärzweck befasst. In Bezug auf die Bestimmung ist umstritten, ob sich ihre Funktion auf einen Kompatibilitätstest beschränkt oder ob sie als Erlaubnistatbestand für Zweckänderungen figuriert.[885]

613 Ebendiese Zweckorientierung findet sich ebenso im DSG, allerdings auf einer nachgeschalteten Stufe. Im DSG, wo sowohl vor als auch nach Totalrevision für den privaten Bereich die prinzipielle Verarbeitungsfreiheit mit Schranken verankert wird, fliessen entsprechende Zweckerwägungen über die gesetzlich vorstrukturierten Rechtfertigungsgründe, namentlich das überwiegende Interesse ein, vgl. Art. 13 Abs. 2 DSG und Art. 31 Abs. 2 nDSG. Hier formuliert das Gesetz einen Katalog von potentiell anerkannten Interessen, die eine persönlichkeitsverletzende Verarbeitungshandlung zum Schutz der Erreichung gewisser Zwecke legitimieren können.

4.3. Von der Zweckbindung zum Schutzzweck des Datenschutzes

614 Mit der dargelegten «Trias» der Zweckvorgaben – interne Zweckbestimmung, externe Transparenzmachung dieses Verarbeitungszweckes sowie Zweckbindung – wird vorab Rechenschaft vonseiten des Verarbeitenden hinsichtlich seiner Verarbeitungshandlungen abgelegt. Sodann werden die Verarbeitungsaktivitäten eingeschränkt. Der Zweckbindungsgrundsatz gilt mit den umrissenen Elementen in der Kommentarliteratur als «Kernbestandteil» des Datenschutzrechts.[886]

615 Seine datenschutzrechtliche Relevanz erschöpft sich – so die These an dieser Stelle – keineswegs darin. Vielmehr wirft der Zweckbindungsgrundsatz eindringlich die Frage nach dem *Schutzzweck des Datenschutzes selbst* auf.[887] Es ist ebenso dieser Konnex zum Schutzzweck des Datenschutzrechts selbst, der die hervorragende Bedeutung des Zweckbindungsgrundsatzes für das Datenschutzrecht verstärkt. Die nachfolgenden Ausführungen wenden sich der Frage nach dem *Schutzzweck oder den Schutzzwecken resp. -zielen des Datenschutzrechts* zu.

616 In Bezug auf die Frage nach dem *Zweck der Datenschutzgesetzgebung* selbst – die Wissenschaftlerinnen und Wissenschaftler wie keine andere Frage herausfordert – ist auf Art. 1 DSG einzugehen. Unter dem Titel «Zweck» sagt Art. 1 DSG:

885 Vgl. Buchner/Petri, BeckKomm-DSGVO, Art. 6 N 181.
886 Herbst, BeckKomm-DSGVO, Art. 5 N 21.
887 Auch im Rahmen der 12. Tagung zum Datenschutz – Jüngste Entwicklungen am 5. Februar 2019, organisiert vom Europa Institut, wurde in verschiedenen Referaten der Schutz der Persönlichkeit, Grundrechte und Würde der Person als Schutzzweck des Datenschutzrechts betont; vgl. statt vieler entsprechend dem Gesetzeswortlaut Peter, 33; vertiefend zu Zielfunktionen des Datenschutzes grundlegend und früh Mallmann, 16 ff.

> «Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.»

617 Mit der Totalrevision wurde eine Änderung vorgenommen, wonach nur «natürliche Personen» entsprechenden Schutz finden. Neu wird das DSG in Bezug auf Personendatenverarbeitungen von juristischen Personen keine Anwendung mehr finden.

618 In der Schweiz wird der *Zweck des Datenschutzgesetzes* ebenso unter dem Begriff des *Schutzobjektes* abgehandelt. Insofern allerdings findet sich ein Sammelsurium an weiteren Begriffen, vom Privatsphärenschutz über den Schutz der informationellen Selbstbestimmung bis hin zum Schutz des Missbrauches von Personendaten sowie Schutz der informationellen Privatheit.[888] Das DSG beschränkt sich darauf zu statuieren, dass es den Schutz der *Persönlichkeit* (resp. der Grundrechte) bezweckt. Anknüpfungspunkt des zivilrechtlichen Teils des Datenschutzgesetzes ist Art. 28 ZGB.[889] Nach der Auffassung der schweizerischen Datenschutzgesetzgebung geht es damit um den Schutz eines subjektiven Rechts des Individuums.

619 Anders das Konzept in der DSGVO: Die DSGVO stellt ihren ersten Artikel unter den Titel «Gegenstand und Ziel», wobei es die natürlichen Personen (indes ohne konkretisierte Anknüpfung an ein spezifisches subjektives Recht) sowie der freie Verkehr von Personendaten sind, denen die Vorschriften der DSGVO dienen sollen. Zugleich wird auf die Bedeutung des Datenschutzes für die Prosperität sowie den wirtschaftlichen wie sozialen Fortschritt hingewiesen.[890]

620 Die Frage *nach Schutzzweck und Schutzobjekt der Datenschutzregulierung* bleibt bis heute Kernthematik, -problematik und -herausforderung.[891] Die nachfolgenden Ausführungen arbeiten mit der folgenden *Hypothese:* Die herausragende Bedeutung der Vorgaben zum Verarbeitungszweck liegt auch darin begründet, dass aus ihnen *neue Perspektiven für den Schutzzweck des Datenschutzrechts* selbst abgeleitet werden können. Eine Beschäftigung mit dem Zweckbindungsgrundsatz legt eine *hinter resp. unter der individualrechtlichen, insb. der persönlichkeitsrechtlichen Schutzausrichtung angelegte systemische Schutzdimension des Datenschutzrechts frei.* Anders gewendet: Der Schutzzweck und Schutzauftrag der Datenschutzregulierung erschöpft sich nicht im Individualrechtsschutz resp. Persönlichkeitsschutz. Die hier formulierte Hypothese wird anhand einer eingehenden Auseinandersetzung mit dem mittlerweile in die Jahre gekommenen

888 Hierzu vertiefend zweiter Teil, VI. Kapitel.
889 Vgl. BBl 1988 II 414 ff., 414.
890 Vgl. DSGVO ErwG 2 ff.
891 Zur Diversifizierung der Schutzzwecke insb. qua DSGVO vgl. dritter Teil, VIII. Kapitel, A.2.2.

Volkszählungsurteil des deutschen Bundesverfassungsgerichts herausgearbeitet und erhärtet.[892]

Das Urteil wurde als «Magna Carta»[893] resp. «Bergpredigt»[894] des Datenschutzrechts bezeichnet. Eine vertiefte Auseinandersetzung mit den Zweckerwägungen und namentlich der Zweckbindung in dieser Entscheidung erstaunt prima vista: Seit dem Urteil sind Jahrzehnte rasanten technischen Fortschrittes ins Land gegangen. Zudem schrieb das Volkszählungsurteil wegen seiner *Anerkennung des Rechts auf informationelle Selbstbestimmung* Rechtsgeschichte. Allerdings ist das Volkszählungsurteil nicht nur wegen seinem vielzitierten Recht auf informationelle Selbstbestimmung aufschlussreich. Vielmehr ist es ebenso richtungsweisend hinsichtlich seiner *Zweckerwägungen*. Unter Rückgriff auf diese zweckorientierten Erwägungen des Bundesverfassungsgerichts lassen sich Lösungsansätze zwecks Weiterentwicklung des Datenschutzrechts der Zukunft ableiten – eines Datenschutzrechts, das seine Schutzaufträge und -zwecke effizient gewährleisten wird, selbst im Zeitalter der Digitalisierung.[895] 621

Im Folgenden geht es um die Darstellung eines Zusammenspiels zwischen mehreren Aspekten – zweckbezogene Verarbeitungsgrundsätze, Schutz des subjektiven Rechts der informationellen Selbstbestimmung und Schutzzweck des Datenschutzrechts. Die Argumentation des Bundesverfassungsgerichts im Volkszählungsurteil lässt sichtbar werden, dass das *Individuum datenschutzrechtlich nicht einzig mittels subjektiver Rechte hinreichend geschützt werden kann*. Stattdessen führt eine Analyse der Erwägungen zu der Schlussfolgerung, dass nur ein *systemischer Ansatz*, welcher namentlich den diversen und facettenreichen Verarbeitungszusammenhängen und damit gesellschaftlichen Bereichen Rechnung trägt, angemessene Antworten auf die Herausforderungen der Personendatenverarbeitungen liefert. Schlüsselelement bildet hierbei der *Verarbeitungszweck und -zusammenhang*. Im Volkszählungsurteil ging es insofern um Personendatenverarbeitungen durch den deutschen Staat *zwecks Zensus*. 622

Der erste Satz des Volkszählungsurteils und seiner Leitsätze lautet wie folgt: 623

> «Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.»[896]

892 BVerfG 65, 1 – Mikrozensus, Urteil vom 16. Juni 1969.
893 So Hoffmann-Riem, AöR 1998, 513 ff., 515.
894 Meister, DuD 1986, 173 ff., 175.
895 Auf die Bedeutung des Verwendungszusammenhanges und der Zweckbindung weist namentlich Simitis, NJW 1984, 394 ff., 402 ff. hin.
896 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 1.

624 Das Bundesverfassungsgericht macht den Schutz des Menschen mit seiner Persönlichkeit zum Ausgangspunkt des Rechtsschutzes im Kontext der Personendatenverarbeitung. Aufschlussreich insofern eine weitere Passage aus den verfassungsgerichtlichen Erwägungen, die nichts an Aktualität eingebüsst hat:

> «Die Möglichkeiten der modernen Datenverarbeitung sind weiterhin nur noch für Fachleute durchschaubar und können beim Staatsbürger die Furcht vor einer unkontrollierbaren Persönlichkeitserfassung […] auslösen […].»[897]

625 Zum Schutzbereich, der auch im Lichte von Art. 2. Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz beurteilt wurde, sowie zu den datenschutzrechtlichen Herausforderungen heisst es weiter:

> «1.a. Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt […]. Die bisherigen Konkretisierungen durch die Rechtsprechung umschreiben den Inhalt des Persönlichkeitsrechts nicht abschliessend. Es umfasst […] auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. […] Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermassen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiss. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.»[898]

626 Im letzten Satz dieses Zitates findet sich ein Befund, der mit dem jüngsten Facebook-Skandal aus dem Jahre 2018 erneut eine beispiellose Virulenz erfahren hat: Personenbezogene Angaben aus Facebook-Kommunikationsbeziehungen waren durch eine Drittgesellschaft analysiert worden. Mutmasslicherweise wurde in der Folge versucht, das *Wahlverhalten bestimmter Personen* gezielt zu beeinflussen.[899] Das Ansinnen, über die Nutzung von Personendaten, die das Individuum in

897 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 8.
898 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 172.
899 Vgl. Rosenberg/Confessore/Cadwalladry, NYT vom 17. März 2018, abrufbar unter: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> (zuletzt besucht am 30. April 2021).

persönlichen Kommunikationsbeziehungen über Facebook teilte, einzelne Individuen politisch zu manipulieren, beeinträchtigt *nicht* nur die konkret betroffenen Individuen. Ein solches Vorgehen weist eine kollektive Dimension auf, weil über die Manipulation der stimm- und wahlberechtigen Bürgerinnen und Bürger *die Integrität des demokratischen Systems an sich erodiert* wird.

627 Das Bundesverfassungsgericht hatte mit besagtem, zuletzt zitiertem Satz die *systemische Dimension datenschutzrechtlicher Regulierung adressiert*. Gleichwohl fährt es, an diesen heute als zukunftsweisend zu bezeichnenden Passus anknüpfend, mit einem subjektivrechtlichen Fokus fort:

> «Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art, 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insofern die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.»[900]

628 Es ist diese Erwägung zum Recht auf informationelle Selbstbestimmung, die unter dem Stichwort «Volkszählungsurteil» in die Gedächtnisse, Schriften und das Internet eingegangen ist. Mit der Passage werden das Subjekt, die Person und ihre Persönlichkeit sowie die Selbstbestimmung als Schutzzweck des Datenschutzes in das Zentrum der Aufmerksamkeit gerückt. Eine solche individualrechtliche, persönlichkeitsrechtliche Anknüpfung ist und bleibt ebenso für das Schweizer Datenschutzrecht prägend, Art. 1 (n)DSG.[901]

629 Dessen ungeachtet steht gemäss den Ausführungen des Bundesverfassungsgerichts der Schutz der informationellen Selbstbestimmung nicht allein da. Seine Gewährleistung ist zugleich *Garant für mehrere Grundrechte*. Zudem ist das Recht Grundlage für ein demokratisches und freiheitliches Gemeinwesen. Der *individualrechtliche Schutz ist von weiteren Schutzdimensionen nicht nur unterlagert, sondern in diese eingebettet.* Wird hingegen eine Datenverarbeitung isoliert für ein konkretes Datensubjekt als individualrechtliche Problemstellung fokussiert, werden kontextuelle Herausforderungen des Datenschutzes übersehen.[902] Folglich scheint es zu kurz gegriffen, ein wie auch immer geartetes subjektives Recht zu definieren, dieses aber nicht in seine gesellschaftlichen Bezüge einzubetten. Es ist das Bundesverfassungsgericht, das neben der Anerkennung eines Rechts auf informationelle Selbstbestimmung eine solche *Bezugnahme anhand seiner Erwägungen zum Verarbeitungszweck und namentlich zur Zweckbindung* vornimmt.

900 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 173.
901 Vgl. zur persönlichkeitsrechtlichen Anknüpfung als drittes Leitprinzip des DSG zweiter Teil, VI. Kapitel.
902 Vgl. insofern Teubner, KritV 2000, 388 ff., 388 und 404; Ders., in: Brüggemeier (Hrsg.), 303 ff.; Hensel/Teubner, KritJ 2014, 150 ff.

630 Unbestritten steht ein subjektives Recht, das Recht auf informationelle Selbstbestimmung resp. das Persönlichkeitsrecht als «Schutzzweck» datenschutzrechtlicher Regelung, in den Urteilserwägungen im Vordergrund. In diesem Zusammenhang aktualisiert sich auch die traditionsreiche Unterscheidung zwischen «gewöhnlichen» und «sensiblen» Personendaten. Das Bundesverfassungsgericht erteilte der datenschutzrechtlichen Tragfähigkeit einer zweigeteilten Welt indes eine punktuelle Absage:[903]

> «Die Verfassungsbeschwerden geben keinen Anlass zur erschöpfenden Erörterung des Rechts auf informationelle Selbstbestimmung. Zu entscheiden ist nur über die Tragweite dieses Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt. Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses Datum" mehr.»[904]

631 Der Hinweis, wonach eine Anknüpfung des Datenschutzes an die Kategorisierung von personenbezogenen Daten als sensibel resp. nicht-sensibel im Zeitalter der neuen Datenverarbeitungstechnologien zu kurz greife, steht nicht isoliert da.[905] Von entscheidender Bedeutung in Bezug auf die Ausgestaltung der datenschutzrechtlichen Vorgaben kann nicht die «Natur» einer bestimmten Personenangabe sein; eine Personenangabe ist nicht per se besonders schutzwürdig. Vielmehr ist der *Verwendungszusammenhang* das einschlägige Kriterium, wie das Bundesverfassungsgericht wie folgt attestiert:

> «Wieweit Informationen sensibel sind, kann hiernach nicht alleine davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhanges: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten.»[906]

903 Nissenbaum, 232, schlägt vor, beide dichotomen Konzepte – «privat»-«öffentlich», «gewöhnliche Personendaten»-«besonders schutzwürdige Personendaten» – für das Private ruhen zu lassen.

904 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 176.

905 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 176.

906 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 177; zu den «sensitiven Daten» als festem Bestandteil der Datenschutzgesetzgebung mit einer Kritik Simitis, in: Brem/Druey/Kramer/Schwander (Hrsg.), 469 ff.; die Untauglichkeit einer gesetzlichen Einteilung von Personendaten in gewöhnliche und besonders schutzwürdige Angaben als Orientierungskriterium für die Datenschutzregulierung wurde auch wissenschaftlich kritisch diskutiert, namentlich durch Simitis, Nomos-Komm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 20 ff. und N 34 ff., wobei der Datenschutzexperte zur Veranschaulichung der Untauglichkeit folgendes Beispiel nennt: Den Namen als belangloses Datum zu taxieren, greife offensichtlich zu kurz. Denn sobald es darum geht, dass dieser

Das Bundesverfassungsgericht hinterfragt somit den tradierten Differenzierungsmechanismus einer bezugslosen Taxierung von Personendaten als besonders schutzwürdig und damit einschlägiges Anknüpfungskriterium für erhöhte Schutzpflichten. Stattdessen betont es die Bedeutung des konkreten Verwendungszusammenhangs.[907] Es weist damit implizit auf die datenschutzrechtliche Notwendigkeit einer *differenzierten Sichtweise in Bezug auf die Verwendungszusammenhänge* hin. Verfassungsgerichtlich wird die hohe Bedeutung betont, wonach der Bearbeitungszweck bereichsspezifisch und präzise bestimmt und die gesammelten Angaben für diesen Zweck geeignet und erforderlich zu sein haben.[908] 632

Zugleich verdeutlicht das Gericht, dass der sog. öffentliche Bereich kein einheitlicher ist. Vielmehr sind staatliche Datenverarbeitungen facettenreich und jeweils an spezifische Stellen, Verwaltungseinheiten usf. angebunden. Den Verarbeitungszweck im öffentlichen Bereich mit einer allgemein umschriebenen «öffentlichen Aufgabe» abbilden zu wollen greift damit zu kurz. Betreffend den Verwaltungsvollzug sind stets die konkreten Aufgaben zu beachten. Dieser notwendigen Differenzierung trägt man im «öffentlichen Bereich» gerade auch über das Legalitätsprinzip Rechnung. Sowohl das deutsche als auch das schweizerische Datenschutzgesetz verlangen für den *öffentlichen Sektor*, dass die Umschreibung des *Zwecks der Datenbearbeitung* Inhalt einer *Rechtsnorm* ist (Prinzip der Spezialermächtigung). 633

In Deutschland waren es bis zum Inkrafttreten der revidierten Fassung mit ihren Anpassungen infolge der DSGVO die §§ 13 ff. BDSG, die als «Einfallstor»[909] für eine Vielzahl zulässiger Bearbeitungszwecke beschrieben wurden. § 13 Abs. 1 BDSG lautete: 634

> «Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stellen erforderlich ist.»[910]

Name auf die Liste der Mafia komme, werde offensichtlich, dass der Name nicht per se als nicht besonders schutzwürdige Angabe qualifiziert werden könne; Nissenbaum, 232.

907 Hierzu auch Simitis, in: Brem/Druey/Kramer/Schwander (Hrsg.), 469 ff., insb. 485 ff.; im DSG bildet die Einteilung zwischen «gewöhnlichen» und «besonders schutzwürdigen» Personendaten, vgl. insofern Art. 3 lit. c DSG und Art. 5 lit. c nDSG, bis heute ein zentrales Strukturierungselement. In dieser dualistischen Konzeptionierung bildet sich eine Vorstellung ab, wonach bestimmte Personendaten per se «gewöhnlich», andere per se «besonders schutzwürdig» sind – und zwar ungeachtet ihres konkreten Verarbeitungszusammenhanges. Weiterhin korreliert die Schwere eines Eingriffes resp. die Höhe der Schutzvorgaben mit einer abstrakten Qualifizierung der Daten. Dreh- und Angelpunkt ist die quasi abstrakte Definition von Personenangaben als besonders schutzwürdig resp. sensibel.

908 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 179.

909 So Buchner, 38.

910 § 13 Abs. 1 BDSG war mithin keine Ausnahmebestimmung zu § 4 BDSG; es handelte sich nicht um eine Legitimationsgrundlage, personenbezogene Daten dann erheben zu dürfen (ungeachtet einer spezifischen Grundlage), sofern dies zur Erfüllung der «übergeordneten» öffentlichen Aufgabe diente. Vielmehr verlangte das Datenschutzgesetz selbst, dass eine rechtliche Grundlage den Zweck der Datenbearbeitung mit der öffentlichen Aufgabe korrelierte, in einem Sachzusammenhang stand. § 13

635 Der deutsche Gesetzgeber beschränkte sich damit nicht darauf, für eine Datenbearbeitung eine gesetzliche Grundlage, die sich zum öffentlichen Interesse sowie dem Zweck der Datenbearbeitung äussert (und zwar hinreichend konkret), zu fordern. Vielmehr musste der *Zweck der Datenbearbeitung mit der Erfüllung von Aufgaben des jeweiligen Aufgaben- und Kompetenzbereichs der verantwortlichen Stelle korrelieren*. Der Zweck und die Zweckbindung werden im Rahmen der Datenerhebung an die *Organisations- resp. Verwaltungseinheit sowie deren spezifische Aufgaben* gekoppelt.

636 Einen solch engen Koppelungsmechanismus zwischen Verarbeitungszweck und Organisationseinheit mit ihrem Aufgabenbereich kennt die Schweiz in ihrem DSG nicht. Zwar gilt nach DSG das Erfordernis, wonach der *Zweck der Datenbearbeitung* selbst in einer spezifischen gesetzlichen Grundlage zu definieren ist, gemäss Art. 17 i. V. m. Art. 4 Abs. 3 und 4 DSG resp. Art. 6 Abs. 1 und Art. 34 nDSG. Gleichwohl plädierte der Bundesrat bereits im Zuge des Erlasses des DSG dafür, keine allzu hohen Anforderungen an die «gesetzliche Grundlage» hinsichtlich der Formulierung von Verarbeitungszwecken zu stellen; es solle genügen, dass eine Datenbearbeitung in einem «einsichtigen sachlichen Zusammenhang» mit der Aufgabe des betreffenden Bundesorgans stehe.[911] Ist die öffentliche Aufgabe selbst hinreichend rechtlich legitimiert, dann gelten Personendatenverarbeitungen zwecks Erfüllung dieser Aufgaben als darin inkludiert.

637 Zurück zum Volkszählungsurteil: Dem zur Beurteilung vorliegenden Verarbeitungszusammenhang, der Personendatenerhebung für einen Zensus, werden Besonderheiten zugemessen, die in ein Dilemma hinsichtlich der Zweckbindung münden: Der Staat in seinem «heutigen» Zuschnitt bedarf der Datensammlung und Datenspeicherung auf Vorrat hin, um seinen Aufgaben nicht unvorbereitet gegenüberzustehen.[912] Eine Datenerhebung für statistische Zwecke kann somit gerade nicht an eine strikte Zweckbindung gekoppelt werden, ohne damit zugleich des Erreichens ihres eigentlichen Zieles verlustig zu gehen. Die Volkszählung solle eine «gesicherte Datenbasis für weitere statistische Untersuchungen» liefern sowie die politische Planung ermöglichen. Beide seien auf verlässliche Feststellungen über Zahl wie Struktur der Bevölkerung angewiesen.[913]

Abs. 1 BDSG stellte eine eigentlich verschärfende Konkretisierung mit Blick auf den Verarbeitungszweck dar.

911 BBl 1988 II 414 ff., 467; vgl. zu den erhöhten Anforderungen an die gesetzliche Grundlage, wenn es um besonders schutzwürdige Personendaten geht, Epiney/Fasnacht, Jusletter vom 24. Februar 2014, N 20 ff., spezifisch bezogen auf das Klienten-Informationssystem für Sozialarbeit. Der Beitrag zeigte indes, dass in erster Linie das kantonale Datenschutzrecht für besagtes System einschlägig ist.

912 Vgl. insofern auch Buchner, 72 ff., der darauf hinweist, dass dem Staat relativ viel Vertrauen entgegengebracht wird, nicht dagegen den Privaten als Datenbearbeitenden. Spezifisch problematisiert er Zugriffsbegehrlichkeiten des Staates auf private Datenbestände; vgl. hierzu auch Prieur, AJP 2015, 1644 ff., 1646.

913 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 184.

Mehrzweckverarbeitungen seien in einem solchen Sinne im Rahmen statistischer Erhebungen zuzulassen.[914] Eine strikte Zweckbindung könne demnach im Zusammenhang statistischer Erhebungen ebenso wenig Geltung beanspruchen wie das Verbot der Vorratsdatenspeicherung.

638 Gerade wegen dieser Spezialitäten zweckorientierter Vorgaben im Rahmen statistischer Erhebungen verlangte das Bundesverfassungsgericht *flankierende und kompensierende Vorkehrungen*. Gefordert wurde die Implementierung eines Mechanismus der *Abschottung der Statistik*, und zwar durch *Anonymisierung resp. durch Geheimhaltung* für den Fall (und die entsprechende Zeitdauer), wonach Angaben noch einen Personenbezug aufweisen. Im Ergebnis heisst das nichts anderes, als dass Angaben, die personenbezogen und zu statistischen Zwecken erhoben wurden, zwar zu anderen Zwecken verarbeitet und weitergegeben werden dürfen, allerdings grundsätzlich erst, wenn eine Anonymisierung stattgefunden hat.[915] Damit bleibt gewissermassen der ursprüngliche statistische Zweck rechtlich wirksam:

> «Eine Weitergabe der für statistische Zwecke erhobenen, nicht anonymisierten oder statistisch aufbereiteten Daten für Zwecke des Verwaltungsvollzugs kann hingegen in unzulässiger Weise in das Recht auf informationelle Selbstbestimmung eingreifen».[916]

639 Das Bundesverfassungsgericht macht auch insofern die *zwei- resp. mehrdimensionale Schutzwirkung* seiner zweckorientierten Erwägungen auch unter diesem Aspekt deutlich: Die *Gewährleistung des Statistikgeheimnisses* schütze nicht (nur) das Individuum, sondern auch die *Integrität und Funktionstüchtigkeit statistischer Erhebungen* und damit letztlich den Staat mit seinen gegenwärtigen Aufgaben und Strukturen. Denn:

> «Für die Funktionsfähigkeit der amtlichen Statistik ist ein möglichst hoher Grad an Genauigkeit und Wahrheitsgehalt der erhobenen Daten notwendig. Dieses Ziel kann nur erreicht werden, wenn bei dem auskunftspflichtigen Bürger das notwendige Vertrauen in die Abschottung seiner für statistische Zwecke erhobenen Daten geschaffen wird, ohne welches seine Bereitschaft, wahrheitsgemässe Angaben zu machen, nicht herzustellen ist. Eine Staatspraxis, die sich nicht um die Bildung dieses Vertrauens durch Offenlegung des Verarbeitungsprozesses und strikte Abschottung bemühte, würde auf längere Sicht zu schwindender Kooperationsbereitschaft führen, weil Misstrauen entstünde. Da staatlicher Zwang nur begrenzt wirksam werden kann, wird ein die Interessen der Bürger überspielendes staatliches Handeln allenfalls kurzfristig vorteilhaft erscheinen; auf Dauer gesehen wird es zu einer Verringerung des Umfangs und der Genauigkeit der Informationen führen […]. Kann damit nur durch eine Abschottung der Statistik die Staatsaufgabe „Planung" gewährleistet werden, ist das Prinzip der Geheimhaltung und möglichst früh-

914 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 173.
915 Vgl. entsprechende Forderungen aufgreifend Art. 31 Abs. 2 lit. e nDSG.
916 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 191; die Anonymisierungspflicht ist, wie erwähnt, eine mit der DSGVO sowie der Totalrevision des DSG nunmehr konkretisiert vorgesehene Pflicht zur Umsetzung des Zweckbindungsgebotes.

> zeitigen Anonymisierung der Daten nicht nur zum Schutz des Rechts auf informationelle Selbstbestimmung des Einzelnen vom Grundgesetz gefordert, sondern auch für die Statistik selbst konstitutiv.»[917]

640 Auch wenn das Bundesverfassungsgericht auf Relativierungen strikter Zweckbindung und folgend kompensatorischer Vorkehrungen im Rahmen statistischer Erhebungen einging, blieb die Idee des Verbotes der Zweckänderung zentral für seine Ausführungen:

> «Würden hingegen personenbezogene, nicht anonymisierte Daten, die zu statistischen Zwecken erhoben wurden und nach der gesetzlichen Regelung dafür bestimmt sind, für Zwecke des Verwaltungsvollzuges weitergegeben (Zweckentfremdung), würde in unzulässiger Weise in das Recht auf informationelle Selbstbestimmung eingegriffen.»[918]

641 Das Bundesverfassungsgericht markierte damit Notwendigkeit und Grundsatz der *Trennung von Statistik und Vollzug*.[919] Folglich bringt es zum Ausdruck, dass der öffentliche resp. staatliche Bereich kein monolithischer, sondern ein hoch ausdifferenzierter Bereich ist, innerhalb dessen zahlreiche Verarbeitungszwecke verfolgt werden.[920] *Datenschutzrechtliche Vorgaben dienen hierbei auch dem Schutz der Integrität des jeweiligen Bereichs*.

642 Das Volkszählungsurteil, obschon dieses primär und untrennbar mit dem Grundrecht auf informationelle Selbstbestimmung assoziiert wird, lädt somit zu einem *Perspektivenwechsel* resp. einer Ergänzung des Blickes um eine grundlegende, dahinterstehende Schutzdimension des Datenschutzrechts ein: Die Lektüre des Urteils führt zu der Erkenntnis, dass der *«Zweck» des Datenschutzrechts* – über ein Recht auf informationelle Selbstbestimmung hinausgehend – in der Gewährleistung *mehrdimensionaler Schutzrichtungen liegt*. Zwar wird dem individualrechtlichen Schutz (bis heute) eine prioritäre Rolle zugewiesen, indem das Datenschutzrecht am Schutz des Menschen, der Person, dem Datensubjekt und an den Individualrechten der Persönlichkeit oder der Selbstbestimmung anknüpft.[921]

643 Die Kontextrelevanz wird in der verfassungsgerichtlichen Problematisierung des *Transfers von Personenangaben, die zum Zweck der Statistik erhoben werden sollten, in weitere und andere Kontexte des Verwaltungsvollzuges* deutlich. Insofern kam das Gericht zu dem Schluss, dass eine Zuführung von Personenangaben, die im Zuge der statistischen Erhebung erhoben wurden, in diverse andere Verwaltungskontexte sowohl die *Integrität der Statistik als auch allgemein staatliche Aufgaben* beeinträchtigen würde. Einzig die Abschottung der statistischen Erhebung durch das Statistikgeheimnis resp. die spätere Anonymisierung der Per-

917 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 188.
918 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 223.
919 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 223.
920 Der Bearbeitungszweck wird von Glass, 125 ff. als Instrument zur Beschreibung des rechtmässigen Kontextraums beschrieben.
921 Vertiefend für das DSG im privaten Bereich zweiter Teil, VI. Kapitel.

sonenangaben liefere eine hinreichend wirksame Garantie, dass die Bürgerinnen und Bürger die im Rahmen des Zensus gestellten Fragen wahrheitsgetreu und vollständig beantworten würden. Müssten sie dagegen fürchten, dass ihre Angaben später in anderen Feldern des Verwaltungsvollzuges «gegen sie verwendet würden», würde dies das Aussageverhalten negativ beeinträchtigen.[922]

644 Die Bedeutung, die das *Bundesverfassungsgericht datenschutzrechtlich dem Schutz der Integrität der statistischen Erhebung zuweist*, untermauert es argumentativ mit der beschränkten Wirksamkeit von Zwangsmassnahmen. Vollstreckende Zwangsmassnahmen, die der Staat bekanntermassen durchaus zur Hand hat, griffen zu kurz, um dem Missbrauch der statistischen Erhebung entgegenzuwirken.[923] Nur wenn die Bürgerinnen und Bürger das notwendige *Vertrauen* haben, dass ihre personenbezogenen Daten einzig zu statistischen Zwecken verarbeitet und nicht weiterreichend zum Verwaltungsvollzug genutzt werden, sei davon auszugehen, dass die erfragten Angaben vollständig und wahrheitsgetreu erteilt würden. Müsse dagegen basierend auf einer Volkszählung mit einer «plötzlichen» Steuernachforderung oder einer Ausweisungsverfügung gerechnet werden, dürfe aller Voraussicht nach weder mit wahrheitsgetreuen noch vollständigen Antworten gerechnet werden. Die Integrität der Statistik und deren Funktionsfähigkeit würden damit über den Zweckbindungsgrundsatz und das Vertrauen der «Hauptpersonen» abgesichert, also quasi *intrinsisch* gewährleistet. Die Möglichkeit, die statistisch erhobenen Daten für den weiteren Verwaltungsvollzug zu nutzen, mag verführerisch erscheinen – auch aus staatlichen «Effizienzerwägungen», denen die Statistik ja gerade verpflichtet ist. Der Preis indes wäre, so das Bundesverfassungsgericht, zu hoch.

645 Das Volkszählungsurteil anerkennt mit diesen Ausführungen, dass der *öffentliche Bereich im Sinne des staatlichen Bereiches* kein einheitlicher Bereich ist. Er konstituiert sich aus facettenreichen Unterbereichen mit entsprechenden Aufgaben. Diese sind ihrerseits relevant für den Datenschutz, der sich als *relational oder akzessorisch zu den jeweils dahinterliegenden Verarbeitungszusammenhängen, Zielen und Zwecken* der einschlägigen staatlichen Bereiche bestätigt. Die Pluralität der Verarbeitungszusammenhänge anzuerkennen und voneinander abzugrenzen, erfolgt *nicht nur zum Schutz des Individuums*. Es dient *ebenso und gerade zum Schutz der Integrität der diversen Bereiche*.

646 Der Zweckbindungsgrundsatz präsentiert sich damit als Barriere-Mechanismus für Personendatenflüsse. Personendaten, die zu einem bestimmten Zweck erhoben und in einen zugehörigen Kreislauf eingespeist wurden, dürfen nicht unbe-

922 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 188.
923 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 178 und E 188.

schränkt in weitere, andere Kreisläufe eingespeist und dort anderen Verarbeitungszwecken zugeführt werden.

647 Mit diesen Ausführungen werden die bereits anhand der Geheimworte und Geheimhaltungspflichten herausdestillierten *dynamischen sowie akzessorischen Dimensionen* datenschutzrechtlicher Themen bestätigt.[924] Datenschutzrechtliche Herausforderungen sind folglich besser zu bewältigen, wenn als *Ausgangslage das Bild von Personendatenflüssen* gewählt wird. Diese sind eingebettet in verschiedene Verarbeitungszusammenhänge resp. Kontexte, was durch die Metapher der Landschaft symbolisiert werden könnte. In der Folge sind insb. die Grenzübertritte zwischen verschiedenen Bereichen sowie die Gestaltung von Personendatenflüssen vonseiten des Rechts zu adressieren.[925] Eine solche Herangehens- und Betrachtungsweise der datenschutzrechtlichen Ausgangslage konterkariert die traditionsreiche Anknüpfung an das dualistische Regime mit Datensubjekt resp. Person und Personendaten als Quasi-Objekten.

648 Der Zweck datenschutzrechtlicher Regulierung beschränkt sich damit, wie die vorangehenden Reflexionen zum Volkszählungsurteil freigelegt haben, nicht auf den Schutz des Individuums, also des Datensubjektes. Vielmehr kommt dem Datenschutzrecht eine Garantenstellung zum Schutz der Integrität verschiedener gesellschaftlicher Systeme, Institutionen oder Bereiche zu.

649 Die Zweckerwägungen destillieren eine richtungsweisende Facette des Zwecks des Datenschutzrechts selbst heraus: Aussagekräftige Statistiken seien, so das Bundesverfassungsgericht, für den Staat zeitgenössischen Zuschnittes unverzichtbar, um seine mannigfachen Aufgaben angemessen planen und bewältigen zu können. Wenn allerdings die Bürgerinnen und Bürger damit rechnen müssen, dass die personenbezogenen Angaben, die sie im Rahmen der Statistikerhebung offenbaren, Konsequenzen in anderen Bereichen – vonseiten der Einwohnerbehörde, des Steueramtes, der «Vormundschaftsbehörde» usf. – nach sich zögen, würde der *statistische Zweck selbst gefährdet*. Statistische Erhebungen können nur dann erfolgreich sein, wenn die zur Auskunft verpflichteten Bürgerinnen und Bürger nicht dazu «verleitet» werden, Angaben zu verweigern oder zu verfälschen. Dazu sind sie allerdings gerade dann veranlasst, wenn sie fürchten müssen, dass ihre Angaben Auswirkungen in anderen Zusammenhängen haben könnten. Die zweckorientierten Erwägungen und kompensatorischen Mechanismen zur Abschottung der Statistik präsentieren sich damit nicht nur als Schutzinstrument der Bürgerinnen und Bürger, sondern quasi als staatliches Selbstschutz-

924 Vgl. insb. erster Teil, I. Kapitel, A.

925 Vgl. zu den Data Flows zwischen Ländern, aber auch Gesellschaftsbereichen Birnhack, CLSR 2008, 508 ff., 512 f.; dazu, dass es bei der privacy um den Fluss von Personendaten gehe, Kang/Buchner, Harv. J.L. & Tech. 2004, 229 ff., 231 f., wobei ihr interessanter Beitrag in Dialogen strukturiert wird; der erste Dialog ist der Market-Talk, der zweite Talk ist der Dignity-Talk.

instrument: Mit ihrer Gewährleistung schützt der Staat sich selbst, seine Funktionstüchtigkeit und die Funktionstüchtigkeit seiner Instrumente und Bereiche, im Volkszählungsentscheid die Statistik und die sog. *Integrität der Statistik*. Die datenschutzrechtlichen Vorgaben haben sich ebenso dem Schutz der Integrität dieser anerkannten gesellschaftlichen «Institution» zu widmen. Mit einem solchen *systemischen Schutz* wird das Datensubjekt inkludierend geschützt.

650 Neben dem *individualrechtlichen* und *systemisch-institutionellen Gesicht* wurde anhand dieser Ausführungen zur Zweckbindung erneut das *dynamisch-relationale (oder auch dynamisch-akzessorische) Gesicht* der Thematik sichtbar. Der Zweckbindungsgrundsatz fixiert *personenbezogene Daten in einem bestimmten Informationskreislauf*. Er schreibt vor, dass zu einem bestimmten Zweck erhobene personenbezogene Daten nicht zu einem anderen Zweck bearbeitet werden dürfen. Kurz: *Eine Zweckentfremdung ist verboten, die Überleitung von zweckgebundenen Daten zur Erfüllung anderer Zwecke ist unzulässig*. Diese dynamische Dimension des Datenschutzrechts richtet den Fokus auf eine Vorstellung, nach welcher personenbezogene Daten aufgrund des definierten Zweckes in einem bestimmten Verarbeitungszusammenhang dienen – in einem bestimmten Flussbett fliessen. Unter welchen Voraussetzungen personenbezogene Daten aus diesem Flussbett abgeleitet und in einen anderen Datenflusslauf, in einen anderen Verarbeitungszusammenhang eingespeist werden dürfen, ist die zentrale Frage. Es geht damit – unter Beibehaltung der geografischen Sprache – um die Flussmündungen und Grenzübertritte («Schnittstellen»[926], «Schaltstellen», «Knotenpunkte»[927]). Das Datenschutzrecht befasst sich, wie es die zweckorientierten Leitvorstellungen zeigen, mit *Datenflüssen zwischen und in unterschiedlichen Systemen, mit Datenverarbeitungen zu unterschiedlichen Zwecken, in diversen Verarbeitungszusammenhängen*. Bei einer solchen Konzeptionierung steht die Frage nach den sog. *Transmissionsprinzipien im Vordergrund*.[928] Im Laufe dieser Arbeit wurden bislang insofern bereits nebst dem Geheimnis und der Einwilligung auch das Instrument der Anonymisierung vorgestellt.

651 Eine *kontextuelle Betrachtung* kommt zur Vervollständigung des Bildes nicht umhin, eine einbettende Klarstellung vorzunehmen: Es war ein Entscheid zum Datenschutzrecht des öffentlichen i. S. des staatlichen Bereiches, anhand dessen zweckorientierten Erwägungen und namentlich der Zweckbestimmung sowie -bindung sich *drei datenschutzrechtliche Herausforderungen, Schutzziele, Aspekte sowie Dimensionen* herausarbeiten liessen. Kontextuell betrachtet wird inso-

926 Vgl. zum Begriff im Zusammenhang mit Verarbeitungsprozessen von Personendaten durch Spitäler Gogniat, Jusletter vom 20. Juni 2016, N 2.

927 So Ladeur, Vortrag Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021).

928 Hierzu Nissenbaum, 145 ff., 192 f., 201 ff., 217 ff.; vertiefend dritter Teil, IX. Kapitel.

fern seit jeher und bis heute die Problematik des staatlichen Zugriffes vonseiten des Staates auf Datenbestände privater Akteure thematisiert.[929] Damit fragt sich sogleich weiter: Lässt sich die systemisch-institutionelle sowie dynamisch-akzessorische Bedeutung des Datenschutzes, der bis heute nicht die gebotene Aufmerksamkeit geschenkt wurde, auch für den *sog. privaten Bereich im Sinne der (Zivil-)Gesellschaft* nachzeichnen?

652 Hinweise in diese Richtung finden sich im bereits zitierten Logistep-Urteil des Bundesgerichts. Zwar legte das Gericht den Schwerpunkt auf den Befund, wonach das Vorgehen der Logistep AG und hierbei auch der *Zweck* ihrer Datenerhebungen *nicht erkennbar* waren. Gleichwohl enthalten auch die bundesgerichtlichen Ausführungen Hinweise zur Einschlägigkeit *pluraler Verarbeitungskontexte*. Im Logistep-Entscheid verortete das Bundesgericht den *Zweck* der Datenbearbeitung in der *Aufklärung von Urheberrechtsverletzungen*. Das *Interesse* der die Bearbeitungsgrundsätze verletzenden Partei allerdings war, wie geschildert, ein *wirtschaftliches*:

> «Die Beschwerdegegnerin selbst verfolgt ein wirtschaftliches Interesse. Sie strebt eine Vergütung für ihre Tätigkeit an. Diese Tätigkeit besteht darin, mit Hilfe einer eigens dafür entwickelten Software in P2P-Netzwerken nach urheberrechtlich geschützten Werken zu suchen und von deren Anbietern Daten zu speichern.»[930]

653 Für die Einhaltung der Grundsätze gemäss Art. 4 Abs. 3 und Abs. 4 DSG genügt es, dass der unmittelbare Datenbearbeitungszweck einer konkreten Datenverarbeitungshandlung als Massstab dient. Entscheidend war für das Bundesgericht, dass der relevante unmittelbare Zweck der Datenerhebung für die Datensubjekte im Dunkeln blieb, was gegen Art. 4 Abs. 3 und Abs. 4 DSG verstosse.[931] Es ergänzte indes sogleich, dass dieser Verstoss – entgegen dem zu engen Wortlaut von Art. 12 Abs. 2 lit. a DSG – gerechtfertigt werden könne. Allerdings würde im vorliegenden Fall kein überwiegendes privates oder öffentliches Interesse den Verstoss gegen die Bearbeitungsgrundsätze von Art. 4 Abs. 3 und Abs. 4 DSG rechtfertigen, selbst wenn man über das wirtschaftliche Interesse der bearbeitenden Partei dasjenige der Auftraggeberin an der Aufklärung von Urheberrechtsverletzungen in die Erwägungen integriere. Die Annahme überwiegender Interessen dürfe von vornherein nur mit Zurückhaltung angenommen werden.[932]

---

929 So jüngst Lobsiger, Verschärfung der Datenschutzaufsicht über die Polizei, Vortrag vom 7. Februar 2019, Zürcher Juristenverein; Buchner, 72 ff.; die Problematik ist akzentuiert, wenn die datenschutzrechtlichen Vorgaben, wie im schweizerischen DSG, für den öffentlichen Bereich strikter sind als für den privaten Bereich. Eine Lösung hierfür liegt in einem monistischen Ansatz mit identischem Regime für die beiden Sektoren, wie ihn nunmehr die DSGVO implementiert.

930 BGE 136 II 508, E 6.3.3.

931 BGE 136 II 508, E 4.

932 BGE 136 II 508, E 6.3.3. und E 6.4.; für einen umfassenderen Überblick über die Praxis des EDÖB, die Verwaltungsgerichtspraxis und die Bundesgerichtspraxis vgl. die einschlägigen Datenschutzkommentare.

Im vorliegenden Fall wurde eine Rechtfertigung verneint, wobei in diesem Entscheid für «den privaten Bereich» die *systemisch-institutionelle Dimension* des Datenschutzes und seiner Herausforderungen angelegt ist. Es ist der Kontext der Ökonomie, der mit dem privaten Lebensbereich kollidiert, wobei zugleich ein privater Akteur eine Aufgabe, die der staatlichen Strafbehörde zugewiesen wird, an sich zieht.[933] 654

Das dieser Studie den Titel verleihende Recht auf informationellen Systemschutz wird im dritten Teil, IX. Kapitel elaboriert. Es ist Konsequenz eines im Zuge dieser Schrift an diversen Stellen freigelegten systemrelativen Elements, wie es im zeitgenössischen Datenschutzrecht angelegt ist. Für die Herleitung des Rechts auf informationellen Systemschutz wird eine vergleichbare Konstellation gewählt werden, wie sie sich im Logistep-Entscheid findet. In beiden Fällen finden verdeckte Ermittlungen zwecks Aufdeckung mutmasslich unrechtmässiger Handlungen statt. Bei der im letzten Kapitel dieser Studie gewählten Konstellation geht es um die Versicherungsobservation zur vermeintlichen Betrugsaufdeckung. Auch hier kollidieren infolge von Personendatenverarbeitungen gesellschaftliche Kontexte miteinander, womit die *Integrität der gesellschaftlichen Bereiche* selbst aufs Spiel gesetzt wird.[934] 655

933 Interessant die historische Annäherung an den nur vermeintlich klaren Begriff der Ökonomie durch die Beiträge in Dejung/Dommann/Speich (Hrsg.).

934 Vgl. hierzu dritter Teil, IX. Kapitel; aufschlussreich sodann der jüngste Entscheid des Bundesverwaltungsgerichts, in dessen Argumentation zum Zweckbindungsgrundsatz ebenso die systemrelative Bedeutung aufscheint: Bearbeite die Beklagte im Rahmen des Helsana+-Programmes Personendaten, die bei einer anderen Versicherungsgesellschaft der Helsana-Gruppe im Zusammenhang mit der obligatorischen Krankenkasse gespeichert worden seien, stehe dies im Konflikt mit der Zweckbindung, Art. 4 Abs. 3 DSG, BGer A-3548/2018 vom 19. März 2019, E 3 ff. Mit Blick auf die Zweckbindung nimmt man in erster Linie das Unternehmen in den Blick, welches zu einem bestimmten und erkennbar gemachten Zweck Personendaten verarbeitet – an diesen Zweck ist das Unternehmen alsdann gebunden. In casu ist es in erster Linie die Krankenversicherungsgesellschaft, welche Personendaten zwecks Abwicklung der Grundversicherung verarbeitet, die gegen den Zweckbindungsgrundsatz verstösst, wenn sie zu diesem Zweck gesammelte Personendaten weitergibt. Doch nach bundesverwaltungsgerichtlichem Entscheid verletzte ebenso die Zusatzversicherung das Zweckbindungsgebot, indem sie auf Personenangaben einer anderen Versicherungsgesellschaft zugriff, die durch die Grundversicherung in ebendiesem Kontext und zu ebendiesem Zweck erhoben und gespeichert worden waren. Eine solche weite Auslegung zum Zweckbindungsgrundsatz schottet offensichtlich verschiedene Bereiche voneinander ab – die Grundversicherung gegenüber der Zusatzversicherung. Der Fluss von Personendaten zwischen diesen beiden Bereichen wird verhindert, indem selbst das «Drittunternehmen» an den Verarbeitungszweck des «Erstunternehmens» gebunden ist; die konsequenteste Weise, die Einschlägigkeit des Verwendungszusammenhanges datenschutzrechtlich zum zentralen Ansatzpunkt und Lösungsansatz zu machen, findet sich in einer sektoriellen Datenschutzgesetzgebung. Namentlich die USA kennt für den privaten Bereich kein datenschutzrechtliches Querschnittsgesetz. Auch in Europa finden sich bereichsspezifische Datenschutznormierungen, ohne dass auf eine Querschnittsgesetzgebung verzichtet wird.

4.4. Resümee

656 Die vorangehenden Ausführungen haben die zentrale Bedeutung der *Zweckvorgaben* im und für das Datenschutzrecht analysiert. Gezeigt wurde, dass die verschiedenen Regelungsinhalte verschiedene Stossrichtungen verfolgen. Das Verhältnismässigkeitsprinzip wird an den Verarbeitungszweck angebunden, indem Verarbeitungshandlungen zur Erreichung eines definierten Zweckes geeignet, erforderlich und verhältnismässig im engeren Sinne zu sein haben. Mit diesen Vorgaben werden Verarbeitungsmöglichkeiten von Anfang an vordefiniert und damit zurückgebunden. Zudem greifen in Bezug auf den Verarbeitungszweck Transparenzvorgaben, wobei mit der Totalrevision des DSG neu eine Informationspflicht verankert wird.

657 Spezifisch unter dem Grundsatz der Zweckbindung (im weiteren Sinne) lassen sich die Vorgaben an die vorgängige Zweckfixierung resp. -definierung, die Transparenzvorgaben hinsichtlich des Verarbeitungszweckes sowie die Zweckbindung im engeren Sinne unterscheiden. Der faktischen Einhaltung der Zweckvorgaben dienen Instrumente wie das Verarbeitungsverzeichnis, Löschungs- und Anonymisierungsvorgaben, die Datenschutz-Folgenabschätzung, aber auch die Anforderungen an die hinreichend konkrete sowie granulare Transparenzmachung von Verarbeitungszwecken im Rahmen von Datenschutz- und Einwilligungserklärungen.

658 Nachdem der Inhalt der Gebote auch in ihren Entwicklungslinien nachgezeichnet wurde, gelangte die Arbeit zu einer *Grundsatzfrage: zur Frage nach dem Zweck der Datenschutzgesetzgebung*. Im Zentrum stand eine vertiefte Beschäftigung mit den Ausführungen des Bundesverfassungsgerichts in seinem Volkszählungsurteil. Hierbei wurde gezeigt, dass das Urteil, das für «sein» Recht auf informationelle Selbstbestimmung berühmt wurde, den Schutzzweck des Datenschutzes zwar durchaus stark individual- und persönlichkeitsrechtlich anknüpft. Allerdings wurde auch manifest, dass das Bundesverfassungsgericht anhand seiner Erwägungen zu den Zweckgrundsätzen eine *systemische resp. institutionelle* Schutzdimension des Datenschutzes betont. Das Bundesverfassungsgericht machte deutlich, dass innerhalb des «öffentlichen Bereiches» plurale Verarbeitungszusammenhänge und -zwecke zu differenzieren seien und es nicht angehe, zu statistischen Zwecken erhobene Angaben beliebig den unzähligen und facettenreichen Bereichen des Verwaltungsvollzuges zugänglich zu machen. Der öffentliche Bereich und die öffentliche Verwaltung ist folglich aus datenschutzrechtlicher Perspektive gerade kein einheitlicher Bereich. Vielmehr konstituiert er sich aus zahlreichen Einheiten, Institutionen, Aufgabenfeldern mit jeweils «eigenen» Datenverarbeitungszwecken.

Zweckbindungsvorgaben, die eine Schlüsselrolle in der Argumentation des Bundesverfassungsgerichts einnahmen, zielen entsprechend nicht nur auf den *Subjektschutz*, sondern namentlich auch auf den *Systemschutz* ab. Der Datenschutz dient damit nicht nur dem Schutz des einzelnen Individuums, sondern ebenso dem *Schutz der Integrität verschiedener Bereiche resp. Systeme*. Die datenschutzrechtlichen Vorgaben sind also auch darauf auszurichten, die Funktionstüchtigkeit und Integrität der jeweils auf dem Spiel stehenden Kontexte, Institutionen und Bereiche zu gewährleisten.[935] Angemessene und befriedigende Antworten vonseiten des Datenschutzrechts, das beide Schutzdimensionen und -zwecke seiner selbst anerkennt, können nur durch eine systemrelative Betrachtung gefunden werden. 659

Die im Volkszählungsurteil thematisierte systemische Dimension und Relevanz des Datenschutzes wird viele Jahrzehnte später durch den jüngsten Facebook-Skandal bestätigt: Personendaten, die aus persönlichen Kommunikationsbeziehungen über Facebook generiert wurden, gelangten an ein Drittunternehmen zur Analyse (es ist anzunehmen, dass diese verkauft wurden), woraufhin man Nutzerinnen und Nutzer in ihrer Rolle als Wählerinnen und Wähler im US-Wahlkampf zu beeinflussen versuchte. Personendaten wurden losgelöst von ihrem ursprünglichen Verarbeitungskontext, losgelöst von persönlichen Kommunikationsbeziehungen, in intransparenter Weise und vermutlich auch aus wirtschaftlichen Interessen ausgewertet, um damit die politische Willensbildung zu beeinflussen. Damit wurde nicht nur die Integrität des Lebensbereiches persönlicher Beziehungen, sondern auch die Integrität des politischen Kontextes, des demokratischen Systems korrumpiert. Eine Betrachtung, die einzig und isoliert die Manipulation des einzelnen Datensubjektes problematisiert, vermag der systemischen Herausforderung nicht gerecht zu werden. 660

Mit der Freilegung der *subjektrechtlichen und systemischen Schutzdimension* anhand des Blickes auf die Zweckbindungsvorgaben wurde auch die *dynamisch-akzessorische Dimension* der Datenschutzthematik herausgearbeitet. Sie hängt aufs Engste mit der systemischen Schutzdimension zusammen: Mit der Zweckbindung werden Personendaten in einem bestimmten Informationsflussbett oder Verarbeitungskontext gehalten, ein Übertritt in einen anderen Informationskreislauf oder einen anderen Verarbeitungskontext soll verhindert werden. Der bis spätestens 661

935 Zu diesem Ansatz Nissenbaum, *passim*; wie das Bundesverfassungsgericht prägnant ausführte: Keine obrigkeitliche Vollstreckungsmassnahme vermag zu gewährleisten, dass die Bürgerinnen und Bürger korrekt und vollständig an dem für «den Staat» so wichtigen Zensus teilnehmen. Müssten diese fürchten, dass ihre Angaben in weiteren Feldern des Verwaltungsvollzuges ausgewertet würden, bestünde das Risiko, dass die Bürgerinnen und Bürger im Rahmen der statistischen Erhebungen keine korrekten und vollständigen Informationen gäben, womit Ziel und Zweck der statistischen Erhebung aufs Spiel gesetzt würden. Lediglich das Statistikgeheimnis (neben weiteren konkreten Massnahmen) könne das notwendige Vertrauen bei den Bürgerinnen und Bürgern generieren und damit ihre unverzichtbare Kooperation sicherstellen.

zum Zeitpunkt der Erhebung festgelegte Verarbeitungszweck, der transparent gemacht werden muss, bindet die hierfür erhobenen Personendaten in dem Bereich, für dessen Zwecke sie erhoben werden.

662 Die vorangehenden Ausführungen beantworten die Frage nach dem Schutzzweck des Datenschutzrechts wie folgt: Anhand des Zweckbindungsgrundsatzes lassen sich *drei Facetten* des Datenschutzes, des Zwecks des Datenschutzrechts und einer Schutzkonzeptionierung beschreiben: die *subjektivistische*, die *systemische* und die *dynamische* Dimension. Die erste Dimension steht bis heute im Vordergrund, die letzteren beiden dagegen bleiben, obschon im geltenden Datenschutzrecht angelegt, im Hintergrund. Inwiefern die systemisch-institutionelle sowie dynamisch-akzessorische Sichtweise zur Fortentwicklung des Datenschutzrechts fruchtbar gemacht werden können, ja müssen, wird im letzten Kapitel dieser Arbeit erörtert.[936]

663 Nunmehr ist in Kürze auf die beiden Grundsätze der Datenrichtigkeit und -sicherheit einzugehen, um den Katalog der gemeinsamen und allgemeinen Verarbeitungsgrundsätze abzurunden.[937]

5. Die Vorgaben an die Richtigkeit von Personendaten

5.1. Gesetzliche Entwicklungen und Inhalte

664 Mit der Datenrichtigkeit befasst sich explizit Art. 5 DSG, dessen Abs. 1 verschiedene Pflichten gegenüber den Verarbeitenden formuliert und dessen Abs. 2 DSG einen Berichtigungsanspruch des Datensubjektes verbürgt. Der Inhalt des Richtigkeitsgebotes gemäss Art. 5 Abs. 1 DSG in seiner qua Novelle von 2006 verankerten Fassung ist in *vielerlei Hinsicht unklar.* Der vormaligen Version «Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern», wurde ein zweiter Satz angefügt:

> «Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.»

665 Der vergleichende Blick auf die Divergenz zwischen dem Normtext gemäss Art. 5 Abs. 1 DSG und der DSGVO macht eine erste Unklarheit der Bestimmung des DSG sichtbar: Während Art. 5 Abs. 1 lit. d DSGVO verlangt, dass Personendaten bezüglich des verfolgten Zwecks richtig und erforderlichenfalls aktuell sein müssen, stipuliert das DSG in seinem Art. 5 Abs. 1 vorab eine *Pflicht zur Vergewisse-*

936 Beachte nach Totalrevision zu den Befugnissen des EDÖB Art. 49 ff. nDSG, wobei er im Rahmen von Empfehlungen und Leitfäden zur guten Praxis erarbeitet und hierbei die «Besonderheiten des jeweiligen Anwendungsbereichs» berücksichtigt.

937 Hierzu sei auf die einschlägige Kommentar- und Spezialliteratur verwiesen.

rung bezüglich der Richtigkeit von Personendaten, nicht aber ein allgemeines Gebot, wonach nur richtige Personendaten verarbeitet werden dürfen. Beide Normtexte sprechen sodann von «angemessenen Massnahmen», um die Richtigkeit resp. Vollständigkeit der Personendaten sicherzustellen. Eine «Prüfungspflicht» in Bezug auf die Datenrichtigkeit und Vollständigkeit sowie die Verpflichtung, angemessene Massnahmen zur Sicherstellung der faktischen Richtigkeit sowie Vollständigkeit zu ergreifen, ist zumindest dem Wortlaut nach nicht dasselbe wie eine Pflicht, die Richtigkeit der Personendaten selbst sicherzustellen. Die Aspekte können damit auch auf einem Zeitstrahl, der den «Lebenszyklus» von Personendaten und ihrer Verarbeitung in den Blick nimmt, reflektiert werden.

666 Die Totalrevision inkludiert die Vorgaben in Bezug auf die Datenrichtigkeit systematisch überzeugend neu in den Katalog der allgemeinen Verarbeitungsgrundsätze, niedergelegt in Art. 6 Abs. 5 DSG. Die Bestimmung lautet:

> «[5] Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich ab von der Art und dem Umfang der Bearbeitung sowie vom Risiko, das die Bearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringt.»

667 Das Gebot der Richtigkeit wird damit etwas detaillierter normiert, wobei weiterhin die «Pflicht zur Vergewisserung» statuiert wird. Auf die explizite Verankerung eines Aktualisierungsgebotes wird verzichtet. Der Berichtigungsanspruch resp. -vermerk des Datensubjektes wird nach Totalrevision neu mit Art. 32 Abs. 1 und Abs. 3 nDSG verbürgt. In Anbetracht der Totalrevision soll punktuell insoweit auf die Herausforderungen des noch geltenden Art. 5 Abs. 1 DSG eingegangen werden, als daraus ein Erkenntnisgewinn auch für die datenschutzrechtlichen Entwicklungen gezogen werden kann.

668 Die Richtigkeit von Personendaten kann nicht isoliert beurteilt werden. Vielmehr bedarf sie der *Kontextualisierung*. Entsprechend wird sie auch als «relativ» beschrieben und von Gesetzes wegen in einen Bezug zum *Verarbeitungszweck* gesetzt.[938] Als verletzt gilt der Verarbeitungsgrundsatz gemäss Art. 5 Abs. 1 DSG sodann, wenn es der Verarbeitende unterlassen hat, die Richtigkeit von Personendaten zu überprüfen *und* die Personendaten tatsächlich nicht richtig sind.

669 Die Anforderungen an den Prüfungsmassstab hinsichtlich des «Sich-Vergewisserns» betreffend die Datenrichtigkeit dürften höher sein, wenn verarbeitende Stellen Personendaten nicht unmittelbar beim Betroffenen erheben. «Vergewis-

938 Illustrativ das Beispiel Rosenthal, HK-DSG, Art. 5 N 2.

sern» verlange die hinreichende Aufmerksamkeit und Sorgfalt, um in angemessener Weise sicherzustellen, dass die erhobenen Daten richtig sind.[939] Art. 5 Abs. 1 DSG stipuliere eine *Vergewisserungspflicht*, was – so die Kommentarliteratur – gerade nicht mit einem Gebot, nur richtige Personendaten zu verarbeiten, gleichzusetzen sei.[940] Letzteres ergäbe sich aus anderen und weiteren Datenverarbeitungsgrundsätzen.[941] Als «richtig» i. S. v. Art. 5 Abs. 1 DSG beurteilt werden Personendaten, wenn sie Tatsachen in Bezug auf die betroffene Person sachgerecht sowie aktuell wiedergeben und ein vollständiges, wahrheitsgetreues (objektives) Bild liefern.[942]

670 Umstritten ist das Verhältnis der Richtigkeitsvorgaben in Bezug auf eine anfängliche gegenüber einer sukzessiv zu wiederholenden Prüfungs- resp. Verifizierungspflicht mit kontinuierlich andauernden Pflichten zur Berichtigung, Vervollständigung, Aktualisierung.[943] Damit ist die Frage nach der Relation zwischen dem ersten Satz und dem zweiten, 2006 eingeführten Satz sowie dessen Haupt- und Relativsatz aufgeworfen. Die Interpretationen divergieren:

671 Wermelinger/Schweri konstatieren, dass sich der «neue» Regelungstext (eingefügt 2006) auf den ersten Blick wie eine Verschärfung des Rechts ausnähme. Doch bei Lichte betrachtet handle es sich um das Gegenteil, «eine Relativierung der Nachführungspflicht». Mit der sog. Nachführungspflicht sei weniger der Charakter der Dauerpflicht und wiederholenden Prüfungspflicht gemeint als vielmehr die Pflicht zur inhaltlichen Bereinigung unrichtiger, veralteter oder unvollständiger Angaben. Der Datenbearbeiter müsse nunmehr angemessene Massnahmen zur Sicherstellung der Richtigkeit nur bezüglich derjenigen Daten treffen, die im Hinblick auf ihren Zweck und ihre Bearbeitung diese Nachführung voraussetzen.[944] Anders die Interpretation von Rosenthal: Seiner Ansicht nach stelle der Satz 2 die Tragweite von Satz 1 klar und zwar relativierend: Eine allgemeine und in zeitlicher Hinsicht regelmässige Nachführungspflicht werde nicht verankert; vielmehr bestünde diese lediglich dort, wo das Risiko einer Persönlichkeitsverletzung vorliege für den Fall, dass unrichtige (resp. unvollständige oder veraltete) Personendaten verarbeitet würden.[945] Nach Maurer-Lambrou/

939 Zur Vergewisserungspflicht, deren Angemessenheit für den Einzelfall zu prüfen ist, Rampini, BSK-DSG, Art. 12 N 11 ff.; Rosenthal, HK-DSG, Art. 5 N 5.

940 So Rosenthal, HK-DSG, Art. 5 N 4; ebenso Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 11.

941 Vgl. BGer 1A.6/2001, E 2.a.; zu Art. 5 Abs. 1 DSG beachte auch BVGer A-7588/2015.

942 Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 4; Schweizer, digma 2007, 64 ff.; Meier, N 745.

943 Ungeachtet eines vom Datensubjekt geltend gemachten Berichtigungsanspruchs, vgl. Art. 5 Abs. 2 DSG und Art. 32 Abs. 1 nDSG.

944 Wermelinger/Schweri, Jusletter vom 3. März 2008, N 14; so auch Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 13.

945 Rosenthal, HK-DSG, Art. 5 N 9; wann dies der Fall ist, wird nicht präzisiert. Der Autor vertritt zugleich, dass sich eine Pflicht, nur richtige Personendaten zu verarbeiten, zwar nicht aus Art. 5

Schönbächler ist eine prinzipiell «regelmässige Fortschreibung» geboten.[946] Epiney/Nüsch differenzieren konsequent zwischen der Verifizierungspflicht und der Berichtigungs- resp. Löschungspflicht und reflektieren diese jeweils auf der Zeitachse. Hierbei vertreten sie, dass es sich bei der Vergewisserungspflicht nicht nur um eine einmalige, initiale Pflicht handle und stattdessen die periodische Überprüfung angezeigt sei. Sodann seien angemessene Massnahmen zu ergreifen, um die als unrichtig eruierten Angaben zu berichtigen oder zu vernichten.[947]

672 Eine vergleichbare Systematisierung des sog. Richtigkeitsgebots findet sich namentlich bei Meier, der zwischen der *materiellen und der temporellen Komponente* unterscheidet.[948] Meier vertritt die Ansicht, dass mit der Revision von 2006 sowohl die Verpflichtung zur Vergewisserung betreffend die Richtigkeit der Daten (an sich und namentlich bereits mit der Erhebung) als auch die Pflicht zur rollenden Aktualisierung aufgrund der Einfügung des zweiten Satzes nicht mehr absolut gelte. Den Verarbeitenden träfe keine allgemeine proaktive Berichtigungspflicht. Vielmehr sei eine Relativierung des Grundsatzes für sich sowie der Pflichten des Bearbeiters vorgenommen worden.[949] Der Autor weist allerdings auf einen einschlägigen Punkt im Rahmen des damaligen Gesetzgebungsprozesses hin: Die Relativierung durch den 2. Satz von Art. 5 Abs. 1 DSG sei auf eine Fehlannahme im Parlament zurückzuführen:[950] Dort ging man mit Blick auf das Regelungsregime im privaten Bereich davon aus, dass gemäss geplanter Neufassung von Art. 12 Abs. 2 lit. a DSG *keine* Rechtfertigungsgründe für einen Verstoss gegen den «Grundsatz der Datenrichtigkeit» möglich seien. Allerdings wurde eine derartige Interpretationsweise des Art. 12 Abs. 2 lit. a DSG bald schon verworfen: Heute ist anerkannt, dass eine Rechtfertigung selbst hier, wenn auch zurückhaltend, möglich sein soll.[951] Verhältnismässigkeitserwägungen würden damit über die Rechtfertigungsgründe einfliessen; eine Relativierung durch die Einfügung eines zweiten Satzes mit besagtem Inhalt wäre unnötig.

673 Vor dem Hintergrund der jüngsten Rechtsentwicklungen ist m. E. hinsichtlich die *Richtigkeitsvorgaben* von Folgendem auszugehen: Die Vergewisserungspflicht ist eine eigenständige Pflicht, deren Missachtung eine Persönlichkeitsverletzung begründet. Eine Vergewisserungspflicht betreffend die Richtigkeit weist zweierlei Ingredienzen auf, eine objektive und eine subjektive.

Abs. 1 DSG, doch aber aus den allgemeinen Bearbeitungsgrundsätzen ergäbe, vgl. N 4; früh verwies Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 29, auf die Problematik von Entscheidungen, die auf unrichtigen, unvollständigen oder veralteten Informationen basieren.

946 Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 13.

947 Epiney/Nüsch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.94 ff.

948 Meier, N 745.

949 Ders., N 750.

950 Ders., N 751.

951 Vgl. BGE 136 II 508, E 5.2.4.

674 Der Formulierung, wonach man sich über die Richtigkeit von Personendaten zu *vergewissern* hat, liegt eine Basisannahme zugrunde, wonach die Personendaten auch *faktisch* richtig sind – man *vergewissert* sich ihrer Richtigkeit. Gleichwohl scheint der Gesetzgeber keinen ergebnisorientierten, objektiven Fokus einzunehmen. Vielmehr wird die gebotene Sorgfalt, «Anstrengung», die Prüfungspflicht hervorgehoben. Zudem werden die angemessenen Massnahmen zum Kernkriterium gemacht. Damit werden die Richtigkeitsvorgaben an die Zweckvorgaben gekoppelt. Die parlamentarischen Erwägungen dokumentieren, dass der Gesetzgeber dem Richtigkeitsgebot keinen absoluten Geltungsanspruch zuweisen wollte. Es sollte an das Verhältnismässigkeitsgebot gebunden werden.

675 Vorgeschlagen wird an dieser Stelle zudem, die Erwägungen des Google-Street-View-Urteils sinngemäss wie folgt zu integrieren: Auch im Zusammenhang mit der Richtigkeit von Personendaten ist anzuerkennen, dass eine *Nullfehlertoleranz nicht verlangt werden kann*.[952] In dem Entscheid wurde im Rahmen des Verpixelns von Gesichtern usf. eine Fehlertoleranz von einem Prozent akzeptiert, was analog leitend sein könnte.[953] Entsprechend ist im Geiste der schon für die Physik anerkannten «Fehlerrechnung» ein («angemessener») Fehlerquotient im Rahmen der Richtigkeitsvorgaben anzuerkennen.[954] Massnahmen, welche die Richtigkeit von Personendaten – gemessen am Verarbeitungszweck – gleichwohl nicht innerhalb dieser oder einer im Vorfeld definierten «Fehlermarge» gewährleisten können, sollen ihrerseits dem Grundsatz nach nicht als angemessen qualifiziert werden. Mit anderen Worten sollen sich Verarbeitende nicht hinter das Argumentarium zurückziehen können, «sich vergewissert» und «angemessene Massnahmen» ergriffen zu haben, wenn hieraus nicht auch als Resultat – gemessen am Zweck – ein *Mindestquotient an Richtigkeit, Vollständigkeit und Aktualität* resultiert. Die Vergewisserungspflicht sowie die angemessenen Massnahmen sind somit *objektiv und ergebnisorientiert* zu interpretieren. Sie haben als Resultat ein bestimmtes Niveau der Richtigkeit zu erreichen.

676 Eine Relativierung ist gleichwohl angezeigt: Sofern eine Unrichtigkeit *keinen Einfluss auf die Zweckerfüllung hat*, kann sie unter Umständen toleriert werden.[955] Sodann gibt es Personendaten, deren Speicherung gerade in der nicht aktuellen resp. aktualisierten Weise geboten ist. Exemplarisch sind die Angaben zu einer Person zum jeweiligen Untersuchungszeitpunkt durch eine Ärztin (Gewicht, Hör-

952 BGE 138 II 346, Regeste und E 10.6.2.

953 So Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.29 ff. mit Hinweis auf BGE 138 II 346, E 10.7.

954 Vgl. allerdings zum Ausmass der Fehlerhaftigkeit im Rahmen von Kreditauskünften vertiefend unter dem Vollzugsdefizit dritter Teil, VII. Kapitel, B.2.; zur Problematik der Fehlerhaftigkeit auch im Zusammenhang mit Auskunfteien, insb. auch Kreditauskunfteien bereits Forstmoser, SJZ 1974, 217 ff., 218 f.

955 Vgl. hierzu sogleich vertiefend.

und Sehvermögen, Blutdruck, Puls usf.).[956] In diesem Zusammenhang ist zu beachten, dass archivierte Daten keiner Aktualisierung bedürfen.[957] Wird mit geschätzten und ca.-Angaben gearbeitet, ist für den Fall, dass ebendies angegeben wird, ebenso von einer Richtigkeit auszugehen, sofern die Personendaten (in zutreffender Weise) innerhalb der angegebenen Marge liegen.

677 Im Übrigen ist dem Grundsatz nach anzunehmen, dass sich eine verarbeitende Stelle nicht mit Erfolg auf «unzumutbare Massnahmen» berufen können soll, die nicht dazu führen, ein mit einem Fehlertoleranzquotienten versehenes Richtigkeitsniveau der Personendaten zu erreichen, sofern die Zweckerreichung untergraben wird. In diesem Fall ist der Verarbeitungsprozess aus datenschutzrechtlicher Perspektive nicht nur im Lichte der Richtigkeitsvorgaben an sich als ungenügend zu bezeichnen.

678 Der Grundsatz der Datenrichtigkeit erstreckt sich über den *gesamten Zyklus* von Datenverarbeitungsprozessen. Die Vorgaben für die Datenrichtigkeit sind wiederholt und regelmässig zu beachten, wobei im gerade beschriebenen Sinne Korrekturen, Aktualisierungen resp. Löschungen vorzunehmen sind. Es handelt sich damit um Dauerpflichten – unter dem Vorbehalt von Personendaten, die ihrerseits als «historische Daten» gelten.[958] Eine über einen bestimmten Fehlerquotienten hinausgehende Unrichtigkeit ist als Verletzung des Richtigkeitsgebotes zu qualifizieren, sofern damit die Erreichung des Zweckes torpediert wird, wobei Rechtfertigungsgründe hierfür zumindest theoretisch (wenn auch mit Zurückhaltung) nicht ausgeschlossen sind.

679 Für die präsentierte Auslegung von Art. 5 DSG ist auch das der Logik entspringende methodenrechtliche Argument in Erinnerung zu rufen, wonach ein Abweichen von einem Gesetzeswortlaut bei krass stossenden Ergebnissen resp. bei einem offenkundigen Irrtum des Gesetzgebers selbst *contra verba legis* zulässig ist.[959] Logische Folgerung aus diesem Argument ist, dass eine Auslegung, die im Rahmen des Wortlautes eines Gesetzestextes liegt, bei irrtümlicher Annahme des Gesetzgebers *a fortiori* zulässig sein muss.

680 Zur Untermauerung der hier vertretenen erhöhten Anforderungen an die Gewährleistung der Richtigkeitsvorgaben seien sodann die folgenden systematischen Erwägungen ins Feld geführt: Die Pflichten im Zusammenhang mit der Richtigkeit von Personendaten hängen untrennbar mit weiteren *generalklauselartigen Verarbeitungsgrundsätzen* zusammen, vorab mit den aus dem *Verhältnismässigkeitsgrundsatz* abgeleiteten Vorgaben. Damit sind sie zugleich eng mit den

956 Vgl. Herbst, BeckKomm-DSGVO, Art. 5 N 61.
957 Vgl. Ders., a. a. O.
958 Hierzu Rosenthal, HK-DSG, Art. 5 N 2.
959 Vgl. BGE 128 I 34, E 3.

Zweckvorgaben verzahnt.[960] Die Verarbeitung von unzutreffenden Personendaten kann regelmässig nicht geeignet sein, den damit verfolgten Verarbeitungszweck zu erfüllen, weshalb die Verarbeitung zugleich regelmässig unverhältnismässig sein dürfte.[961] Auch das Aktualitäts- resp. Aktualisierungsgebot kann entsprechend als Ausdruck des Verhältnismässigkeitsgebots gelesen werden. Die endlose Speicherung von Personendaten, die ihre Richtigkeit und Aktualität längst verloren haben, ist folglich (unter dem Vorbehalt namentlich von Archivierungsvorgaben) prinzipiell unzulässig.

681 Die hier vertretene Auslegung, wonach die Richtigkeit von Personendaten nicht nur im Zeitpunkt der Erhebung zu prüfen und unter Berücksichtigung eines Fehlerquotienten umzusetzen ist, wobei nach geltendem DSG eine rollende Überprüfungspflicht und daran anschliessend eine Berichtigungs- resp. Löschungspflicht einzuhalten sind, wird somit innergesetzlich von einer *systematischen Auslegung* getragen. Die objektivierte und ergebnisorientierte Rückkoppelung der Gebote des Richtigkeitsgrundsatzes nimmt eine Garantenstellung für die Einhaltung weiterer Verarbeitungsgrundsätze ein: So gewährleistet eine regelmässige Überprüfung der Richtigkeit, Aktualität und Vollständigkeit von Personendaten (gemessen am Verarbeitungszweck) und darauf basierend das Ergreifen von Folgemassnahmen, dass dem Grundsatz der Verhältnismässigkeit und der Zweckbindung effizient und nachhaltig Nachachtung verliehen wird.

682 Eine systemische Auslegung berücksichtig internationale resp. supranationale Normtexte. Hierbei ist namentlich Art. 5 Abs. 4 lit. d der am 8. Mai 2018 verabschiedeten Modernisierung der Datenschutzkonvention 108 des Europarates zu erwähnen.[962] Der Bestimmung gemäss müssen Personendaten «accurate, and, where necessary, kept up to date» sein.[963] Personendaten haben richtig zu sein, womit das Ergebnis zum Kriterium erhoben wird und nicht eine Vergewisserungspflicht oder «angemessene Massnahmen». Die Konjunktion «and» verdeutlicht zudem, dass es sich bei der Berichtigung und Aktualisierung um zwei eigenständige Pflichten handelt, wobei die Aktualisierungspflicht nicht absolut gilt.[964]

683 Ähnlich lautete Art. 6 Abs. 1 lit. d der EU-Richtlinie 95/46, nach der die Mitgliedstaaten sicherzustellen hatten, dass personenbezogene Daten richtig sind

960 Vgl. Meier, N 752.

961 Zur Alimentierung «wirtschaftlicher» Begehrlichkeiten, der hohen Fehlerhaftigkeit namentlich von Score-Werten im Zusammenhang mit Kreditauskünften und der über die Verletzung des datenschutzrechtlichen Richtigkeitsgebotes hinausgehenden Dimension der Problematik vertiefend dritter Teil, VII. Kapitel, B.2.

962 Der Schweizerische Bundesrat verabschiedete das Änderungsprotokoll im Herbst 2019 <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-76861.html> (zuletzt besucht am 30. April 2021).

963 Daten:recht, Europaratskonvention 108 verabschiedet, Zürich 2018, <http://datenrecht.ch/europaratskonvention-108-verabschiedet> (zuletzt besucht am 30. April 2021).

964 Das naheliegende Illustrationsbeispiel sind Archive, die personenbezogene Angaben enthalten.

und, sofern erforderlich, aktualisiert werden.[965] Die Richtlinie wurde ersetzt durch die DSGVO. Art. 5 Abs. 1 lit. d DSGVO verlangt, dass die Personendaten sachlich richtig sind. Es handelt sich damit um ein objektives Kriterium.[966] Verlangt wird die Übereinstimmung von Personendaten mit der Realität.[967] Darüber hinaus müssen Personendaten (erforderlichenfalls) auf dem neusten Stand sein; es sind angemessene Massnahmen zu treffen, damit Personendaten, die für den Verarbeitungszweck unrichtig sind, unverzüglich aktualisiert resp. gelöscht werden. Es greifen drei Grundsatzpflichten: Das Verbot der Erhebung und Speicherung unrichtiger Personendaten, das Gebot der Aktualisierung unrichtig gewordener Personendaten sowie dasjenige der Löschung resp. Berichtigung gespeicherter unrichtiger Personendaten.[968]

684 Besagte Vorgaben gelten gleichwohl nicht absolut. Die DSGVO verlangt unter Ausrichtung am Verarbeitungszweck «angemessene Massnahmen». Indem nach DSGVO allerdings an den Richtigkeitsgrundsatz ein objektiver Massstab angelegt wird (und keine Vergewisserungspflicht), dürfte unter Sichtung der Kommentarliteratur das Folgende gelten: Personendaten haben gemessen am Verarbeitungszweck richtig und aktuell zu sein, unrichtige resp. veraltete Personendaten sind zu berichtigen resp. zu löschen. Eine Berufung auf die Angemessenheit der Massnahmen, die kein Mindestmass an Richtigkeit im Ergebnis zu erreichen vermögen, dürfte ausgeschlossen sein. Zugleich bringt Art. 5 Abs. 1 lit. d DSGVO unmissverständlich zum Ausdruck, dass es sich bei der Sicherstellung der Datenrichtigkeit *und* der Aktualität um einen Prozess handelt, der kontinuierlich resp. wiederholend durchzuführen ist. Die DSGVO räumt zudem individualrechtliche Ansprüche der Datensubjekte ein, die auf die Gewährleistung der Richtigkeits- und Aktualitätsvorgaben abzielen, vgl. zum Berichtigungsanspruch des Datensubjektes Art. 16 DSGVO und zum Löschungsbegehren Art. 17 sowie Art. 21 Abs. 1 und Abs. 2 DSGVO.

685 Entsprechende Ansprüche finden sich auch im DSG mit dem Berichtigungsanspruch im Sinne eines Betroffenenrechts, vgl. Art. 5 Abs. 2 DSG resp. Art. 32 Abs. 1 nDSG (in engem Zusammenhang damit stehen auch Löschungsansprüche).[969] Die Berichtigung ist kosten- und formlos möglich.[970] Während ein Teil

965 Die Richtlinie wurde von Birnhack, CLSR 2008, 508 ff., 515 als das erfolgreichste internationale Instrument zur Globalisierung des Datenschutzrechts beschrieben; der Autor weist zudem darauf hin, dass die Richtlinie von amerikanischen Wissenschaftlern als aggressiv beschrieben wurde, 519; zur Bedeutung, das Datenschutzrecht «international» zu adressieren, Cottier, SRIEL 2016, 255 ff.

966 Vgl. Herbst, BeckKomm-DSGVO, Art. 5 N 60.

967 Ders., a. a. O., Art. 5 N 60.

968 Hierzu Reimer, NomosKomm-DSGVO, Art. 5 N 34 ff.

969 Im Einzelnen zu diesem Recht, das unentgeltlich und formlos geltend gemacht werden kann, Rosenthal, HK-DSG, Art. 5 N 12 ff.; Meier, N 761 ff.; vgl. sodann den Anspruch gemäss Art. 15 Abs. 3 DSG.

970 Mit Hinweis auf das Musterformular des EDÖB Rosenthal, HK-DSG, Art. 5 N 15.

der Lehre dieses Individualrecht in Abhängigkeit von Ziel, Funktion oder Typ der Bearbeitung einschränken will, vertritt Meier mit Referenz auf ein Recht auf informationelle Selbstbestimmung, dass das Berichtigungsrecht uneingeschränkt gelten müsse.[971] Auch Widmer tritt in zutreffender Weise dafür ein, dass selbst geringfügige Fehler dem Berichtigungsanspruch zugänglich seien.[972] Der Anspruch auf Berichtigung lässt sich als Element des sog. Selbstdatenschutzes bezeichnen.[973] Nachweis und Beweis der Unrichtigkeit von Personendaten obliegen dann der betroffenen Person. Misslingt der betroffenen Person der Unrichtigkeitsbeweis, wird sie auf die Möglichkeit eines Bestreitungsvermerks gemäss Art. 15 Abs. 2 DSG und Art. 32 Abs. 3 nDSG verwiesen. Im Lichte der datenschutzrechtlichen Realitäten greift allerdings das individualrechtliche Instrumentarium über weite Strecken ins Leere.[974] Die Betroffenen werden nur ausnahmsweise von Verstössen gegen die Verarbeitungsvorgaben Kenntnis erlangen.[975]

686 Nach diesen Auslegungserwägungen zum Regelungsinhalt im Zusammenhang mit der Datenrichtigkeit ist bezüglich der Gewährleistung des Grundsatzes mit seinen Unteraspekten auf die Herausforderungen und insb. die Interessenlagen einzugehen.

5.2. Herausforderungen

687 Die Verarbeitung falscher, veralteter und unvollständiger Angaben bleibt aus Datenschutzperspektive ein Kernproblem. Der Grundsatz wird als häufig verletzt beschrieben. Verarbeitende stossen hinsichtlich der Umsetzung allfälliger Löschungsvorgaben auf technische Hürden. Das Richtigkeitsgebot und die Problematik der (Un-)Richtigkeit wird im Rahmen der Bedeutung des sog. Vollzugsdefizites im dritten Teil dieser Arbeit anhand der Kreditauskünfte vertieft thematisiert. Hier wird sich zeigen, weshalb *nur* eine *ergebnisorientierte Interpretation* der Richtigkeitsvorgaben den Zielen und Zwecken des Datenschutzrechts Rechnung zu tragen vermag.[976]

688 Die Bedeutung der datenschutzrechtlichen *Richtigkeitsvorgaben* hängt damit von einer Auseinandersetzung mit den *Interessenlagen sowie Schutzmotivationen* ab:

971 Meier, N 768.
972 Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 5 N 5.55.
973 Vgl. zum Selbstdatenschutz Pärli, digma 2011, 66 ff., 67; zu den verschiedenen Betroffenenrechten Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 5; spezifisch zum Löschungsanspruch gemäss DSGVO als Selbstdatenschutz Gesmann-Nuissl, InTeR 2018, 201 ff., 208.
974 Spezifisch zur seltenen Geltendmachung des Berichtigungsanspruches Rosenthal, HK-DSG, Art. 5 N 17.
975 Ein Szenario, in welchem das Datensubjekt von der Unrichtigkeit von Personendaten Kenntnis erlangt, ist im Rahmen der Bonitätsauskünfte dann gegeben, wenn einer Person, die stets ihre Rechnungen fristgerecht bezahlt hat, dennoch beispielsweise ein Kreditkauf aufgrund eines «vermeintlich» schlechten Score-Wertes verweigert wird.
976 Vgl. hierzu dritter Teil, VII. Kapitel, B.2.

Das *Richtigkeitsgebot* dient – knüpft man am individualrechtlichen Ansatz des Datenschutzrechts an – zunächst dem *Schutz und den Interessen der Betroffenen*. Persönlichkeitsverletzungen durch die Bearbeitung unrichtiger Daten sollen verhindert werden, vgl. für den privaten Bereich auch Art. 12 Abs. 2 lit. a i. V. m. Art. 5 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 Abs. 5 nDSG. Wie gezeigt, verbürgen sowohl das DSG als auch die DSGVO subjektive Rechte resp. Betroffenenrechte der Datensubjekte, um die Richtigkeitsvorgaben durchzusetzen. Solche Rechtsbehelfe stehen in der Tradition der Anknüpfung des Datenschutzrechts im Schutz der Person und einer individualgüterrechtlichen Rechtsposition.

689 Allerdings wurde gezeigt, dass gerade mit der jüngsten datenschutzrechtlichen Weiterentwicklungswelle eine neue Facette in die Rechte integriert wird. Sie stellt sich neben die individualrechtliche Abstützung: Integriert wird eine prozessorientierte Sichtweise, welche die proaktive Dauerpflicht der Verarbeitenden anerkennt und die Etablierung entsprechender organisatorischer und prozeduraler Massnahmen gebietet, um das Richtigkeitsgebot zu erfüllen. Damit zeigt das Datenschutzrecht sowohl in der EU mit der DSGVO als auch in der Schweiz mit der Totalrevision eine markante Abkehr resp. Weiterentwicklung eines ursprünglich ganz im defensivrechtlichen Individualgüterrechtsschutz verankerten Datenschutzrechts. Gleichwohl bleibt dieser Ansatz nicht nur im DSG, sondern auch in der DSGVO erhalten.

690 Das Richtigkeitsgebot wird durch weitere Aspekte faktisch auf den Prüfstand gestellt: Es gilt zwar als im rechtlich geschützten Interesse des Individuums. Die Verarbeitenden haben dieses neu durch die Etablierung und den Einsatz angemessener technischer, organisatorischer und prozeduraler Instrumente sowie Massnahmen zu gewährleisten. Allerdings korrelieren die Interessen an der Einhaltung und Erfüllung der Richtigkeitsvorgaben nur teilweise mit dahinterliegenden *geschäftlichen Interessen der Bearbeitenden*.

691 Eine Korrelation lässt sich wie folgt beschreiben: Für die Bearbeitenden haben in erster Linie richtige, aktuelle und vollständige Daten einen (Aussage-)Wert, womit die Einhaltung der datenschutzgesetzlichen Vorgaben durch dahinterliegende Geschäftsinteressen motivational abgesichert wird. Die Einhaltung der Richtigkeitsgebote ist insofern durchaus im Geschäftsinteresse der Verarbeitenden. Unrichtige Personendaten können für personendatenverarbeitende Stellen nutzlose Aufwendungen verursachen.[977] Marketingstrategien und -massnahmen beispielsweise, die auf personenbezogener Werbung durch Zustellung von Katalogen basieren, generieren Fehl- und Mehraufwand, sofern sie auf Falschinformationen beruhen. Bei Data-Mining und Warehousing können bereits die ins

977 Vgl. Meier, N 743.

Data Warehouse integrierten Rohdaten unrichtig oder veraltet sein.[978] Werden an sich richtige Daten ungleicher Präzision und Herkunft – vom Anmeldeformular, von Scannerkassen oder Drittanbietern – aus ihrem ursprünglichen Kontext extrahiert und in verkürzter Form in ein Informationssystem eingespeist, kann dies zudem aufgrund des Bezugsverlustes ein verzerrtes Gesamtbild ergeben und zu falscher Kundenbewertung führen.[979] Gerade bei automatisierten personenbezogenen Analyseinstrumenten wird davon ausgegangen, dass mehrere Faktoren zu einem hohen Fehlerpotential beitragen können.[980] Verarbeitungen von unrichtigen Personendaten sind hier *sowohl für die Datensubjekte als auch für die verarbeitenden Unternehmen kritisch* – und zwar nicht nur aus datenschutzrechtlicher Perspektive, sondern auch aus Effizienzerwägungen mit Blick auf Geschäftsaktivitäten. In entsprechenden Szenarien herrscht *Kongruenz* dergestalt, dass sowohl die Interessen der Betroffenen als auch die der Bearbeitenden auf die Richtigkeit der Daten gerichtet sind. Die Verantwortlichen dürften damit eine mehrfache Motivation haben, den datenschutzrechtlichen Grundsatz der Richtigkeit einzuhalten: die Einhaltung der Datenschutzgesetzgebung an sich, damit einhergehend der Schutz der Individuen (als Datensubjekte, aber auch z. B. als Konsumentinnen und Konsumenten) sowie die Effizienz der eigenen Geschäftsaktivitäten, denen Personendatenverarbeitungshandlungen dienen.

692 Anders scheint die Einhaltung der weiteren datenschutzrechtlichen Verarbeitungsgrundsätze (für den Fall, dass man die Gültigkeit eines Gesetzes resp. des Datenschutzgesetzes und das Handeln im Einklang mit diesem Gesetz nicht als hinreichenden Anreiz für ein rechtskonformes Handeln beurteilt) keinen vergleichbaren direkten Vorteil für die Verarbeitenden zu generieren. Vielmehr handelt es sich um einen Vorteil, der erst in jüngerer Zeit mit der Aufwertung der Bedeutung des Datenschutzrechts, aber auch der Medienlandschaft verbunden ist: die Vertrauenswürdigkeit in das Geschäftsgebaren der Handelnden und die Integrität des Markts.

693 Die vorangehenden Befunde sind vor dem Hintergrund, wonach Verstösse gegen das DSG bislang nur ganz selten Konsequenzen nach sich zogen – was gleichzeitig Ausdruck und Mitursache für das im dritten Teil zu vertiefende Vollzugsdefizit des Datenschutzrechts ist – von besonderem Interesse für diese Studie.

694 Dafür, dass das Richtigkeitsgebot nur ungenügend umgesetzt wird, gibt es verschiedene Ursachen. Dazu gehören die Techniken wie der Aufwand und damit

978 Hierzu und zu weiteren datenschutzrechtlichen Herausforderungen von Data Mining und Data Warehousing Burkert, in: Jung/Winter (Hrsg.), 117 ff., 119 f.

979 M. w. H. Peter,136 f.; Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 6 ff.; Rampini, BSK-DSG, Art. 12 N 9; hier zeigt sich übrigens die Rückkoppelung des Richtigkeits- an das Zweckbindungsgebot.

980 Schweizer, digma 2007, 64 ff.

auch die Interessen der verschiedenen involvierten Parteien an der (Nicht-)Einhaltung des Grundsatzes. Sodann ist zu attestierten, dass es Praktiken gibt, in denen die Datenbearbeitenden gerade kein *Interesse* haben, dem Richtigkeitsgebot Nachachtung zu verschaffen: Weder das Datenschutzrecht an sich noch die geschäftliche Motivationslage veranlassen in diesen Fällen die Verarbeitenden dazu, die Richtigkeitsgebote der Datenschutzerlasse einzuhalten. Angesprochen ist an erster Stelle die Praxis der Kreditauskunfteien.[981] Falsche, inakkurate, vorurteilsbehaftete oder aufgrund einer unvollständigen Datenlage unzutreffende Bonitätsauskünfte führen hier zur wirtschaftlichen Alimentierung sowohl der Kreditauskunfteien als eigenständiger Branche als auch der krediteinräumenden Institutionen.[982] Der Bereich der Bonitätsauskünfte gilt aus datenschutzrechtlicher Perspektive seit jeher als neuralgisch.[983] Hier zeigen sich empfindliche Schwachstellen, nicht nur bezogen auf die Transparenz der Verarbeitungsprozesse, sondern auch bezüglich der Richtigkeits- und Vollständigkeitsvorgaben. Letztere bezeichnet Buchner als unverzichtbares Korrelat zulässiger Datenverarbeitung, wobei insofern gravierende Defizite und Devianzen nachgewiesen wurden.

695 In den USA dokumentierten mehrere Studien eine hohe Fehlerquote von Kreditauskünften. Eine Untersuchung geht davon aus, dass rund ein Fünftel aller amerikanischen Verbraucher dem Risiko ausgesetzt ist, aufgrund fehlerhafter Credit Scores in eine *höhere* Risikoklasse eingeordnet zu werden und infolgedessen beträchtliche finanzielle Einbussen zu erleiden. Für den amerikanischen Hypothekarmarkt wird die Mehrbelastung mit bis zu USD 124'000.00 beziffert für den Fall, dass eine Schuldnerin aufgrund einer fehlerhaften Datenverarbeitung zu Unrecht einer höheren Risikoklasse zugewiesen wird.[984]

696 Für die Fehlerhaftigkeit kann es verschiedene Ursachen geben – Identifikationsfehler und -verwechslungen, Falschauskünfte, unvollständige oder widersprüchliche Akten, im Rahmen von automatisierten Entscheidungen auch «vorprogrammierte» Vorurteile.[985] Die Wohnlage kann, muss aber keineswegs einen richtigen Schluss auf die Kreditwürdigkeit und Liquidität einer Person zulassen. Die Konsequenzen von dergestalt unrichtigen Personenangaben tragen alsdann in erster Linie die Individuen, wobei diese – in Zahlen gefasst – schwer wiegen. Für die in-

981 Vertiefend hierzu dritter Teil, VII. Kapitel, B.2.; zu den jüngsten technischen und faktischen Möglichkeiten vgl. Radlanski, 26; vertiefend zum Kreditscoring Helfrich, *passim*; kritisch zu diesem vor dem Hintergrund des BDSG bereits Möller/Florax, NJW 2003, 2724 ff.; kritisch auch Mallmann, 80 ff., zu den Handels- und damit Kreditauskunfteien.

982 Letztere können basierend auf unter Umständen zu Unrecht schlechten Score-Werten höhere Zinsfüsse veranschlagen.

983 Buchner, 119 ff.; Möller/Florax, NJW 2003, 2724 ff.

984 M. w. H. Buchner, 124 f.

985 Der Name beispielsweise ist kein zuverlässiger Identifikator, was auch ein Grund für Überlegungen ist, einheitliche Personen-Identifikatoren wie die AHV-Nummer zu implementieren; vgl. insb. zur Richtigkeit und Vollständigkeit im Kontext von Kreditauskunfteien Mallmann, 89 ff.

volvierten Unternehmen erweist sich diese «Unrichtigkeit» der Datenverarbeitungen umgekehrt als lukrativ. Der Sektor alimentiert sich selbst anhand fehlerhafter Auskunfteien, die den Anschein erwecken, besonders rational-analytisch, mathematisch und «zuverlässig» zu sein. Die Praktiken sind aus datenschutzrechtlicher Perspektive problematisch. Dies gilt nicht nur hinsichtlich des Richtigkeitsgebots, sondern auch mit Blick auf weitere Verarbeitungsgrundsätze, insb. die Vorgaben in Bezug auf die Transparenz und Einwilligung, zudem das Verhältnismässigkeitsgebot.[986] Die Verarbeitung von und der Umgang mit «unrichtigen resp. nicht akkuraten» Personenangaben ermöglicht einen *wirtschaftlichen Profit zulasten der Betroffenen*. Allerdings ist dies wohl bloss kurzfristig vorteilhaft für die profitierenden Unternehmen. Denn eine solche Praxis verletzt nicht nur die datenschutzrechtlichen Verarbeitungsgrundsätze, allem voran das Richtigkeitsgebot. Sie beschädigt das Vertrauen in den Finanzsektor selbst, was dessen Produktivität untergräbt.[987]

697 Genau diesen Aspekt greift der *Fair Credit Reporting Act* mit seinem *Amending Act*, dem *Fair and Accurate Credit Transactions Act* von 2003 auf: § 1681 hält fest, dass der Banksektor von einem «fair and accurate credit reporting» abhängig sei. Unfaire und inakkurate Kreditauskünfte dagegen erodieren das Vertrauen der Allgemeinheit – ein Vertrauen, auf das ein effizienter Banksektor angewiesen sei. Damit ist erneut eine *kontextuelle Dimension des Datenschutzes* anerkannt.

698 Über die Richtigkeitsvorgaben wurde die kontextuelle Ingredienz des Datenschutzrechts sichtbar: explizit für das US-amerikanische Recht über den *Fair Credit Reporting Act*, der bereichsspezifisch und folglich bereichsschützend reguliert. Die Richtigkeit und Akkuratheit der Personendaten sind von entscheidender Bedeutung. Indirekt fliesst diese kontextuelle Schutzdimension ebenso in die allgemeine Datenschutzgesetzgebung der Schweiz und der EU ein, und zwar über das Richtigkeitsgebot.

699 An dieser Stelle bestätigt sich somit ein Befund, wie ihn auch die Analyse des Volkszählungsurteils zu Tage förderte: Die kontextuelle Relevanz der Richtigkeit und Vollständigkeit von Personenangaben wurde in besagtem Entscheid bereits vom Bundesverfassungsgericht festgestellt. Mit der Gewährleistung entsprechender Richtigkeits- und Vollständigkeitsvorgaben sollten nicht nur individuelle,

986 Dass gerade der Bereich des Profiling und automatisierter Analyseverfahren und Einzelfallentscheidungen den Datenschutz herausfordert, artikulieren die DSGVO, aber auch die Totalrevision des DSG. Sie widmen diesen Prozessen neu spezifische datenschutzrechtliche Bestimmungen. Insofern ist auf die Vorgaben im Zusammenhang mit der automatisierten Einzelfallentscheidung und dem Profiling hinzuweisen, welche die Gewährleistung nachvollziehbarer Ergebnisse beispielsweise von Scoring-Praktiken erreichen wollen, vgl. Art. 2 lit. f, Art. 13 Art. 15 Abs. 1 lit. h, Art. 22 DSGVO und Art. 5 lit. f und g, Art. 18, Art. 25 Abs. 2 lit. f, Art. 35 nDSG. Im Zusammenhang mit automatisierten Entscheiden setzen die Erlasse primär auf Transparenzvorgaben und Betroffenenrechte.

987 Vertiefend dritter Teil, VII. Kapitel.

sondern ebenso institutionelle Schutzziele erreicht werden – in besagtem Fall die Wahrung der Integrität der statistischen Erhebung.[988]

Im Rahmen der Auseinandersetzung mit den Richtigkeitsvorgaben bestätigt sich, dass eine Sichtweise, die den dynamischen Aspekt der Datenverarbeitungsprozesse sowie der datenschutzrechtlichen Herausforderungen einnimmt, produktiv ist.[989] Beschrieben wurde die primäre und fortwährende Verantwortlichkeit der Verarbeitenden zur Gewährleistung der Vorgaben. Mit der Statuierung einer kontinuierlichen Prüfungs- und Berichtigungs-, Aktualisierungs- resp. Löschungspflicht lässt sich ebenso unter dem Richtigkeitsgebot eine neue Konzeptionierung feststellen. Das Datenschutzrecht hat eine systemrelative sowie eine an kontinuierlichen Datenflüssen orientierte dynamische Dimension. Damit bahnt sich ein Paradigmenwechsel oder zumindest eine Ergänzung des ursprünglichen Ansatzes eines statisch-defensivrechtlichen und isoliert persönlichkeitsrechtlich gedachten Datenschutzrechts den Weg.[990] 700

6. Der Grundsatz der Datensicherheit

Unter dem Stichwort «Datensicherheit» eröffnet sich heute ein weites Feld. Ursprünglich primär mit der Verhinderung von Datendiebstahl oder Hacking assoziiert, könnte man «Datensicherheit» namentlich im Zuge der jüngsten datenschutzrechtlichen Novellierungen als *Schirmbegriff für ein elaboriertes Gefüge* von Vorgaben umschreiben, der sich nicht auf technische und organisatorische Massnahmen beschränkt. Unter dem Tatbestandselement des unbefugten Bearbeitens werden als Bedrohungssituationen insb. die unautorisierte Vernichtung oder Löschung genannt, sodann der unbeabsichtigte Wegfall der Verfügbarkeit, der Diebstahl, die Fälschung, Änderung oder das Kopieren durch Unberechtigte.[991] 701

Nachfolgend wird zunächst der Grundsatz der Datensicherheit gemäss noch geltendem Recht und Art. 7 DSG erörtert. Es folgt ein Abriss über die jüngsten Entwicklungen im Zusammenhang mit der Datensicherheit, wie sie insb. die DSGVO und Totalrevision des DSG bringen.[992] Auch hier verdichten sich die 702

988 Hierzu oben zweiter Teil, V. Kapitel, B.4.2.; zur Gewährleistung von Richtigkeit und Vollständigkeit als Zielfunktion des Datenschutzes allgemeiner bereits Mallmann, 70 ff.

989 Vgl. zum Betrachtungsgegenstand des Datenflusses im Rahmen der Studie zum Kreditscoring der SCHUFA auch Helfrich, 29.

990 Hierzu vertiefend zweiter Teil, VI. Kapitel.

991 Lehmann/Sauter, in: Schweizer (Hrsg.), 135 ff., 142.

992 Vgl. zum Begriff der Verletzung der Datensicherheit Art. 5 lit. h nDSG und zum Grundsatz der Datensicherheit Art. 8 nDSG, zudem zur Meldepflicht bei Verletzungen der Datensicherheit Art. 24 nDSG; sodann relevant sind die Massnahmen gemäss Art. 7 und Art. 22 nDSG; eine gute Übersicht zur Datensicherheit findet sich bei Beranek Zanon, in: Thouvenin/Weber (Hrsg.), 86 ff., 94 ff.; sodann zu Vorgaben zur Datensicherung ausserhalb des DSG, insb. aber nach DSG vgl. Lehmann/Sauter, in: Schweizer (Hrsg.), 135 ff.; zu den Themen Datenschutz und IT-Sicherheit sodann Tinne-

neuen Akzente zu einem *Perspektivenwechsel in der Datenschutzregulierung*, wonach die systematische und konsequente Forderung nach Vorkehrungen zum Datenschutz *und* zur Gewährleistung der Datensicherheit primär von den Verantwortlichen zu implementieren ist. Dabei werden risikobasiert verschiedene Umsetzungsinstrumente vorgesehen. Anhand der Weiterentwicklungen im Zusammenhang mit der Datensicherheit fliesst wiederum eine im Vergleich zu einem einzelfallorientierten, deliktsrechtlich gedachten Verletzungsfall des Datensubjektes, gegen welchen in erster Linie über eine persönlichkeitsrechtliche Klage durch das Individuum vorgegangen werden soll, neue Konzeptionierung ein.[993] Auch hier sind es die datenverarbeitenden Stellen, die früher und an erster Stelle konsequent und nachhaltig in die Pflicht sowie Eigenverantwortung genommen werden, die datenschutzrechtlichen Vorgaben mittels Datenschutzvorkehrungen zu implementieren und eine Strategie resp. ein Programm zur Datensicherheit zu entwickeln, umzusetzen und zu überprüfen.[994]

703 Bei der Datensicherheit handelt es sich um kein starres Konzept. Die Anforderungen lassen sich nicht abstrakt bestimmen. Im Sinne des Grundsatzes aus der Homöopathie «Gleiches mit Gleichem zu heilen» kommt den Technologien und ihrer Fortentwicklung bei der Gewährleistung der datenschutzrechtlichen Datensicherheit besondere Bedeutung zu. Damit verändert sich das, was zur Gewährleistung einer angemessenen Datensicherheit geboten ist, sukzessive. Zudem können Veränderungen in den Geschäftsmodellen Anpassungen der Datensicherheitsmassnahmen bedingen. Die zu treffenden, angemessenen Massnahmen zur Sicherstellung der Datensicherheit hängen stets von den *korrelierenden Risiken* der jeweiligen Verarbeitungshandlungen ab.[995]

704 Art. 7 Abs. 1 DSG fordert angemessene technische und organisatorische Massnahmen, um *unbefugtes Verarbeiten* zu verhindern. Die gemäss Art. 7 Abs. 2 DSG verlangten konkretisierenden Bestimmungen finden sich, den Dualismus des DSG rezipierend, differenziert für den privaten Bereich in Art. 8 ff. VDSG und für den öffentlichen Bereich des Bundes in Art. 20 ff. VDSG (beachte allerdings die im Zuge der Totalrevision des DSG ebenso revidierte Verordnung). Im privaten Bereich sind Verarbeitende zur Gewährleistung der Datensicherheit nicht nur

---

FELD/BUCHNER/PETRI, 413 ff.; einschlägige Bestimmungen finden sich zudem in der ausführenden Verordnung, die mit der Totalrevision des DSG revidiert wird, wobei entsprechende Anpassungen hier nicht integriert werden können.

993 Vgl. zum Persönlichkeitsschutz als drittem Strukturmerkmal zweiter Teil, VI. Kapitel. Ebenda wird der Fokus auf den privaten Bereich verengt.

994 Vgl. Botschaft 2017–1084, 1 ff., 30 und 34.

995 Vgl. STAMM-PFISTER, BK-DSG, Art. 7 N 9 ff.; dazu, dass die Sensitivität der Personendaten einen Einfluss auf die Beurteilung der Angemessenheit der Massnahmen hat LEHMANN/SAUTER, in: SCHWEIZER (Hrsg.), 135 ff., 139; vgl. zu den Sicherheitsmassnahmen zwecks Gewährleistung der Informationssicherheit in Netzwerken im Zusammenhang mit haftungsrechtlichen Fragen der Internet-Provider nach Schweizer Recht ROHN, 41 ff., aber auch 263 ff.

datenschutzrechtlich, sondern ebenso basierend auf Handels- oder Geschäftsgeheimnissen verpflichtet.[996]

705 Mit den Massnahmen zur Gewährleistung der Datensicherheit werden primär solche des Schutzes vor *unberechtigten Zugriffen* durch Datendiebstahl, Phishing sowie vor Datenverlusten, Fälschungen oder widerrechtlichen Verwendungen aufgeführt. Die Sicherung von Personendaten vor dem *Zugriff durch Unbefugte* gilt als Kernelement der Schutzvorgaben; die Konsequenzen unbefugter Zugriffe infolge unzureichender Sicherungsvorkehrungen haben meist weitreichende Auswirkungen, nicht zuletzt, weil grosse Datenmengen mit unter Umständen sensiblen resp. besonders schutzwürdigen Personendaten in den Einflussbereich Unberechtigter gelangen können.[997] Die Verarbeitungshandlungen sind in der Folge kaum mehr kontrollierbar – *a fortiori* nicht durch die Datensubjekte selbst.

706 Allerdings wird vertreten, dass sich die Tragweite von Art. 7 Abs. 1 DSG nicht darin erschöpft, den Zugriff durch Unbefugte zu verhindern. Vielmehr leite der Grundsatz dazu an, ganz allgemein die unbefugte Datenbearbeitung zu verhindern.[998] Art. 7 Abs. 1 DSG verlange generell *angemessene Massnahmen* zur Verhinderung auch unrechtmässiger, unverhältnismässiger oder zweckwidriger Datenbearbeitung i. S. v. Art. 4 Abs. 1–4 DSG. Zur Frage, ob sich Art. 7 DSG über einen eigenständigen Regelungsgehalt hinausgehend auch auf die Grundsätze von Art. 4 Abs. 1–4 DSG erstreckt, soll nicht detailliert erörtert werden, zumal die Debatte eher theoretischer Natur ist.[999]

707 Die Pflicht, angemessene technische und organisatorische Massnahmen zur Sicherstellung der Einhaltung der datenschutzrechtlichen Verarbeitungsgrundsätze zu treffen, wird *direkt und unmittelbar* aus diesen selbst abgeleitet.[1000] Es steht ausser Frage, dass diese grossen materiellen Grundsätze des Datenschutzrechts der Implementierung durch passende Massnahmen bedürfen.

708 Zudem darf angenommen werden, dass mit einem Verstoss gegen den Grundsatz der Datensicherheit oft zugleich weitere Grundsätze tangiert und verletzt werden. Meier konstatiert insofern, dass die Datensicherheit im weiteren Sinne – die ma-

996 Meier, N 781.
997 Vertiefend zweiter Teil, VI. Kapitel.
998 Rosenthal, HK-DSG, Art. 7 N 7.
999 So räumt Rosenthal, HK-DSG, Art. 7 N 7 ein, dass es sich eher um eine Frage von akademischem Interesse handelt. Eine etwas anders gelagerte, für personendatenverarbeitende Stellen indes besonders problematische Konstellation liegt vor, wenn im Rahmen eines Datensicherheitsvorfalles, beispielsweise eines Hacking-Angriffes, auf sog. sensible Personendaten zugegriffen wird, zu deren Haltung die betroffene Stelle, hätte sie die Verarbeitungsgrundsätze eingehalten, gar nicht mehr berechtigt wäre. Der Datensicherheitsvorfall und unter Umständen die Enthüllung eines Verstosses gegen die Vorgaben des Grundsatzes der Datensicherheit figurieren dann zugleich als Detektor für Verletzungen der materiellen Datenschutzgrundsätze gemäss Art. 4 DSG resp. Art. 6 nDSG.
1000 Vgl. umfassender zu den zu ergreifenden Massnahmen technischer, organisatorischer, baulicher und rechtlicher Natur zwecks Umsetzung der Datenschutz-Compliance Art. 24 DSGVO.

terielle Legitimität der Datenbearbeitung – ein Ziel des gesamten Datenschutzgesetzes sei.[1001] Dagegen verpflichte die Datensicherheit im engeren Sinne darauf, zu gewährleisten, dass keine unbefugten Personen Zugriff auf Daten und damit die Möglichkeit einer Bearbeitung haben.[1002]

709 Dass der Grundsatz der Datensicherheit i. e. S. eine eigenständige Bedeutung hat, dokumentieren die ausführenden Bestimmungen gemäss Art. 8–10 VDSG (vor Revision). Die Vorgaben an die Datensicherheit werden somit in der ausführenden Verordnung zum Datenschutzgesetz präzisiert.

710 Die Verabschiedung der Totalrevision des DSG im Parlament am 25. September 2020 bedingte auch die Anpassung der Ausführungsbestimmungen zum DSG. Die Revision der VDSG sowie VDZS (Datenschutzzertifizierung) wurden 2022 verabschiedet.[1003] Entsprechend findet sich nachfolgend eine Darstellung der Bestimmungen der VDSG nach noch nicht revidierter Fassung.

711 Art. 8 Abs. 1 VDSG umschreibt die Komponenten der Datensicherheit i. S. v. Art. 7 Abs. 1 DSG: Umzusetzen ist erstens die *Vertraulichkeit*, wonach Personendaten nur durch befugte Personen verarbeitet werden. Zweitens ist die *Verfügbarkeit* zu gewährleisten, wonach Personendaten disponibel zu sein haben, wenn sie gebraucht werden. Drittens wird die *Integrität* verlangt, nach welcher sicherzustellen ist, dass Personendaten nicht unbefugterweise verändert werden dürfen.[1004] Dem Schutz von Systemen vor den Risiken der Vernichtung, des Verlustes, technischer Fehler, Fälschungen, des Diebstahls oder widerrechtlicher Verwendung, des unbefugten Änderns, Kopierens, Zugriffs oder anderer unbefugter Bearbeitungen kommt spezifische Bedeutung zu.[1005]

712 Massnahmen zur Gewährleistung der Datensicherheit sind sowohl für technologisch unterstützte sowie digitale Systeme und Verarbeitungshandlungen (Stichworte «Cyber Security», «Cyber Defense») wie auch für manuelle Verarbeitungen zu ergreifen.[1006] Angezeigt sein können z. B. auch raumgestalterische Massnahmen (Sichtschutz) oder Weisungen, wonach bestimmte Akten «unter Verschluss» zu halten sind.

713 Ob die getroffenen Massnahmen zur Gewährleistung der Datensicherheit *angemessen* sind, bestimmt sich nach Zweck, Art und Umfang der Datenbearbeitung

1001 Meier, N 780.
1002 Vgl. Ders., N 785 ff.
1003 Vgl. <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html> (zuletzt besucht am 3. Juni 2021).
1004 Vgl. zu den Umschreibungen Stamm-Pfister, BSK-DSG, Art. 7 N 7; Epiney/Civitella/Zbinden, 30 f.
1005 Vgl. Art. 7 Abs. 1 lit. a–d VDSG (vor Revision).
1006 Vgl. vertiefend allerdings zu spezifischen Bedeutungszusammenhängen von Cyber Security Hansen/Nissenbaum, Int. Stud. Q. 2009, 1155 ff.; zur Regulierung von Cyber Security sowie den Verantwortlichkeitsfragen Studer/de Werra, Expert Fokus 2017, 511 ff.

und Einschätzung potentieller Risiken für die Betroffenen sowie nach dem aktuellen Stand der Technik, Art. 8 Abs. 2 lit. a–d VDSG. Insofern werden in entsprechenden Korrelationen *vier verschiedene Schutzniveaus* unterschieden.[1007]

714 Die Vorgaben an die Datensicherheit implementieren *einen risikobasierten Ansatz*. Die Anforderungen zur Gewährleistung der Datensicherheit variieren je nach Risiken und hierbei auch Verarbeitungskonstellationen (Kategorie der Personendaten, Verarbeitungszusammenhang, Menge und Tiefe der bearbeiteten Personendaten usf.). Die Anforderungen an die Datensicherheit für den öffentlichen Bereich sind höher als für den privaten Bereich: Die Pflicht zum Erlass eines Bearbeitungsreglements geht für den privaten Sektor weniger weit als bei Bundesorganen.[1008] Allgemein anerkannt ist unter dem Grundsatz der Datensicherheit zudem, dass absolute Sicherheit nicht verlangt werden kann.[1009]

715 Obwohl die Einhaltung des Grundsatzes der Datensicherheit gemäss der expliziten Anknüpfung des Datenschutzrechts, vgl. Art. 1 DSG resp. Art. 1 nDSG, auf den Schutz der Datensubjekte abzielt, ist seine Einhaltung ebenso im *Interesse der Verarbeitenden*. Dies gilt *a fortiori*, sobald die Einhaltung des Datenschutzrechts und der Datensicherheit eine aufgewertete Bedeutung in Recht und Gesellschaft erfährt. Diese Aufwertung ist im Zuge der jüngsten datenschutzrechtlichen Neuerungswellen unübersehbar. Die Verarbeitenden sollten namentlich nicht die Folgen von medialen Reaktionen auf Datensicherheitsvorfälle und damit einhergehende Reputations- und Vertrauensverluste ausblenden.[1010] Verstösse gegen die Datensicherheit, Datenschutzpannen sowie daraus resultierende Reputationsverluste sind zudem in besonders empfindlicher Weise geeignet, einschneidende wirtschaftliche Konsequenzen für die Unternehmen nach sich zu ziehen.[1011] Es wird indes davon ausgegangen, dass zahlreiche Unternehmen die Vorgaben der Datensicherheit nicht eingehalten haben. In der Zeit vor dem Inkrafttreten der DSGVO und vor der Planung einer Totalrevision des DSG wurden indes allfällige rechtli-

1007 Meier, N 793.
1008 Vgl. Rosenthal, HK-DSG, Art. 7 N 21 f.
1009 Insofern ist die Situation vergleichbar mit den Reflexionen im Rahmen der Vorgaben zum Richtigkeitsgebot, wo ebenso wenig von einer Nullfehler-Vorgabe ausgegangen werden kann.
1010 Vertiefend zur Problematik des Vollzugsdefizites des (bisherigen) Datenschutzrechts dritter Teil, VII. Kapitel, A.
1011 Vgl. Aerotelegraph, Datenleck: Kriminelle erbeuten Passagierdaten von British Airways, Zürich 2018, <https://www.aerotelegraph.com/datenleck-bei-british-airways-kundendaten-gefaehrdet> (zuletzt besucht am 30. April 2021); Blick, Gescannte Führerausweise und Pässe waren einsehbar, Mega-Datenleck bei VW, Tesla und Co.!, Zürich 2018, <https://www.blick.ch/news/wirtschaft/automobilindustrie-bericht-datenleck-bei-autobauern-ueber-100-unternehmen-betroffen-id8640517.html> (zuletzt besucht am 30. April 2021); Blick, Datenleck beim Krankenversicherer CSS, Heikle Infos über Kundin landeten bei Fremdem, <https://www.blick.ch/news/wirtschaft/datenleck-beim-krankenversicherer-css-heikle-infos-ueber-kundin-landeten-bei-fremdem-id8549037.html> (zuletzt besucht am 30. April 2021); zum medialen Rauschen als Hauptwirkung des Datenschutzes Vesting, in Ladeur (Hrsg.), 155 ff., 182; Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f., 23.

che Konsequenzen bei einer Verletzung der Datensicherheitsvorgaben noch als bedeutungslos beurteilt.[1012]

716 Mittlerweile wurden im Anwendungsbereich der DSGVO entsprechende Sicherheitsvorfälle bereits mit einschneidenden Bussen belegt.[1013] Mit den aktuellen datenschutzrechtlichen Neuerungen gewinnt das Datenschutzrecht selbst deutlich an Wirkungskraft. Damit einhergehend haben die Vorgaben für die Datensicherheit *merkliche Stärkung* erfahren.[1014]

717 Die DSGVO verlangt unter dem Titel der Datensicherheit gemäss Art. 5 Abs. 1 lit. f. DSGVO, dass Personendaten nur in einer Weise verarbeitet werden dürfen, die eine angemessene Sicherheit gewährleistet, was mit den Begriffen «Integrität» und «Vertraulichkeit» bezeichnet wird.[1015] Entsprechend ergriffene Massnahmen haben auf sämtlichen Verarbeitungsstufen und während des *gesamten Lebenszyklus von Personendaten* und deren Verarbeitungen zu greifen. Sie zielen darauf ab, das Risiko ungewollter Datenverluste, Transfers, Zerstörungen oder Beschädigungen sowie, allgemeiner, unrechtmässiger Datenverarbeitungen zu reduzieren. Der Verarbeitungsgrundsatz wird insb. über Art. 32 ff. DSGVO, aber auch Art. 24 f. DSGVO konkretisiert.[1016] Mit Blick auf diese Bestimmungen bestehen teilweise Abgrenzungsschwierigkeiten.

718 Art. 32 DSGVO, der den Abschnitt 2 mit dem Titel «Sicherheit personenbezogener Daten» einleitet, steht seinerseits unter dem Titel der «Sicherheit der Verarbeitung». Sowohl von einem Verantwortlichen wie vom Auftragsverarbeiter wird verlangt, geeignete technische und organisatorische Massnahmen (TOM) zur Gewährleistung eines angemessenen Schutzes vor der Verletzung von Rechten und Freiheiten der Datensubjekte zu ergreifen.[1017] Art. 32 DSGVO befasst sich folglich auch, aber nicht nur mit dem technischen Datenschutz, indem er die Gewährleistung der «Daten- und Systemsicherheit» verlangt («Sicherheitsmassnahmen»).[1018] Im Kontext des Schutzes der Integrität von informationstechnischen Systemen sei spezifisch auch auf das Urteil des Bundesverfassungsgerichts verwie-

1012 Rosenthal, HK-DSG, Art. 7 N 21.
1013 Zum Bussgeld, das gegenüber British Airways im Jahr 2020 verhängt wurde, vgl. <https://www.bbc.com/news/technology-54568784> (zuletzt besucht am 3. Juni 2021).
1014 So auch Reimer, NomosKomm-DSGVO, Art. 5 N 45.
1015 Ders., a. a. O., Art. 5 N 45 ff.; Meier, N 786 ff.; Stamm-Pfister, BK-DSG, Art. 7 N 7 und N 24 ff.; vgl. zum Grundsatz auch Art. 8 nDSG.
1016 Vgl. auch Herbst, BeckKomm-DSGVO, Art. 5 N 76.
1017 Bei den sog. TOM handelt es sich um Massnahmen, die sowohl von einem Verantwortlichen als auch einem Auftragsverarbeiter zu ergreifen sind. Neben solchen «gemeinsamen» Vorgaben gibt es sodann solche, die nur vom Verantwortlichen zu beachten sind, und solche, die lediglich den Auftragsverarbeiter treffen. Eine entsprechende Rollendifferenzierung und daraus resultierende teilweise Differenzierungen der Vorgaben der DSGO sind Kernelemente des Regelungsregimes der DSGVO; zu den Rollen des Verantwortlichen und des Auftragsverarbeiters vgl. Art. 4 Nr. 7 resp. Nr. 8 DSGVO und Art. 26 DSGVO.
1018 Jandt, BeckKomm-DSGVO, Art. 32 N 1.

sen, das 2008 mit dem sog. Computer-Grundrecht eine spezielle Ausprägung des allgemeinen Persönlichkeitsrechts anerkannte.[1019]

719 Damit Massnahmen i. S. v. Art. 32 DSGVO als geeignet qualifiziert werden können, sind neben dem Stand der Technik die Eintrittswahrscheinlichkeit eines Vorfalles sowie die (materiellen und immateriellen) Folgen und die Schwere der Risiken zu ermitteln, wobei Art, Breite und Tiefe der Personendaten(bestände) ebenso einschlägig sind. Die zu treffenden technischen und organisatorischen Massnahmen zur «Datensicherheit» orientieren sich, wie erwähnt, an einem risikobasierten Ansatz, wobei insofern die sog. Datenschutz-Folgenabschätzung gemäss Art. 35 DSGVO vor Augen zu halten ist. Im Rahmen der Evaluation der Eignung der zu ergreifenden Sicherheitsmassnahmen können die Implementierungskosten in die Analyse miteinbezogen werden.

720 Hinsichtlich der angemessenen Massnahmen zur Datensicherheit ist weiter Art. 24 DSGVO in Betracht zu ziehen, wobei die Abgrenzung gegenüber Art. 25 DSGVO sowie Art. 32 DSGVO nicht gänzlich geklärt ist. Art. 24 DSGVO wird als Generalauftrag zur Gewährleistung der Datenschutz-Compliance sowie der Datensicherheit beschrieben.[1020] Die Bestimmung verpflichtet Verantwortliche und Auftragsverarbeitende, alle sachlich notwendigen Vorkehrungen zur Gewährleistung der Datenschutz-Compliance und -Sicherheit zu ergreifen.[1021] Mit «Datenschutzvorkehrungen» sind Compliance- und Sicherheitsmassnahmen gemeint, die erforderlich und verhältnismässig sind, um die Einhaltung der DSGVO zu gewährleisten. Dazu gehören betriebliche Massnahmen technischer, baulicher, rechtlicher und organisatorischer Natur.[1022] In Bezug auf die Gewährleistung der Datensicherheit sowie auf das Vorgehen bei Datensicherheitsvorfällen kommt der angemessenen Schulung und Instruktion der Mitarbeitenden Bedeutung zu.

721 Für die Implementierung angemessener Massnahmen der Datensicherheit ist, um das Bild zu vervollständigen, auf weitere *Umsetzungsinstrumente* hinzuweisen. Sie finden sich in der DSGVO. Die Totalrevision des DSG sieht vergleichbare Instrumente und Normen vor. Sie sollen nachfolgend in Kürze umrissen werden:

722 Der Erfüllung der Sicherheitsvorgaben dient zunächst das sog. *Verarbeitungsverzeichnis* als Basisinstrument, vgl. Art. 30 DSGVO und Art. 12 nDSG. Es bildet die Landschaft der Verarbeitungsprozesse, die Kategorie von Personendaten so-

1019 BVerfGE, Az. 1 BvR 270/07 – Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Urteil vom 27. Februar 2008; zu diesem sog. Computer-Grundrecht namentlich Karavas, Neue Zeitschrift für Sozialforschung 2010, 95 ff.; Gusy, DuD 2009, 33 ff.; Böckenförde, JZ 2008, 925 ff., 927 ff.; Dralle, 5 ff.

1020 Raschauer, NomosKomm-DSGVO, Art. 24 N 1.

1021 Ders., a. a. O., Art. 24 N 1 ff.

1022 Ders., a. a. O., Art. 24 N 10 f.

wie die Personendatenflüsse ab, womit sich die zu ergreifenden angemessenen Sicherheitsmassnahmen klarer bestimmen lassen.

723 Weiter leistet die erwähnte *Datenschutz-Folgenabschätzung* einen Beitrag zur «Sicherung der Datensicherheit», Art. 35 DSGVO und Art. 22 nDSG. Sie ist bei besonders «riskanten» Verarbeitungen vorzunehmen, wobei sich hieraus Rückschlüsse auf die zu treffenden angemessenen (Sicherheits-)Massnahmen ergeben.[1023] Das Instrument verlangt im Vorfeld die Evaluierung von Risiken sowie von angemessenen Mitigationsmassnahmen.

724 Zudem sind im Zusammenhang mit der Datensicherheit im Sinne eines «Vorfeldschutzes» die Bestimmungen und Vorgaben einschlägig, die unter dem Terminus des «*privacy by design*» (Gewährleistung von Datenschutz durch Technikgestaltung) resp. «*privacy by default*» (Gewährleistung von Datenschutz durch datenschutzfreundliche Voreinstellungen) figurieren, vgl. Art. 25 DSGVO und Art. 7 nDSG. Im Rahmen von «privacy by design» sind Aspekte des Datenschutzes und der Datensicherheit bereits im Zuge der Prozessentwicklung zu integrieren.

725 Die Datensicherheit wird sodann neuerdings über die *Meldepflichten* im Zusammenhang mit sog. *Datensicherheitsvorfällen* adressiert, Art. 33 f. DSGVO, sog. Data Breach Notification. Die Totalrevision sieht neu explizit entsprechende Pflichten vor, vgl. Art. 24 nDSG. Ein Datensicherheitsvorfall liegt bei einer Verletzung der Sicherheit von Personendaten vor. Angenommen wird eine solche für den Fall, in welchem ein Defizit bezüglich der Datensicherheit infolge ungenügender technischer oder organisatorischer Massnahmen zu einer objektiv unbeabsichtigten, unrechtmässigen oder unbefugten Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten führt.[1024] Nach DSGVO gilt eine Notifikationspflicht gegenüber den Aufsichtsbehörden mit einer Meldefrist von 72 Stunden, wobei die Etablierung entsprechender Prozesse die verarbeitenden Stellen in der Praxis vor Herausforderungen stellt. Zudem greift eine Meldepflicht gegenüber den Betroffenen für den Fall, dass die Verletzung der Datensicherheit ein hohes Risiko für diese darstellt.[1025]

726 Der Verantwortliche und ggf. der Auftragsverarbeiter sind gemäss Art. 33 Abs. 5 DSGVO verpflichtet, nicht nur die getroffenen Massnahmen zur Datensicherheit und eine Risikoeinschätzung, sondern auch Verletzungen mit sämtlichen einschlägigen Informationen zu *dokumentieren*.[1026] Auch gemäss Art. 24 Abs. 1 und

1023 Hierzu WP 248 (Entwurf); ISO 2913:2017; beachte sodann die Liste der Datenschutzstelle des Fürstentum Liechtensteins, abrufbar unter: <https://www.datenschutzstelle.li/application/files/6715/5127/0000/Liste_der_Verarbeitungstaetigkeiten.pdf> (zuletzt besucht am 30. April 2021).

1024 Vgl. auch Art. 4 Nr. 12 DSGVO zum sog. Eintritt einer Verletzung des Schutzes personenbezogener Daten Jandt, BeckKomm-DSGVO, Art. 32 N 7.

1025 Vgl. WP 29/248, Data Breach Notification, WP250rev.01, 20 ff., 30 ff.

1026 Vgl. DSGVO ErwG 85.

Art. 5 Abs. 2 DSGVO müssen die Verantwortlichen in der Lage sein, jederzeit Rechenschaft über die risikobasiert evaluierten und angemessenen Massnahmen ablegen zu können.[1027] Die Totalrevision des DSG sieht keine entsprechende explizite Dokumentationsvorgabe vor. Sie wird allerdings in der Praxis bereits heute als Element der datenschutzrechtlichen Governance beurteilt und umgesetzt.

727 Anhand der gerade im Zusammenhang mit der Datensicherheit beschriebenen Instrumente zeigen sich *zwei Aspekte*, die mit den datenschutzrechtlichen Neuerungen Akzentuierung finden: Erstens sollen die Verarbeitungsgrundsätze durch einen Katalog neuer Instrumente auch faktisch effizient umgesetzt werden. Zweitens wird anhand dieser Instrumente die zeitliche und prozesshafte Dimension des neueren Datenschutzrechts sichtbar. Die entsprechenden Massnahmen sichern die Vorgaben an die Datensicherheit über sämtliche Etappen der Verarbeitungszyklen ab.

728 Der Ausbau von Vorgaben an Massnahmen zwecks Einhaltung der Datensicherheit und hierbei insb. des technischen Datenschutzes reflektiert gewissermassen ein Prinzip des *vices rependere* (Gleiches mit Gleichem vergelten) und ebenso des *Verursacherprinzips* (polluter pays principle, namentlich für das Umweltrecht bekannt).[1028] Markiert wird damit ein Trend, das Augenmerk auf die faktische Verwirklichung und die Umsetzung des Rechts in der Realität zu lenken.[1029] Mit dem Trend, technische, aber auch organisatorische sowie prozedurale Massnahmen vorzusehen, um dem Datenschutzrecht mit dem Aspekt der Datensicherheit in der Realität Griffigkeit zu verleihen, steht das Datenschutzrecht nicht isoliert da – ebenso wenig mit der Korrelierung, die Zuständigkeit hierfür in erster Linie in die Hände des Verursachers resp. des «Geschäftsherren» («Verantwortlichen») zu legen.

729 Beschrieben wird diese Entwicklung, die durch diverse Prozesse konstituiert wird, auch als Integration des Datenschutzes und der Datensicherheit in die DNA der verarbeitenden Organisationen.[1030] Teilelemente sind insofern die Durchführung der Datenschutz-Folgenabschätzung, die Erstellung des Inventars, aber auch die Etablierung der Prozesse zwecks Erfüllung der Meldepflichten bei Datensicherheitsvorfällen.

1027 Sog. Accountability-Ansatz.

1028 Zum Verursacherbegriff im Umweltrecht Caluori, URP 2011, 541 ff.; zum Verursacherprinzip in diesem Kontext auch Rööösli, URP 2021, 117 ff., unter Darstellung des Instruments der Gesundheitsgefährdungsabschätzung, die als Parallele zur Risikofolgenabschätzung der neuen Datenschutzerlasse gesehen werden kann; zu Umwelt, Sicherheit sowie Information und damit zur Herausbildung eines Umwelt-, Sicherheits- und Informationsstaates Hassemer, in: Simon/Weiss (Hrsg.), 121 ff., 122 ff.

1029 Eine entsprechende Entwicklung lässt sich zudem für den Kontext des Familienrechts nachweisen.

1030 Vgl. hierzu Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f., 23.

730 Anhand der erwähnten Instrumente lässt sich unter dem Aspekt der Datensicherheit eindrücklich nachzeichnen, inwiefern der Datenschutz und das Datenschutzrecht im Begriff sind, einen *Systemwechsel zu vollziehen*: Die Existenz und Relevanz des Datenschutzrechts soll sich nicht erst im Falle einer «widerrechtlichen Persönlichkeitsverletzung» und einer resultierenden Klage manifestieren und aktualisieren. Mit den datenschutzrechtlichen Neuerungen findet eine Ergänzung und punktuell eine Abkehr von einer individualrechtlichen und defensivrechtlichen Anknüpfung des Datenschutzrechts statt. Neu wird die Einhaltung des Datenschutzrechts und damit auch der Datensicherheit zur *Governance- und Compliance-Aufgabe*, für die an erster Stelle die «Verantwortlichen» in die Pflicht genommen werden. Die entsprechenden Pflichten lassen sich nicht in einem einmaligen Akt erfüllen. Vielmehr bedarf es eines kontinuierlichen, risikobasierten Managements der diversen Prozesse, welche die Vorgaben des Datenschutzrechts und damit auch der Datensicherheit gewährleisten sollen. Gerade anhand des Grundsatzes der Datensicherheit wird hierbei der risikobasierte Ansatz der datenschutzrechtlichen Neuerungen deutlich.

731 Im Ergebnis wird damit der Datenschutz zu einem Element des Risikomanagements.[1031] Wenn die ergriffenen Massnahmen und deren Angemessenheit zur Gewährleistung der Datensicherheit gemäss dem Accountability-Ansatz zu dokumentieren sind und der Verarbeitende insofern in der Rechenschaftspflicht steht, wird ein weiterer Kontrapunkt gegenüber einem bisher persönlichkeitsrechtlich und damit deliktsrechtlich gedachten Datenschutzrecht gesetzt, der die primäre «Eigenverantwortung» der Verarbeitenden anerkennt.

732 Damit sind die Erkenntnisse *zu den generalklauselartigen Verarbeitungsgrundsätzen* als zweites Strukturmerkmal des DSG zu resümieren.

C. Ergebnisse

733 Die vorangehenden Ausführungen haben sich mit den gemeinsam für den öffentlichen und den privaten Bereich statuierten «allgemeinen» und über weite Strecken generalklauselartig formulierten Verarbeitungsgrundsätzen befasst, wie sie das eidgenössische Datenschutzgesetz in seiner noch in Kraft stehenden Fassung

1031 Zur Forderung eines Perspektivenwechsels im Datenschutzrecht weg vom «Schadensrecht» hin zum Risikorecht: Ladeur, Vortrag, Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021); zur Bedeutung der Kategorien «Risiko» (und «Vertrauen») für das heutige Zusammenleben im Zusammenspiel mit dem Privaten als Schutzkonzept Hotter, 74 ff.; auf die Relevanz von risiko- und zweckbezogenen Erwägungen für eine ausdifferenzierte Gestaltung des Datenschutzrechts weist auch Rossnagel, digma 2011, 160 ff., 163 f. hin; zum Datenschutz als Risikorecht auch Donos, 179 ff.

in Art. 4 ff. DSG niederlegt.[1032] Nach der Totalrevision finden sich die allgemeinen Verarbeitungsgrundsätze in Art. 6 nDSG, der den Grundsatz der Datenrichtigkeit neu inkludiert. Die Vorgaben an die Datensicherheit normiert Art. 8 nDSG, wobei die ausführende Verordnung zum DSG in einer angepassten Fassung zu beachten ist.

734 Unter Reflexion der Lehre und Praxis wurde den grundsatzbasierten Verarbeitungsvorgaben Kontur verliehen, wobei ihre Inhalte und Funktionen konkretisiert wurden. Zur Erreichung des Ziels, die datenschutzgesetzlich generalklauselartigen oder offenen Bearbeitungsgrundsätze griffiger zu beschreiben, wurden zudem Erkenntnisse aus der allgemeinen Methodenlehre zu den unbestimmten Rechtsbegriffen sowie den Generalklauseln angewendet. Herausdestilliert wurden Kerninhalte, Akzente und Entwicklungslinien zu den einzelnen allgemeinen, weitgehend generalklauselartigen und damit abstrakten Verarbeitungsgrundsätzen.

735 Es wurden zugleich die Neuerungen berücksichtigt, wie sie mit der DSGVO, aber auch der Totalrevision des DSG vorgesehen werden. An den grossen und traditionsreichen materiellrechtlichen Verarbeitungsgrundsätzen wird weitgehend festgehalten. Für die Totalrevision des DSG stellt insb. der Ausbau der Transparenzvorgaben ein Kernelement dar, das sich seinerseits ebenso auf die Verarbeitungsgrundsätze bezieht. Eine wesentliche Neuerung im Zusammenhang mit den Verarbeitungsgrundsätzen bilden sodann die neuen Umsetzungsinstrumente. Weiter wurden die Stärkung der Eigenverantwortung, der risikobasierte Ansatz sowie der Accountability-Ansatz vorgestellt.

736 Zu den einzelnen allgemeinen generalklauselartigen Grundsätzen, die trotz dieser Trends als *zweites Strukturmerkmal* des noch geltenden, aber auch künftigen DSG benannt wurden, sind die folgenden Kernbefunde festzuhalten:

737 Das *Rechtmässigkeitsprinzip* wurde als *Koppelungsinstrument* qualifiziert. Als Metapher figurierte das «Drehkreuz», wobei über den Grundsatz – in verschiedene Richtungen gestellt – die *Gesamtlandschaft* datenschutzrechtlicher Vorgaben in Gestalt eines «Netzes» sichtbar wird. Vorab präsentiert es sich als Brücke für die *ausserhalb* des Datenschutzgesetzes befindlichen datenschutzrechtlichen Vorgaben. Von besonderer Bedeutung sind hierbei zahlreiche spezifische Informationsnormen, wie sie in Spezialgesetzen, weiter im OR oder im ZGB zu finden sind. Sie formulieren bereichs-, sektor- oder kontextspezifische datenschutzrechtliche Vorgaben.[1033] Die Koppelungsfunktion des Rechtmässigkeitsprinzips des DSG zeigt sich indes *nicht nur nach aussen*, sondern auch *nach innen unter Be-*

1032 Vgl. Art. 6 nDSG.

1033 Grundlegend zu Art. 328b OR und DSG sowie zum Datenaustausch zwischen Arbeitgeber und Versicherung, Pärli, insb. 123 ff.

zugnahme auf das duale Regime des DSG. Über das Rechtmässigkeitsprinzip erfolgt die Anknüpfung des gewählten *Ausgangspunktes*. Rechtmässigkeit bedeutet gemäss DSG mit Blick auf den Ausgangspunkt der Datenverarbeitung – Grundsatz des Verarbeitungsverbotes mit Erlaubnisvorbehalt für den öffentlichen Bereich resp. Grundsatz der Verarbeitungsfreiheit mit Schranken für den privaten Bereich – nicht dasselbe.[1034] Unrechtmässig sind im privaten Bereich, unter Anlehnung der Datenschutzgesetzgebung an Art. 28 ZGB, nur qualifizierte Personendatenverarbeitungen.[1035] Hierbei gelten namentlich Verstösse gegen die allgemeinen Verarbeitungsgrundsätze als Schranken der grundsätzlich freien Datenverarbeitung; ihre Verletzung begründet die unrechtmässige Personendatenverarbeitung und damit die Persönlichkeitsverletzung. Das Vorliegen von Rechtfertigungsgründen ist in einem zweiten Schritt zu prüfen. Anders dagegen bedarf die rechtmässige Personendatenverarbeitung im öffentlichen Recht prinzipiell eines Erlaubnistatbestandes basierend auf einer rechtlichen Grundlage. Das *Rechtmässigkeitsprinzip* im schweizerischen Datenschutzrecht ist folglich *kein einheitliches Prinzip*. Vielmehr inkorporiert es ein differenziertes Regime für die verschiedenen Bereiche, namentlich auch des traditionsreichen «Zweikammersystems» mit dem öffentlichen Bereich gegenüber dem privaten Bereich. Mit einer solchen Strukturierung implementiert man in der Schweiz über das Rechtmässigkeitsprinzip ein *nuanciertes und abgestuftes Datenschutzregime, das sich harmonisch in die gesamte Rechtsordnung mit ihren für die jeweiligen Bereiche etablierten Leitprinzipien einfügt*. Im DSG wird damit, obschon dieses als Querschnittsgesetz oftmals gewissermassen als Synonym für das Datenschutzrecht gelesen wird, in markanter Weise auch über das Rechtmässigkeitsprinzip die datenschutzrechtliche Einschlägigkeit *bereichsspezifischer Ausdifferenzierung* sichtbar. Dagegen geht die DSGVO zumindest dergestalt zu einem «bereichsindifferenten Modell» über, als dass diese dem Grundsatz nach identische Vorgaben für die rechtmässige Verarbeitung von Personendaten durch öffentliche Stellen wie Private formuliert. Anknüpfend an das Rechtmässigkeitsprinzip sowie die im zweiten Teil, IV. Kapitel herausgearbeitete *duale Struktur des DSG* sah man sich folglich wiederholt mit der Herausforderung konfrontiert, die «gemeinsamen, allgemeinen Verarbeitungsgrundsätze», die dem Datenschutzrecht für den öffentlichen und den privaten Bereich als «gemeinsamer Nenner» vorangestellt sind, sinnvoll mit den «beiden Bereichen» zu korrelieren und harmonisieren.

738 Zum Verarbeitungsgrundsatz von *Treu und Glauben* wurde vorab statuiert, dass im Rahmen des noch in Kraft stehenden DSG die Transparenzvorgaben für den öffentlichen und privaten Bereich differieren. Als Kernbefund für Treu und Glauben im Datenschutzrecht wurde seine richtungsweisende und akzentu-

1034 Vertiefend zum Dualismus als erstes Strukturmerkmal zweiter Teil, IV. Kapitel.
1035 Vertiefend hierzu zweiter Teil, VI. Kapitel.

ierte Bedeutung in Bezug auf das *Thema der Transparenz* herausdestilliert. Vom Grundsatz geht, so wurde es nachgewiesen, eine *dezidierte Anstosswirkung in Bezug auf den Ausbau von Transparenzvorgaben* aus. Weit weniger produktiv entfaltet sich Treu und Glauben in seinem Charakter als Verarbeitungsgrundsatz in seiner Funktion als Handlungsanweisung gegenüber den Verantwortlichen und damit in der Praxis. Vielmehr liegt seine Hauptleistung in den Impulsen, die er für die Datenschutzgesetzgebung geliefert hat, womit er als *Quellrecht* für den Ausbau und die Erhöhung der Transparenzvorgaben im Datenschutzrecht zu bezeichnen ist. Hervorgegangen ist ein Fächer mit diversen Instrumenten und variablen Stossrichtungen: Neben den aktiven Informationspflichten gegenüber den Datensubjekten und den Einwilligungsvorgaben schaffen neue oder ausgebaute Meldepflichten, Auskunftsrechte, Dokumentations- und Rechenschaftspflichten, die Pflicht zur Erstellung des Verarbeitungsverzeichnisses, aber auch Zertifizierungsverfahren erhöhte Transparenz in Bezug auf Prozesse der Personendatenverarbeitung sowie ihrer Übereinstimmung mit den datenschutzrechtlichen Vorgaben. Die umfassenden Rechenschafts- und Dokumentationspflichten bezüglich der zur Einhaltung des Datenschutzes implementierten Massnahmen bilden ein zentrales Instrument, um Verarbeitungsprozesse transparent und damit auch auf ihre Rechtskonformität hin überprüfbar zu machen. Freigelegt wurde somit ein *Trend*, über Treu und Glauben im Rahmen des Datenschutzes *Transparenzerfordernisse sowie Dokumentations- und Rechenschaftspflichten* in diversen Facetten auszubauen sowie die Verantwortlichkeiten für die Einhaltung der Datenschutzvorgaben nachhaltig und früher in den Zuständigkeitsbereich der Verarbeitenden zu legen. Mit diesen massgeblich über Treu und Glauben vollzogenen Entwicklungen wird die Bedeutung der *Kategorie des Vertrauens* im und für das Datenschutzrecht adressiert, was auch der Tatsache geschuldet ist, dass die Bewältigung informationeller Herausforderungen nicht in identischer Weise geleistet werden kann, wie sie beispielsweise im Umgang mit Sachgütern möglich ist. Damit verbunden ist eine Veränderung der Perspektive dergestalt, dass der *integre Umgang mit Personendaten* vorgeschaltet und nachdrücklich in den Verantwortungsbereich der Verarbeitenden gestellt wird, womit sich eine Ergänzung resp. Überwindung der defensiv- und deliktsrechtlichen Konzeption manifestiert, wie sie in der persönlichkeitsrechtlichen Anknüpfung des Datenschutzrechts angelegt ist. Nebst dem Aspekt der Transparenz wurde unter dem Grundsatz von Treu und Glauben im Datenschutzrecht zudem auf die Figur der «vernünftigen Erwartungen» resp. die US-amerikanische Doktrin der *«reasonable expectations of privacy»* eingegangen, die ansatzweise in Europa Rezeption findet, namentlich in der Rechtsprechung des EGMR.[1036] Hier wurde dargelegt, inwiefern der Ansatz der *«reasonable expectations of privacy»* – nicht individualisiert, sondern

1036 Hierzu dritter Teil, IX. Kapitel; Paefgen, 33 ff.

kontextualisiert verstanden – Impulse geben kann, um tradierte Konzepte des geltenden Datenschutzrechts fortzuentwickeln.

739 Bezüglich des *Verhältnismässigkeitsgrundsatzes* wurde festgestellt, dass dieser – trotz des Grundsatzentscheides des DSG für ein duales System – im privaten wie im öffentlichen Bereich in seinem «öffentlich-rechtlichen» Gehalt der Trias von Eignung, Erforderlichkeit und Verhältnismässigkeit i. e. S. Anerkennung findet. Für beide Bereiche müssen Personendatenverarbeitungen geeignet sowie erforderlich zur Erreichung des Zweckes sowie verhältnismässig im engeren Sinne sein. Das ist zugleich bemerkenswert wie reflexionswürdig. Indem das Verhältnismässigkeitsprinzip als Mittel-Zweck-Relation mit *seinem «engen» öffentlich-rechtlichen Inhalt Gültigkeit auch für den privaten Bereich* beansprucht, wird *ebenso für den privaten Bereich* eine *Machtasymmetrie* in der Beziehung von Datenverarbeitenden und Betroffenen anerkannt. Gleichwohl wird die datenschutzrechtliche Beziehung zwischen Privaten und die hier anerkannte Machtasymmetrie *nicht identisch* gedacht im Vergleich zu derjenigen im öffentlichen Bereich. Die Anerkennung der Differenzierung kommt im Dualismus des DSG aufgrund des entgegengesetzten Ausgangspunktes zum Ausdruck, wobei ein aus dem öffentlichen Bereich in den privaten Bereich importiertes Verhältnismässigkeitsgebot in seiner Trias eine gewisse Angleichung bringt. Anders der Ansatz in einem monistischen System, wie es die DSGVO implementiert, wo eine identische Behandlung stattfindet resp. die Differenzierungswürdigkeit zwischen Personendatenverarbeitungen durch öffentliche und private Stellen verworfen wird. Ein Verhältnismässigkeitsprinzip, das die Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne ebenso für den privaten Bereich verlangt, setzt einer prinzipiellen Verarbeitungsfreiheit, wie sie im DSG für den privaten Bereich verankert wird, *eine enge, griffige und markante Schranke*. Entsprechend kommt dem Verhältnismässigkeitsprinzip eine entscheidende Rolle zu, Personendatenverarbeitungen im privaten Bereich zu limitieren und damit eine gewisse Annäherung an das datenschutzrechtliche Schutzniveau zwischen der Normierung im privaten und derjenigen im öffentlichen Bereich zu erreichen. Darüber hinausgehend wurde dargelegt, inwiefern der Verhältnismässigkeitsgrundsatz und namentlich seine faktische Einhaltung im Rahmen der jüngsten Revisionswellen durch verschiedene konkretisierte Instrumente und Vorgaben abgesichert wird. In diesem Zusammenhang sind erneut namentlich das Verarbeitungsverzeichnis, aber auch Löschungs- und Anonymisierungsvorgaben zu nennen. Das Verhältnismässigkeitsprinzip steht, obschon bis heute im DSG gemeinsam mit Treu und Glauben verankert, seinerseits in untrennbarem Zusammenhang mit dem *Verarbeitungszweck*.

740 In Bezug auf den *Verarbeitungszweck* wurden mehrere konkrete Vorgaben resp. Teilgehalte differenziert durchleuchtet. Dazu gehören insb. die vorgängige

Zweckfixierung und -definierung, die Zwecktransparenzvorgaben sowie die Zweckbindung im engeren Sinne. Im Rahmen der Ausführungen zu den Zweckgrundsätzen durfte sodann eine datenschutzrechtliche Kernfrage nicht unbeachtet bleiben: diejenige nach dem Zweck des Datenschutzrechts. Sie wurde vertieft analysiert, obschon Art. 1 DSG resp. Art. 1 nDSG eine klare Antwort hierauf zu geben scheinen. Anlass dafür, den gesetzlichen Schutzzweck resp. das Schutzobjekt zu hinterfragen, gab nicht nur die Tatsache, dass um die Erfassung des Schirmbegriffs der «Privatheit», der seinerseits als Schutzzweck des Datenschutzrechts gilt, bis heute intensiv gerungen wird. Im Zentrum stand eine Auseinandersetzung mit der Argumentation des Bundesverfassungsgerichts im Volkszählungsurteil zum Zweckbindungsgrundsatz. Im Zuge einer Analyse des Volkszählungsurteils des Bundesverfassungsgerichts, das mit seinem Recht auf informationelle Selbstbestimmung Rechtsgeschichte schrieb, wurde anhand eines bislang wenig rezipierten Aspekts des Urteils die *systemische sowie dynamische Dimension* des Datenschutzes sowie des Datenschutzrechts herausgeschält. Dieser Aspekt findet sich in den Ausführungen zu den Zweckgrundsätzen. Dreh- und Angelpunkt auch der verfassungsgerichtlichen Erwägungen war die *Anerkennung der Einschlägigkeit pluraler Verarbeitungszusammenhänge und Verarbeitungszwecke sowie die Erforderlichkeit, diese voneinander abzuschotten*: Die im Rahmen einer Volkszählung erhobenen Personendaten dürfen – trotz der Besonderheiten einer solchen Datenerhebung zur Erfüllung staatlicher Aufgaben – nicht beliebig für weitere Ziele und Zwecke der vielgestaltigen weiteren Aufgaben des Verwaltungsvollzuges (beispielsweise im Kontext der Steuererhebung, der Strafverfolgung oder Migration) genutzt werden. Der *öffentliche Bereich* wurde vom Bundesverfassungsgericht nicht als einheitlicher und gewissermassen monolithischer, sondern stattdessen als *facettenreicher, diversifizierter und pluralistischer Bereich* mit unzähligen Organisationseinheiten, Zielen und Verarbeitungszusammenhängen präsentiert – was ebenso datenschutzrechtlich als bedeutsam herausgestellt wird. Ausgangspunkt der *systemischen Dimension* des Datenschutzrechts ist damit vorab die Anerkennung *pluraler Verarbeitungszusammenhänge*, wobei der Zweckbindungsgrundsatz insofern einschlägig wird, als er Personendatenverarbeitungen an einen im Vorfeld definierten Verarbeitungszweck ankoppelt und damit ihre «unbeschränkte Diversifizierung» verhindert. Geschützt wird damit namentlich das Datensubjekt und dessen «Recht auf informationelle Selbstbestimmung», was die individualrechtliche Position abbildet. Diese Schutzdimension allerdings steht nicht isoliert da. Vielmehr dienen die fraglichen Vorgaben darüber hinausgehend zugleich dazu, die *Funktionstüchtigkeit und Integrität verschiedener Bereiche mit ihren Zielen, Instrumenten und Verarbeitungszusammenhängen zu gewährleisten*. Spezifisch für das Instrument der statistischen Erfassung der Bürgerinnen und Bürger hält das Bundesverfassungsgericht fest, dass lediglich das *Statistikgeheimnis die Integrität der statistischen Erhebung* und die hierzu

notwendige Kooperationsbereitschaft sowie das Vertrauen der Bürgerinnen und Bürger garantieren könne. Zwangsmassnahmen vonseiten des Staates dagegen können ebendies gerade *nicht* leisten.[1037] Nur wenn die aussagende Person darauf vertrauen kann,[1038] dass die erteilten Personenangaben nicht zu anderen Massnahmen des Verwaltungsvollzuges «gegen sie» verwertet werden, wird sie vollständig und korrekt die in der Volkszählung gestellten Fragen beantworten. Datenschutzrechtliche Vorgaben schützen folglich – so ein Kernergebnis des Urteils, seiner Analyse und dieses Teils – neben dem *Datensubjekt namentlich die Integrität und damit das Funktionieren verschiedener Subsysteme*. Das Volkszählungsurteil öffnet indes nicht nur das Fenster für einen Blick auf die *systemische Dimension* des Datenschutzrechts, sondern gleichermassen für seine *dynamische Dimension*. Es geht um den Schutz «angemessener Datenflüsse», wobei der Zweckbindungsgrundsatz das Instrument ist, einmal zu einem bestimmten Zweck erhobene Personendaten in ebendiesem Flussbett innerhalb eines bestimmten Bereiches, in einem spezifizierten Verarbeitungszusammenhang zu fixieren und den beliebigen, unbeschränkten und freien Übertritt in andere (Bereiche, Felder,) Flussbette zu verhindern. Anhand des Zweckbindungsgrundsatzes wurde dargelegt, dass sich der *Zweck des Datenschutzes und des Datenschutzrechts* nicht auf den Schutz des Datensubjektes, den Persönlichkeitsschutz oder ein Recht auf informationelle Selbstbestimmung beschränkt. Vielmehr zeigen sich neben der – bis anhin oft ausschliesslich betonten – subjektiven Dimension die systemische wie die dynamische Dimension des Datenschutzrechts. Kein Vorfall könnte diese bislang vernachlässigten Aspekte des Datenschutzrechts deutlicher vor Augen führen und bestätigen als der jüngste Facebook-Skandal. Er dokumentiert die disruptiven Wirkungen von Datenflüssen und Verarbeitungsprozessen auf die Kontextintegrität: Aus dem Kontext persönlicher, freundschaftlicher und familiärer Kommunikationsbeziehungen wurden mutmasslich Personendaten abgeleitet, um in der Folge gezielt auf das Wahlverhalten einzuwirken. Im Ergebnis werden damit das *demokratische System*, aber auch der Bereich persönlicher Lebensführung erodiert. Die Problematik des Vorfalles erschöpft sich nicht in der Manipulation eines einzelnen Subjektes; vielmehr werden die Integrität des persönlichen Lebensbereiches wie des politischen Systems untergraben. Vor diesem Hintergrund hat das Volkszählungsurteil aus dem Jahr 1985 nicht bloss Rechtsgeschichte hinsichtlich einem Recht auf informationelle Selbstbestimmung geschrieben. Dem Entscheid lassen sich mit diesen Erkenntnissen weit über 2020

1037 Insofern tritt erneut die auch unter Treu und Glauben sichtbar gewordene «Spezifität» von Informationen und dem rechtlichen Umgang mit diesen zu Tage sowie die Relevanz von Vertrauen im Zusammenhang mit Informations- und Kommunikationsprozessen; vgl. zur Bedeutung von Vertrauen im Zusammenhang mit der Privatsphäre Hotter, 75 f. unter Referenz auf Luhmann.

1038 Zur Bedeutung des Vertrauens und damit auch von Treu und Glauben vorangehend zweiter Teil, V. Kapitel, B.2.

hinausgehende Richtungshinweise für die Entwicklung eines Datenschutzrechts, das seinen Schutzaufgaben gerecht zu werden vermag, gewinnen.

741 Den Abschluss dieses Kapitels zum zweiten Strukturmerkmal bildete der Blick auf die beiden Verarbeitungsgrundsätze der *Datenrichtigkeit und Datensicherheit*. Sie sind zwar konkreter resp. weniger generalklauselartiger Natur. Gleichwohl gehören sie zu den grossen gemeinsamen Verarbeitungsgrundsätzen und weisen entsprechend breite wie facettenreiche Inhalte auf. Zudem gilt auch ihre Verletzung als begründend für eine Persönlichkeitsverletzung im privaten Bereich.[1039]

742 Der exakte Regelungsinhalt, der unter dem Titel des *Richtigkeitsgebotes* eingefangen wird, ist umstritten. Die hier vertretene Ansicht schliesst sich einer Meinung an, wonach absolute Richtigkeit im Sinne einer Nullfehlertoleranz unter dem Grundsatz der Datenrichtigkeit nicht verlangt werden kann. Eine erfolgreiche Berufung auf eine rein subjektiv verstandene Prüfungspflicht («Vergewissern») sowie ergriffene «angemessene Massnahmen» soll indes nicht beliebig zugelassen werden: Als im Sinne des Grundsatzes nicht genügend zu qualifizieren sind Massnahmen, die zwar vielleicht als weit- sowie tiefgreifend und damit gewissermassen in dieser Richtung als «angemessen» beurteilt werden könnten, die indes nicht ergebnisorientiert ein um einen Fehlerquotienten im Vorfeld definiertes statistisches Mindestmass an Richtigkeit erreichen. Ebenso wenig reicht die «Vergewisserung», wenn im Anschluss an die Feststellung der ungenügenden Richtigkeit, die am Zweck zu messen ist, nicht die «angemessenen Massnahmen» ergriffen werden, die das «angemessene Richtigkeitsniveau» bewerkstelligen. Der ergänzende Berichtigungsanspruch des Datensubjektes ist Konsequenz des subjektivrechtlich angeknüpften Datenschutzgesetzes. Zugleich wurde eine systemische Dimension datenschutzrechtlicher Herausforderungen im Rahmen der Erörterungen zum Gebot der Datenrichtigkeit sichtbar gemacht. Einschlägig war insofern die Praxis des «Credit Reporting» mit seinen Fehlerquoten: *Prima vista* scheinen weder die Kreditauskunfteien noch die Kreditinstitute ein Interesse zu haben, datenschutzkonform zu handeln, zumal sich diese vielmehr durch falsche Score-Werte wirtschaftlich alimentieren und es einzig und allein die Betroffenen sind, die durch falsche Score-Werte und damit nachteilige Konditionen belastet werden. An diesem Defizit setzen die USA mit ihrem *Fair Credit Reporting Act* an, einem der sektorspezifischen Erlasse für den privaten Bereich. Er verlangt ein akkurates und faires Kreditauskunftswesen, wobei der Erlass dies nicht primär zum Schutz des Individuums fordert. Vielmehr führt der Act zu Beginn aus, dass der *Bankensektor*, um *effizient* zu sein, auf das *Vertrauen der Allgemeinheit* angewiesen ist; unfaire und inakkurate Kreditauskunftspraktiken

1039 Zur Einbettung der allgemeinen Verarbeitungsgrundsätze in das Regime des datenschutzrechtlichen Persönlichkeitsschutzes im privaten Bereich zweiter Teil, VI. Kapitel, A.–C.

untergraben dieses Vertrauen und im Ergebnis die *Effizienz des Bereichs* selbst. Für die Schweiz wurde unter Berücksichtigung dieser systemischen Schutzdimension – spezifisch in Bezug auf die Vorgaben zur Datenrichtigkeit – eine Auslegeordnung präsentiert, wonach die Richtigkeit von Personendaten initial und rollend sicherzustellen ist. Als angemessene Massnahmen insofern können nur solche gelten, welche – in Anlehnung an die Ausführungen des Bundesgerichts im Google-Street-View-Entscheid – die Richtigkeit unter Berücksichtigung eines Fehlertoleranzquotienten sicherstellen. Eine Berufung auf das Ergreifen von «angemessenen» Massnahmen, die indes nicht dazu führen, dass das geforderte Richtigkeitsniveau erreicht wird, hält vor dem datenschutzgesetzlichen Richtigkeitsgebot nicht stand. Ein Verstoss gegen die Vorgaben ist insofern immerhin theoretisch mit Zurückhaltung rechtfertigbar. Abrundend ist für die Pflichten zur Datenrichtigkeit zu resümieren, dass flankierende Instrumente ausgebaut und konkretisiert werden, wobei ein risikobasierter Ansatz wirksam wird.

743 Zum Grundsatz der *Datensicherheit* wurde festgehalten, dass auch insofern keine «absolute» Sicherheit gefordert werden kann. Zudem sind die zur Gewährleistung der Datensicherheit zu ergreifenden Massnahmen heterogen sowie namentlich unter Berücksichtigung der mit den Personendatenverarbeitungsprozessen einhergehenden Risiken relativ. In diesem Sinne gibt es «no such thing as data security». Darüber hinaus wurde beschrieben, inwiefern die Instrumente und Massnahmen, die den Aspekt der Datensicherheit bewerkstelligen sollen, stark ausgebaut wurden und Ausdifferenzierung erfahren haben. Ein bedeutsames Element bei der Gestaltung der Vorgaben im Rahmen der Datensicherheit ist die *zeitliche Dimension*, indem die Datensicherheit durch Massnahmen im Vorfeld, rollend, aber auch im Falle von Datensicherheitsvorfällen zu garantieren ist. Vorgaben zur Datensicherheit finden sich nicht nur im DSG, sondern auch in der DSGVO. Im Zuge der Totalrevision leisten mehrere Instrumente einen Beitrag, um die Datensicherheit zu effektuieren. Zu nennen sind namentlich die Datenschutz-Folgenabschätzung sowie die Notifikationspflichten bei Datensicherheitsvorfällen, aber auch «privacy by design» sowie die Dokumentationspflichten. Für Personendatenverarbeitungen, die durch informationstechnologische Anwendungen unterstützt werden, haben – analog zum homöopathischen Ansatz, «Gleiches mit Gleichem zu behandeln» – technikbasierte Lösungen spezifische Bedeutung für die Gewährleistung der Datensicherheit.

744 Sowohl im Rahmen des Grundsatzes der Datensicherheit als auch in demjenigen der Datenrichtigkeit wurde aufgezeigt, dass die jüngsten Revisionswellen darauf abzielen, die allgemeinen Verarbeitungsgrundsätze nicht mehr bloss in abstrakter Weise vorzuschreiben. Vielmehr sehen sie *konkrete Umsetzungsinstrumente* vor, um die allgemeinen Verarbeitungsgrundsätze faktisch griffig werden zu lassen. Damit wurde ein Transformationsprozess nachgezeichnet: Die datenschutzrecht-

liche Fixierung auf einen defensiv gedachten Subjektschutz wird aufgeweicht und ergänzt, teilweise sogar verdrängt durch ein Konzept, wonach der Datenschutz zur «Governance»-Aufgabe und Teil eines Risikomanagements wird. Die Verantwortlichen werden frühzeitig und nachhaltig in die Pflicht genommen, angemessene Massnahmen – auch technischer und organisatorischer Natur – zur Gewährleistung der Grundsätze zu ergreifen. Die Angemessenheit dieser Massnahmen orientiert sich neu konsequent an einem risikobasierten Ansatz, womit der individualrechtliche Ansatz, der sogleich vertieft wird, ergänzt wird.

745 Durch eine Analyse der *generalklauselartigen gemeinsamen Verarbeitungsgrundsätze des DSG* zieht sich wie ein roter Faden die Erkenntnis, dass die Einschlägigkeit differenzierter Kontexte und Bereiche für und im bereits geltenden Datenschutzrecht resp. DSG anerkannt wird. Dies ist im Lichte des Eingangstitels, wonach das Datenschutzgesetz die individuellen Rechte des Einzelnen schützt, erstaunlich. Die Kontextrelevanz mag zudem auf den ersten Blick paradox erscheinen, befasst man sich doch mit den gemeinsamen Verarbeitungsgrundsätzen eines «Querschnittsgesetzes». Anknüpfend an das erste Strukturmerkmal, den Dualismus (mit seiner Zweiteilung des Regelungsregimes für den öffentlichen und den privaten Bereich), wurden im Rahmen der «gemeinsamen generalklauselartigen Verarbeitungsgrundsätze» gleichwohl an mehreren Stellen *Differenzierungen* nachgezeichnet, welche sich an der gröbsten Form bereichsspezifischer Differenzierung, am *Dualismus* zwischen staatlichem und gesellschaftlichem Bereich orientieren (z. B. unterschiedliche Transparenzvorgaben unter noch geltendem DSG für den öffentlichen und den privaten Bereich). Zugleich wurden anhand der allgemeinen Verarbeitungsgrundsätze Nuancierungen beschrieben, die weitergehende Differenzierungen eröffnen und gewissermassen die Einschlägigkeit pluraler Verarbeitungszusammenhänge und Kontexte sichtbar machen (so namentlich das Rechtmässigkeitsprinzip sowie der Zweckbindungsgrundsatz).[1040] Umgekehrt wurden Mechanismen nachgewiesen, die eine Annäherung im Schutzniveau der Datenschutznormierung für den privaten und den öffentlichen Bereich vorsehen – so der Import des Verhältnismässigkeitsprinzips im öffentlich-rechtlichen Sinne in den Bereich der Personendatenverarbeitung durch Private im DSG, aber auch der Monismus der DSGVO.

746 Die Bedeutung *pluraler Verarbeitungskontexte* für die Datenschutzgesetzgebung – wie sie anhand des allgemeinen Verarbeitungsgrundsatzes der Zweckbindung besonders gut sichtbar wird – sowie die Relevanz des Schutzes pluraler Bereiche ist damit im schweizerischen Datenschutzrecht selbst in den gemeinsamen, allgemeinen Verarbeitungsgrundsätzen angelegt. Dem Zweckbindungsgrundsatz kommt sowohl *de lege lata* mit seinem individualrechtlichen Rahmen als auch

1040 Zum Ansatz der kontextuellen Relevanz der privacy richtungsweisend die Arbeiten von Nissenbaum.

mit Blick auf die Rekonzeptionalisierung eine entscheidende Rolle zu.[1041] Richtungsweisend für die Erkenntnis, wonach der Zweck der Datenschutzregulierung ebenso im Schutz von gesellschaftlichen Bereichen, Institutionen, Kontexten oder Systemen liegt, waren die Ausführungen des Bundesverfassungsgerichts, insb. zum Zweckbindungsgrundsatz. Die kontextuelle Schutzdimension datenschutzrechtlicher Regulierungen wurde folglich – auch aufgrund der Selbstverständlichkeit, mit der das DSG in einer dualistischen Struktur und in einer individualrechtlichen, persönlichkeitsrechtlichen Anknüpfung verankert ist – in ihrer theoretischen und konzeptionellen Tragweite bislang ungenügend adressiert. Der bis heute prägenden *persönlichkeitsrechtlichen Anknüpfung des DSG für den privaten Bereich* als drittem Strukturmerkmal widmet sich das anschliessende VI. Kapitel dieses zweiten Teils. Es folgt eine vertiefte Beschäftigung mit der Funktionsweise der datenschutzgesetzlichen Vorgaben für den privaten Sektor, womit die subjektiv-, abwehr- und deliktsrechtlichen Ingredienzen genauer umrissen werden.

1041 Die Bedeutung des Verarbeitungszweckes wird für die Schweiz insb. thematisiert von Cichocki, Jusletter IT vom 21. Mai 2015, N 23 ff.

VI. Kapitel: Drittes Strukturmerkmal – Persönlichkeitsschutz

«Nicht die Struktur des Persönlichkeitsrechts bestimmt die Aufgaben des Datenschutzrechts, sondern die Struktur der Gesellschaft.»
– sinngemäss nach Spiros Simitis[1042]

A. Zum Einstieg

747 Der Schutz des Einzelnen vor *Eingriffen* durch Dritte erfolgt im Privatrecht klassischerweise über das *Deliktsrecht*.[1043] Es geht darum, «die Interessen des Geschädigten am Erhalt seiner Rechtsgüter gegen die Handlungsfreiheit des Schädigers abzuwägen».[1044] Indem das DSG an den Persönlichkeitsschutz und damit an die widerrechtliche Persönlichkeitsverletzung anknüpft, ist das *datenschutzgesetzliche Regime in erster Linie dem zivilrechtlichen Deliktsrecht* zugeordnet.

748 An dieser Stelle wird der Fokus auf das Datenschutzgesetz im privaten Bereich verengt. Der «Zweck» des Datenschutzgesetzes ist gemäss Art. 1 DSG resp. Art. 1 nDSG – neben dem Schutz der Grundrechte – der *Schutz der Persönlichkeit*. Die entsprechende Anknüpfung wurde im Rahmen der erstmaligen Verabschiedung des DSG vorgenommen. Insofern wurde vertreten, dass *Art. 28 ff. ZGB* für die Bewältigung der Herausforderungen gerade im Zusammenhang mit der technologisch unterstützten Personendatenverarbeitung datenschutzrechtlich nicht mehr genüge.[1045] Nach langem Ringen setzte sich die Überzeugung durch, wonach sich eine allgemeine Datenschutzgesetzgebung ebenso auf den privaten Bereich erstrecken müsse.[1046] Damit präsentiert sich die Datenschutzgesetzgebung für den privatrechtlichen Bereich – auch nach Totalrevision, trotz der damit einhergehenden Integration eines Compliance-Ansatzes – als *Konkretisierung von Art. 28 ff. ZGB*.[1047] Die nachfolgenden Ausführungen widmen sich der Regelungsmechanik im Detail. Damit wird eine *akkurate Charakterisierung* des Regelungsregimes möglich werden: Das DSG implementiert für den privaten Bereich – so die Schlussfolgerung – in erster Linie einen *Integritätsschutz und gerade kein sog. Recht auf informationelle Selbstbestimmung*.

1042 Insofern Simitis im Interview, <https://www.datenschutzzentrum.de/artikel/940-Interview-mit-Prof.-Dr.-Dr.h.c.-Spiros-Simitis.html> (zuletzt besucht am 30. April 2021).
1043 Ohly, 86.
1044 Ders., a. a. O.
1045 BBl 1988 II 414 ff., 441; Danioth, AB 88.032, 126: «[…] der Rechtsschutz gilt der Persönlichkeit und der Menschenwürde bei der Bearbeitung und Verwendung von Daten über eine Person»; Schweizer, 45; dazu, dass mit der Anknüpfung der privacy resp. des Datenschutzes in der Menschenwürde die Anlehnung an die Grundrechte gemacht wird, Birnhack, CLSR 2008, 508 ff., 509.
1046 Hierzu vertiefend zweiter Teil, IV. Kapitel.
1047 Vgl. neben den Gesetzgebungsmaterialien auch BGE 138 II 364, Regeste und E 8.

749 Die *persönlichkeitsrechtliche Basierung des Datenschutzgesetzes für den privaten Bereich* wird keineswegs bloss im Zweckartikel statuiert, vgl. Art. 1 DSG und Art. 1 nDSG. Vielmehr orientieren sich Art. 12 f. DSG resp. Art. 30 f. nDSG weitgehend konsequent an der Regelungsstruktur von Art. 28 ZGB.[1048] Die persönlichkeitsrechtliche Anknüpfung des DSG für den privaten Bereich schlägt sich logisch folgend zudem im Instrumentarium des Rechtsschutzes nieder, zum einen im Rahmen der Gewährleistung von Betroffenenrechten der Datensubjekte, zum anderen durch die zivilrechtlichen Klagebehelfe der Betroffenen, Art. 15 und Art. 25 DSG resp. Art. 32 nDSG und Art. 25 nDSG.

750 Das DSG ist in seiner Version vor der Totalrevision materiellrechtlich wie prozedural betrachtet für den privaten Bereich konsequent dem Schutz der *Person und Persönlichkeit verpflichtet*. An ebendieser Grundlegung sowie der reflexiven Konzeptionierung der allgemeinen Datenschutzgesetzgebung für den privaten Bereich wird im Zuge der Totalrevision des DSG weitgehend festgehalten, vgl. Art. 1 nDSG und Art. 30 ff. i. V. m. Art. 6 nDSG. Einschneidende Neuerungen finden sich für den privaten Bereich allerdings im Ausbau der Durchsetzungsinstrumente, sowohl was die Kompetenzen des EDÖB als auch was die strafrechtlichen Sanktionen anbelangt. Zudem wird die persönlichkeitsrechtliche Konzeption zwar nicht aufgegeben, doch aber – wie bereits gezeigt – markant ergänzt. Die entsprechenden Entwicklungstrends (Integration eines Compliance-Ansatzes sowie risikobasierten Ansatzes sowie von Instrumenten zur faktischen Einhaltung der Vorgaben) sind massgeblich von der DSGVO angestossen.[1049]

751 Gleichwohl ist – und bleibt – das DSG für den Bereich der Verarbeitung durch Private im *zivilrechtlichen Persönlichkeitsschutz* verwurzelt, Art. 1 i. V. m. Art. 12 i. V. m. Art. 4 ff. DSG resp. Art. 1 i. V. m. Art. 30 f. i. V. m. Art. 6 nDSG. Nachfolgend werden der Regelungsinhalt und die Regelungsstruktur von Art. 12 f. DSG (i. V. m. Art. 4 ff. DSG) resp. Art. 30 f. nDSG (i. V. m. Art. 6 und 8 nDSG) sowie die Details der persönlichkeitsrechtlichen Dogmatik im Rahmen des DSG als dessen *drittes Strukturmerkmal* dargestellt.

752 Vorausschickend in Erinnerung zu rufen sind die Erkenntnisse aus den vorangehenden Teilen, namentlich die beiden bereits beschriebenen Strukturmerkmale des DSG. Sie vervollständigen den Betrachtungsrahmen: Die Analyse im Rahmen

1048 Dazu, dass Art. 28 ZGB und der zivilrechtliche Persönlichkeitsschutz in zahlreichen Spezialgesetzen, auch dem DSG, «herumgeistert», Riemer, sic! 1999, 103 ff., 103; zum allgemeinen Persönlichkeitsrecht Ehmann, in: Stathopoulos/Beys/Philippos/Karakostas (Hrsg.), 113 ff.; eine prägnante Übersicht über die datenschutzgesetzliche Regelung der Verletzungstatbestände im Privatbereich und die Rechtfertigungsgründe findet sich bei Steinauer, in: Schweizer (Hrsg.), 43 ff. und 53, wo er festhält, dass es sich bei den DSG-Normen einzig um eine konkretisierende Wiederholung von Art. 28 DSG handle.

1049 Eine gegenüberstellende Betrachtung des totalrevidierten DSG und der DSGVO legt jüngst auch Baeriswyl, SZW 2021, 8 ff. vor.

der *allgemeinen, «gemeinsamen» und über weite Strecken generalklauselartigen Verarbeitungsgrundsätze* sowie der an diese angekoppelten Neuerungen hat gezeigt, dass in ihnen ergänzende Perspektiven und Dimensionen gegenüber einem defensivrechtlich gedachten Datenschutzrecht, das die Struktur von Art. 28 ZGB rezipiert, angelegt sind. Auch im Rahmen der Beschreibung der *dualen Struktur des DSG* wurde die Anerkennung der Einschlägigkeit der kontextuellen Dimension thematisiert. Herausgearbeitet wurde darüber hinaus, dass mit den jüngsten datenschutzrechtlichen Neuerungen die verantwortlichen personendatenverarbeitenden Stellen primär und nachhaltig in die Pflicht genommen werden, die datenschutzrechtlichen Vorgaben einzuhalten.

753 Damit zeigte sich im Laufe der bisherigen Studie, dass eine subjektivrechtliche, individualrechtliche und deliktsrechtliche Konzeption – wie sie in einer isolierten Betrachtung von Art. 1 (n)DSG und Art. 12 f. i. V. m. Art. 4 DSG resp. Art. 30 f. i. V. m. Art. 6 nDSG durchaus konsequent umgesetzt wird – nicht rein verwirklicht ist. Wird das Herzstück der datenschutzrechtlichen Bestimmungen für den privaten Bereich einbettend analysiert, zeigt sich, dass eine isolierte Betrachtung der datenschutzgesetzlichen Vorgaben als Abbild des zivilrechtlichen Persönlichkeitsschutzes nicht ganz akkurat charakterisiert. Isoliert betrachtet allerdings sind die Bestimmungen des DSG für den privaten Bereich in konsequenter Weise ein Abbild der Konzeption gemäss Art. 28 ZGB. Der *Schutzzweck* des DSG ist demnach für den privaten Bereich ausdrücklich die Persönlichkeit des Datensubjektes, vgl. auch Art. 1 (n)DSG und Art. 12 f. DSG resp. Art. 30 f. nDSG. Eine damit *subjektivrechtliche und – für den privaten Bereich – persönlichkeitsrechtliche Fundierung* hält sich somit bis heute im schweizerischen DSG.[1050] Diese individualrechtliche Anknüpfung datenschutzgesetzlicher Vorgaben für den privaten Bereich gilt gewissermassen als «naturgegeben»: Denn was anderes als das Individuum, der Mensch als Subjekt und damit die Person resp. Persönlichkeit, sollte geschützt werden in Anbetracht von Informationstechnologien, deren Macht in der potentiellen Degradierung des Menschen zum Objekt, zu einer Nummer, beschrieben wird?[1051]

754 In diesem Zusammenhang ist die in kaum einem Beitrag zur Datenschutzgesetzgebung fehlende Kritik an der unglücklichen und missverständlichen Titulierung der Erlasse als «Datenschutz(-gesetz)» zu erwähnen: Mit dem Datenschutzrecht

1050 So unlängst eindrücklich auch die verschiedenen Beiträge im Rahmen der 12. Tagung zum Datenschutz – jüngste Entwicklungen am 5. Februar 2019.

1051 Menschen sollen «nicht einfach Informationsobjekte sein», vgl. Nabholz, 3; vgl. auch Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 32, wonach der Einzelne nicht rechtloses Objekt von Informationsprozessen sein, stattdessen die Kenntnisse und das Bild, welches andere von ihm haben, selbst bestimmen oder beeinflussen können soll; m. w. H. auch Pohle, 18.

resp. den Datenschutzgesetzen würden *nicht* Daten, sondern *Personen*, Menschen, Bürgerinnen und Bürger vor Datenverarbeitungen geschützt.[1052] Denn:

> «Umstrittene Informationsbearbeitungen im öffentlichen wie im privaten Bereich haben uns für die Belange des Persönlichkeitsschutzes unterdessen sensibilisiert, und Datenschutz ist ja nichts anderes als Persönlichkeitsschutz.»[1053]

755 Gleichwohl dokumentiert sich in der Bezeichnung «Datenschutzgesetz» und den hierzu gemachten Ausführungen, dass die datenschutzrechtliche Strukturierung und Herangehensweise in einem *Subjekt-Objekt-Denken* verwurzelt ist. Nicht abgebildet wird mit der Titulierung eine Konzeptionierung, wonach es um die *Gestaltung und Normierung von Datenflüssen* geht. Die Sinnhaftigkeit und Notwendigkeit einer solchen Betrachtungsweise wurde im Laufe dieser Schrift bis hierher an mehreren Stellen dargelegt. Die Neuerungswellen haben eine entsprechende Herangehensweise eindrücklich implementiert. Mit einer Perspektive, welche Personendatenflüsse fokussiert, rückt die Frage nach der Einschlägigkeit von Verarbeitungszusammenhängen und -kontexten in den Blick. Die Analysen zu den Verarbeitungsgrundsätzen mit den neuen Instrumenten, die diese verwirklichen sollen, haben diese prozesshafte Dimension des Datenschutzes vor Augen geführt.

756 Ungeachtet dieser jüngsten Entwicklungen sowie der bis heute von Gesetzes wegen *unmissverständlichen Anknüpfung des DSG im Persönlichkeitsschutz* für den privaten Bereich bleibt die Auseinandersetzung mit dem Rechtsgebiet geprägt von *mannigfaltigen Variationen* in Bezug auf die Nomenklatur, Beschreibungen und Konkretisierungen mit Blick auf Schutzzweck, -ziel und -mechanismen resp. die Regelungsmechanik des DSG. Ebendies ist insofern bemerkenswert, als dass der Gesetzeswortlaut sowie die Kernstruktur der Regelung des DSG eindeutig zu sein scheinen. Es geht im Datenschutzrecht um den Persönlichkeitsschutz in Anlehnung an Art. 28 ZGB. Die Schaffung anderer Überbegriffe resp. Bezüge, z. B. zur Privatheit oder Privatsphäre oder informationellen Selbstbestimmung, könnte sich damit zumindest *prima vista* erübrigen.

757 Dass sich die Schweizer Lehre, Rechtsprechung und Praxis zum DSG mit weiteren Konzepten und Begrifflichkeiten unter dem Titel des Datenschutzrechts befasst, ist gleichwohl gut begründet. An dieser Stelle manifestiert sich eine typologische Herausforderung des Datenschutzes, mit der sich bis heute weltweit die verschiedensten Disziplinen konfrontiert sehen. Es geht um die Kernherausforderung oder -problematik des Datenschutzes und seines Rechts selbst – die

1052 Vgl. Forstmoser, digma 2003, 50 ff., 51; dazu, dass Datenschutzgesetze nicht in erster Linie Daten schützen, sondern eine Degradierung der Bürgerinnen und Bürger zu Informationsobjekten verhindern sollen, Bründler, SJZ 1993, 129 ff., 133; kritisch zu den Begrifflichkeiten Simitis, Nomos-Komm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 2 und N 26.

1053 Koller, AB 88.032, 5. Juni 1991, 984.

Definierung «*des Privaten*», das seinerseits selbst dieser Tage als Schirmbegriff für datenschutzrechtliche Ziele figuriert.[1054] Bis heute gilt das «Versagen», den Dachbegriff des «Privaten» dingfest zu machen und griffig zu beschreiben, als ein Hauptproblem der Datenschutzregulierung und als eine Ursache für dessen ungenügende Wirksamkeit.[1055] In diesem Sinne bezeichnete der Sonderberichterstatter der Vereinten Nationen das «Fehlen einer verbindlichen Definition zur Privatsphäre als Haupthindernis für deren umfassenden rechtlichen Schutz».[1056]

758 Illustrativ und indikativ für die Reichhaltigkeit und Weite der Konzepte, aber auch die Orientierungslosigkeit in Bezug auf Schutzziele und -objekte des Datenschutzes auch in der Schweiz sind die im erläuternden Bericht zur Totalrevision des Datenschutzgesetzes auf rund drei Seiten aufgeführten politischen Vorstösse, die im Kontext des Datenschutzes anhängig gemacht wurden:[1057] Besser geschützt werden soll «das Grundrecht auf informationelle Selbstbestimmung»; gefordert wird ein «Eigentum der Person an ihren Daten»; zu stärken sind das «Recht auf Schutz des Privatlebens», die «Privatsphäre und persönliche Freiheit»; gefordert wird ein «Recht auf Vergessen im Internet»; vorgeschlagen wird ein «Recht auf Kontrolle über persönliche Daten» usf. In der Botschaft zur Revision des DSG mittels Totalrevision wurde die Abschreibung mehrerer entsprechender parlamentarischer Vorstösse beantragt.[1058]

759 In den datenschutzgesetzlichen Anfängen referierte die Botschaft zum DSG über das Recht auf informationelle Selbstbestimmung mit den Worten:

> «Jedermann soll, soweit die Rechtsordnung nichts anderes vorsieht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen und frei über die Aufnahme und Gestaltung seiner Informations- und Kommunikationsbeziehungen entscheiden können».[1059]

760 Insofern sind Präzisierungen angezeigt. Den Ausführungen zur Funktionsweise des DSG im privaten Bereich sei vorausgeschickt, dass das DSG selbst gewissermassen «definitionsblind» und «ohne Etikettierung» eine Regulierung implementiert, die sich konsequent an der Regelungsmechanik von Art. 28 ZGB orientiert und diesen spezifisch für den Umgang mit Personendaten konkretisiert. Ganz ohne Bezugnahme auf Begriffe wie die «Privatsphäre», «informationelle Selbstbe-

1054 Vgl. exemplarisch zur Privatheit Aebi-Müller, N 646 ff., aber auch zu den Kategorien der Privatsphäre und informationellen Selbstbestimmung, N 512 ff. und N 541 ff.

1055 In diesem Zusammenhang zum Inhalt ihres Werks die amerikanische Philosophin Nissenbaum: «It does not carve a pathway through the conceptual quagmire to claim a definition – its definition – of privacy. Nevertheless, it is a book about privacy because it explains why the huge and growing set of technical systems and technology-based practices have provoked and continue to provoke anxiety, protest, and resistance in the name of privacy», 130; zur Privatsphäre als komplexes Konzept, das stets auch wandelbar ist, Hotter, 9 ff.

1056 HRC, Special Rapporteur Right to Privacy 2016, N 9; vgl. EJPD, Erläuternder Bericht, 1 ff., 16.

1057 EJPD, Erläuternder Bericht, 1 ff., 10 ff.

1058 BBl 2017–1084, 17.059, 6941 ff., 6941.

1059 BBl 1988 II 414 ff., 418.

stimmung», «Missbrauchsgesetzgebung», den Blick von einer Definierung resp. Titulierung wegführend wies ebenso Rhinow im Rahmen der parlamentarischen Verhandlungen zur Verabschiedung eines DSG darauf hin, dass dieses

> «im privatrechtlichen Verhältnis die Mechanik des Persönlichkeitsschutzes von Art. 28 ZGB übernimmt».[1060]

761 Mittels konsequenter Referenz auf die persönlichkeitsrechtliche Anknüpfung gemäss Art. 28 ZGB des DSG für den privaten Bereich scheint man den Weg durch das «Dickicht» der unzähligen Definitionsversuche zu dem das Datenschutzrecht prägenden Dachbegriff des Privaten umgehen zu können. Eine Beschreibung könnte sich darauf beschränken, die als Persönlichkeitsverletzung umschriebenen Handlungen und das Rechtfertigungsregime zu benennen, ohne dass damit eine weitere Titulierung einhergehen müsste. Dennoch ist eine Auseinandersetzung mit Definierungs- und Charakterisierungsversuchen zumindest punktuell lohnenswert: Mit ihr lassen sich strukturierende Begrifflichkeiten für das DSG und seine Funktionsweise im privaten Bereich herausarbeiten. Eine präzise Charakterisierung des DSG mit seiner Regelungsmechanik ist ein Fortschritt für den datenschutzrechtlichen Diskurs in der Schweiz, zumal nicht zuletzt in der Allgemeinheit insofern auch Fehlannahmen zu kursieren scheinen.

762 Knüpft das DSG für den Privatsektor an das System des zivilrechtlichen Persönlichkeitsschutzes gemäss Art. 28 ZGB an, ist vorab die entscheidende Frage, wie die Verletzung der Persönlichkeit durch Personendatenverarbeitungen vom DSG umrissen wird. Rezipiert wird das Regime des DSG seinerseits mit einem beachtlichen Variantenreichtum an Begrifflichkeiten und Charakterisierungen. Ebendies sei anhand einiger kurzer Passagen illustriert.

763 Die erste Umschreibung stammt aus dem Evaluationsbericht zum DSG, wobei diese bereits im Licht der bislang generierten Erkenntnisse nicht zu überzeugen vermag. Ebenda liest man:

> «Allgemein gesprochen stellt somit die Bearbeitung von Personendaten durch private Bearbeiter eine widerrechtliche Persönlichkeitsverletzung dar, wenn nicht ein Rechtfertigungsgrund vorliegt.»[1061]

764 Ähnlich, wenn auch ohne Aussage zum Tatbestandselement der Widerrechtlichkeit, wird auch vertreten:

> «Jede Form der privaten Datenbearbeitung ist eine Persönlichkeitsverletzung.»[1062]

765 Aebi-Müller führt unter Referenz auf deutsche Quellen aus:

> «Nicht mehr der Schutz bestimmter Bereiche […] steht nunmehr im Zentrum, sondern der Gedanke, dass dem Betroffenen die Herrschaft über seine Daten und deren Verwen-

1060 Rhinow, AB 88.032, 13. März 1990, 130.
1061 Bolliger/Féraud/Epiney/Hänni, 106.
1062 VPB 68.68. Erw. 31/a.

> dung zukommen soll. Massgebend für das Vorliegen einer Verletzung ist damit der *Wille der Person*, auf dies [sic!] sich die Information bezieht. Kern des Datenschutzgesetzes ist entsprechend dieser Vorstellung ein Recht auf informationelle Selbstbestimmung. Nur der Betroffene bestimmt, welchen Wert er den auf ihn bezogenen Daten zumisst […]. Dieses *Herrschaftsrecht an den eigenen Daten* ergibt sich – obschon der Begriff der informationellen Selbstbestimmung sich im Schweizerischen DSG nicht findet – namentlich aus Art. 12 Abs. 2 Bst. b […], sowie aus Art. 12 Abs. 3 DSG (e contrario) […].»[1063]

766 Und an anderer Stelle weitergehend dieselbe Autorin:

> «Durch das Recht auf informationelle Selbstbestimmung wird die unter der Sphärentheorie begründete Gemeinsphäre vollständig aufgelöst: Es gibt keine Daten mehr, die unabhängig vom Willen des Betroffenen bearbeitet werden können.»[1064]

767 Eine Umschreibung von Rosenthal schliesslich lautet:

> «Um einer Person den Schutz der Persönlichkeit zu erleichtern, hat der Gesetzgeber mit Art. 4 Abs. 1–4 die unwiderlegbare Vermutung aufgestellt, die Persönlichkeit der betroffenen Person sei verletzt. Das ist der einzige Zweck der Bestimmung.»[1065]

768 Eine beachtliche Divergenz für ein und dasselbe Gesetz. Ebendies ist (er)klärungsbedürftig, gerade auch, weil für die zitierten Autorinnen resp. Autoren die Rechtslage in gänzlich unterschiedlicher Weise klar ist. Doch genau darin liegt das Problem.

769 Anders gewendet: Es besteht Klärungsbedarf bezüglich der Persönlichkeitsverletzung durch Personendatenverarbeitungen gemäss DSG im privaten Bereich und, allgemeiner, im Hinblick auf das Schutzobjekt resp. den Schutzzweck sowie die Schutzmechanik. Die nachfolgenden Erörterungen dienen dazu, die persönlichkeitsrechtliche Funktionsweise des schweizerischen Datenschutzgesetzes zu klären. In der Folge soll das Regime einer gesetzeskonformen und präzisen Charakterisierung zugeführt werden.

770 Hierbei wird sich zunächst zeigen, dass sich die markanten Differenzen zwischen den verschiedenen Interpretationen keineswegs auf Auslegungsdetails zurückführen lassen. Vielmehr wird die Analyse des Regimes des DSG für den privaten Bereich die Schlussfolgerung zulassen, wonach die trefflichste Beschreibung der Regelungsmechanik des DSG sich des Begriffs des *Integritätsschutzes* bedient. Er zielt darauf ab, die *elementar(st)en Erwartungen an eine faire Personendatenverarbeitung* zu gewährleisten resp. *missbräuchliche Verarbeitungshandlungen* zu verhindern. Das ist die datenschutzgesetzliche *Basiskonstruktion* für den privaten Bereich, es sei denn, es greifen spezifische Verarbeitungsvorgaben.

1063 M. w. H. Aebi-Müller, N 591 f.
1064 Dies., 611.
1065 Rosenthal, HK-DSG, Art. 4 N 77; vgl. zu den verschiedenen Schutzbegriffen wie Datenschutz, Recht auf informationelle Selbstbestimmung, Recht auf Schutz der Privatsphäre und der Persönlichkeit auch Epiney/Civitella/Zbinden, 7.

771 Grundlegend für das Verständnis der datenschutzgesetzlichen Normierung für den privaten Bereich sind ergänzend die Ausführungen zum *Dualismus* mit dem Ausgangspunkt der prinzipiellen Freiheit der Personenverarbeitung mit Schranken.[1066] Daran anknüpfend und unter Bezugnahme auf die unterschiedlichen Ausgangspunkte für den privaten und öffentlichen Bereich des Bundes wurden die allgemeinen Verarbeitungsgrundsätze dargestellt.[1067] Sie sind der Kern des materiellen Datenschutzrechts, der gleichwohl eine unterschiedliche Bedeutung infolge der unterschiedlichen Ankoppelung für den privaten resp. öffentlichen Bereich findet.

772 Die allgemeinen Verarbeitungsgrundsätze gemäss Art. 4 ff. DSG resp. Art. 6 ff. nDSG spielen eine zentrale Rolle für die *Definierung der Persönlichkeitsverletzung* im privaten Bereich, vgl. Art. 12 Abs. 2 lit. a DSG und Art. 30 Abs. 2 lit. a nDSG. Allerdings erschöpft sich darin das Regime des Datenschutzgesetzes für den privaten Bereich nicht. Vielmehr fügen die Art. 12 Abs. 2 lit. b und lit. DSG resp. Art. 30 Abs. 2 lit. b und c nDSG weitere Ingredienzen ein.

773 Die Analyse von Art. 12 Abs. 2 lit. a–c DSG wird zeigen, dass die *zweite Kammer des dualen Systems* – die Datenschutzgesetzgebung für den privaten Sektor – ein *nuanciertes Regime* darstellt. In diesem werden mehrere Kriterien – objektive, aber auch subjektive – eingesetzt, um die Persönlichkeitsverletzung qua Personendatenverarbeitung konkreter zu definieren.

774 Im Rahmen der Beschreibung dieses Regimes wird insb. auch auf Bedeutung und Funktion der *datenschutzrechtlichen Einwilligung* eingegangen werden, vgl. Art. 12 Abs. 2 lit. b, Art. 12 Abs. 3 und Art. 13 DSG, zudem auch Art. 4 Abs. 5 DSG resp. Art. 30 Abs. 2 lit. b und Art. 30 Abs. 3 nDSG, Art. 31 nDSG sowie Art. 6 Abs. 6 und Abs. 7 nDSG. Die Ausführungen rücken das noch geltende Gesetz vor seiner Totalrevision in das Zentrum. Auf eine vertiefte Darstellung der angepassten und ausgebauten Einwilligungsvorgaben, wie sie das totalrevidierte DSG insb. für spezifisch neu geregelte Konstellationen wie das Profiling vorsieht, wird verzichtet.[1068] Die Vorgaben in Bezug auf die Einwilligung wurde bewusst *nicht* unter dem Titel der allgemeinen Verarbeitungsgrundsätze erörtert, obschon vom Gesetzgeber ebenda eingeordnet. Die Erklärung für die in dieser Arbeit gewählte Systematik ist, dass Art. 4 Abs. 5 DSG resp. neu Art. 6 Abs. 6 und Abs. 7 nDSG die Einwilligung gerade *nicht* als Verarbeitungsgrundsatz resp. Legitimationstatbestand für grundsätzlich verbotene Verarbeitungshandlungen positioniert. Vielmehr umschreibt Art. 4 Abs. 5 DSG einzig die *Anforderungen für eine gültige*

1066 Zweiter Teil, IV. Kapitel.
1067 Zweiter Teil, V. Kapitel.
1068 Verwiesen wird insofern insb. auf die Dissertation von Heuberger, sodann die jüngsten Beiträge zum totalrevidierten DSG; zum Profiling mit Blick auf den Banksektor weiter Vasella, in: Emmenegger (Hrsg.), 189 ff.

Einwilligung genauer, sofern die Einwilligung rechtlich verlangt ist. Ebendies allerdings ist, wie zu zeigen sein wird, nach DSG selbst für den privaten Bereich nur ausnahmsweise der Fall.

775 Die datenschutzgesetzliche Regelung der Schweiz für den privaten Bereich weist, wie zu zeigen sein wird, *verschiedene Komponenten und Ansätze* auf. Sie sind in den Abs. 2 lit. a–c und Abs. 3 von Art. 12 DSG resp. Art. 30 Abs. 2 lit. a–c nDSG und Abs. 3 nDSG abgebildet. Stark ausgeprägt ist die Ingredienz eines *Integritätsschutzes* (Art. 12 Abs. 2 lit. a DSG, Art. 30 Abs. 2 lit. a nDSG); zurückhaltend Eingang findet der Aspekt eines *Selbstbestimmungsrechts* (Art. 12 Abs. 2 lit. b und Abs. 3 DSG, Art. 30 Abs. 2 lit. b und Abs. 3 nDSG), wohingegen sich in prägnanter Weise weiterhin die traditionsreiche *Sphärentheorie* abgebildet findet (Art. 12 Abs. 2 lit. c und Abs. 3 DSG, Art. 30 Abs. 2 lit. c und Abs. 3 nDSG). Obschon das DSG für den privaten Bereich die Schwächen der Sphärentheorie bewältigen wollte,[1069] findet sich weiterhin die an einem sphärentheoretischen Konzept ausgerichtete Zweiteilung zwischen öffentlich versus privat. Damit liesse sich sagen, die kursierenden Umschreibungen hätten alle eine gewisse Berechtigung. Es geht indes fehl, diese in pauschaler und generalisierter Weise als Beschreibung für das datenschutzgesetzliche Regime des privaten Bereichs an sich resp. im Gesamten einzusetzen. Suggeriert werden dann ein Rechtsbestand und ein Regelungsregime, die so (pauschal) vom DSG nicht gewährleistet werden. Zugleich wird damit nicht mehr ersichtlich, wie nuanciert und gleichzeitig konsequent das DSG für den privaten Bereich am zivilrechtlichen Persönlichkeitsschutz ausgerichtet ist. Hierzu sogleich mehr.

B. Regelungsinhalt von Art. 12 f. DSG resp. Art. 30 f. nDSG

776 Der Grundsatz der Bearbeitungsfreiheit ist Ausgangspunkt des Schweizer Systems für den privaten Bereich. Hierbei markieren *qualifizierte Verarbeitungshandlungen* die Schranken der prinzipiellen Verarbeitungsfreiheit, indem diese zugleich die Persönlichkeitsverletzung begründen, vgl. Art. 12 Abs. 1 und Abs. 2 DSG resp. Art. 30 Abs. 1 und Abs. 3 nDSG.

777 Nach schweizerischem DSG ist nicht jede Personendatenverarbeitung prinzipiell verboten; nicht jede Personendatenverarbeitung bedarf eines Erlaubnistatbestandes. Das DSG taxiert auch nach Totalrevision nur die *qualifizierte Personendatenverarbeitung als Persönlichkeitsverletzung, deren Widerrechtlichkeit bei Vorliegen eines Rechtfertigungsgrundes entfallen kann, vgl. Art. 12 f. DSG und Art. 30 f. nDSG*. Umgekehrt und mit anderen Worten bedeutet dies zugleich, dass

1069 Vgl. zu den Mängeln des bisherigen Rechts und der Abwicklung über Art. 28 ff. ZGB Schweizer, 40 ff.

ein weites Feld an Personendatenverarbeitungen *unterhalb der Schwelle der Persönlichkeitsverletzung* und damit innerhalb des freien Verarbeitungsbereiches liegt.

778 Stattdessen geht die DSGVO prinzipiell vom Verarbeitungsverbot sowohl für private als auch für öffentliche Stellen aus. Grundsätzlich bedarf jeder Umgang mit Personendaten eines Erlaubnistatbestandes, vgl. Art. 6 DSGVO. Die DSGVO sieht damit ein gänzlich anderes Regime vor als das DSG mit seinem Dualismus und seiner prinzipiellen Verarbeitungsfreiheit mit Schranken für den privaten Bereich, welche die Struktur des zivilrechtlichen Persönlichkeitsschutzes rezipiert.

779 Gleichwohl sind in der Schweiz mit der Totalrevision neue Instrumente unabhängig von ihrer Einbindung in das persönlichkeitsrechtliche Regime zu beachten. Das totalrevidierte DSG ergänzt den persönlichkeitsrechtlichen Ansatz markant über mehrere neue Elemente, die stets zu beachten und implementieren sind – ungeachtet der Frage, ob eine Personendatenverarbeitung die Schwelle der zivilrechtlichen Persönlichkeitsverletzung über- oder unterschreitet.

780 Der Fokus richtet sich sogleich indes auf *die Kernbestimmungen der datenschutzrechtlichen Persönlichkeitsverletzung* resp. ihre Rechtfertigung und damit die besonderen Bestimmungen zur Datenbearbeitung durch private Personen, vgl. Art. 12 ff. DSG und Art. 30 ff. nDSG. Mit der Totalrevision bleibt die Koppelung der datenschutzgesetzlichen Anknüpfung an den zivilrechtlichen Persönlichkeitsschutz und die Normierung seiner *sedes materiae* weitgehend erhalten. Die besonderen Bestimmungen des DSG für den privaten Bereich, die explizit am Persönlichkeitsschutz anknüpfen, finden nur marginale Änderungen. Ebendies darf aber nicht darüber hinwegtäuschen, dass die Entwicklungen ausserhalb dieser Bestimmungen die persönlichkeitsrechtliche Anknüpfung des DSG neu einbetten.

781 Das Regime gemäss Art. 12 ff. DSG resp. Art. 30 ff. nDSG präsentiert sich weitgehend als Abbild der Struktur von Art. 28 ZGB. Die nachfolgenden Ausführungen widmen sich vorab den Personendatenverarbeitungen, die unterhalb der Schwelle der Persönlichkeitsverletzung liegen. Anschliessend werden die qualifizierten Verarbeitungshandlungen beleuchtet, die eine Persönlichkeitsverletzung verursachen. Es folgt die Betrachtung der Rechtfertigungsgründe sowie des Rechtsschutzes, insb. des zivilrechtlichen Rechtsschutzes gemäss DSG.

1. Nicht persönlichkeitsverletzende Personendatenverarbeitungen

782 Nach DSG sind es im Wesentlichen *zwei Konstellationen*, gemäss denen Personendatenverarbeitungen prinzipiell *nicht als persönlichkeitsverletzend* gelten. Sie sind in Art. 12 Abs. 2 und Abs. 3 DSG resp. Art. 30 Abs. 2 und Abs. 3 nDSG niedergelegt. Abs. 2 umschreibt, wann resp. in welchen Fällen Persönlichkeitsverlet-

zungen qua Personendatenverarbeitung vorliegen – die Konstellation wird als positive Seite von Art. 12 DSG resp. 30 nDSG bezeichnet.[1070] Der negativen Seite widmet sich Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG.

783 *Erstens* begründen die Personendatenverarbeitungen keine Persönlichkeitsverletzung, welche in Einklang mit den allgemeinen Verarbeitungsgrundsätzen vorgenommen werden, Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG.

784 *Zweitens* wird dem Grundsatz nach keine Persönlichkeitsverletzung angenommen bei Personendatenverarbeitungen, die sich auf allgemein zugänglich gemachte Personendaten beziehen, sofern kein ausdrücklicher Widerspruch anhängig gemacht wurde, Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG.

785 Beiden Konstellationen ist gemein, dass die Verarbeitungshandlungen *nicht als hinreichend invasiv* taxiert werden, um die Schwere einer Persönlichkeitsverletzung zu erlangen. In Anlehnung an die in Art. 28 ZGB angelegte Struktur und Dogmatik fehlt es am *qualifizierenden Merkmal* der «hinreichenden Schwere» einer Handlung, eines Verhaltens resp. eines Eingriffs, die diese zur Persönlichkeitsverletzung machen würde.

1.1. Verarbeitungsgrundsätze achtende Verarbeitungshandlungen

786 Die *erste Gruppe von Personendatenverarbeitungen*, die nicht als persönlichkeitsverletzend gilt, umfasst grob diejenigen Verarbeitungshandlungen, welche die allgemeinen Bearbeitungsgrundsätze einhalten, vgl. Art. 12 Abs. 1 und Abs. 2 lit. a *e contrario* i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 1 und Abs. 2 lit. a *e contrario* i. V. m. Art. 6 und Art. 8 nDSG. Kursierende Lehrmeinungen, wonach jede Personendatenverarbeitung eine Persönlichkeitsverletzung begründet oder wonach die Einwilligung des Datensubjektes eine Voraussetzung für eine rechtmässige Datenverarbeitung ist, finden damit im DSG weder vor noch nach seiner Totalrevision eine rechtliche Grundlage. Von Gesetzes wegen greift im privaten Bereich die prinzipielle Freiheit der Datenbearbeitung. Sie wird beschränkt durch Leitplanken in Gestalt der allgemeinen Verarbeitungsgrundsätze.

787 In die Struktur von Art. 28 f. ZGB übersetzt bedeutet dies: Erst *qualifizierte Verarbeitungshandlungen* gelten von Gesetzes wegen als persönlichkeitsverletzend. An erster Stelle sind die Verarbeitungshandlungen, welche die allgemeinen Verarbeitungsgrundsätze missachten, persönlichkeitsverletzend, vgl. Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG. Die allgemeinen Verarbeitungsgrundsätze, denen

1070 Vgl. Rampini, BSK-DSG, Art. 12 N 4.

sich das V. Kapitel widmete, markieren im privaten Bereich den *Grenzverlauf zwischen zu duldender resp. persönlichkeitsverletzender Verarbeitung*.

788 Das datenschutzgesetzliche Regime lässt sich für diese Konstellation wie folgt charakterisieren: Die Vorgaben, die mit den allgemeinen Verarbeitungsgrundsätzen verbürgt werden, gewährleisten mit der Ankoppelung an den prinzipiellen Grundsatz der Verarbeitungsfreiheit im privaten Bereich eine *Garantie der fairen, integren und nachvollziehbaren Datenverarbeitung*. Ebendies steht, ohne die grosse Debatte rund um die Wirkung der Grundrechte im Privatrecht zu eröffnen, durchaus mit der verfassungsrechtlichen Idee gemäss dem Wortlaut von Art. 13 Abs. 2 BV und einem Konzept der Verhinderung von Missbrauch in Einklang.[1071]

789 Der *Integritätsschutz* gemäss Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG wird zwar durch die neu eingeführten Instrumente mit der Totalrevision angereichert um eine organisatorisch-prozesshafte Dimension. Es sind die Verarbeitenden, die zu gewährleisten haben, dass die Personendatenverarbeitungen unter Einhaltung der Verarbeitungsgrundsätze erfolgen. Sie sichern für den Bereich der Personendatenverarbeitung die *Fairness, Integrität resp. Abwesenheit eines Missbrauchs* ab. Die Verarbeitenden sind dazu *proaktiv* verantwortlich, womit das *defensivrechtliche Konzept*, wie es im zivilrechtlichen Persönlichkeitsschutz angelegt ist, ergänzt wird. Die Totalrevision wählt mit der Schaffung neuer Instrumente eine Strategie, die dem materiellrechtlichen Kernbestand des Datenschutzrechts mit seinen Verarbeitungsgrundsätzen Nachachtung verleihen soll. Gleichwohl hängt auch künftig die Effizienz dieses Regimes für den privaten Bereich, das *kein grundsätzliches Verbot* mit Erlaubnistatbeständen vorsieht, wie erläutert nicht unwesentlich davon ab, wie eindeutig die *Verarbeitungsgrundsätze die Demarkationslinien* zwischen persönlichkeitsverletzender und nicht persönlichkeitsverletzender Verarbeitungshandlung fixieren.

790 Die generalklauselartigen Verarbeitungsvorgaben erlangten allerdings in ihrer noch geltenden Fassung nur teilweise strukturierende und konkretisierende Griffigkeit. Das Datenschutzrecht hat bei Lichte betrachtet erst mit der Totalrevision auch in der Schweiz grösseres Interesse im Schrifttum auf sich gezogen. Durch die beschränkten Kompetenzen des EDÖB nach geltendem DSG und der eher rudimentären Lehre konnte für die generalklauselartigen Verarbeitungsgrundsätze

1071 Zu letzterer grundlegend und überzeugend Belser, in: Epiney/Fasnacht/Blaser (Hrsg.), deren Analyse zu einer Qualifikation als Missbrauchsregime führt, 19 ff., 34 ff.; in diese Richtung auch Gächter/Egli, Jusletter vom 6. September 2010, N 8 ff.; dagegen taxiert die h. L., oft ohne Begründung, das Schweizer Regime als Recht der informationellen Selbstbestimmung, vgl. neben Aebi-Müller insb. Schweizer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 2 N 2; Maurer-Lambrou/Kunz, BSK-DSG, Art. 1 N 5 und N 18; vgl. m. w. H. Fasnacht, N 117 ff.

nur punktuell eine stabilisierte Lehre und Rechtsprechung entstehen, vgl. Art. 1 Abs. 3 ZGB, die ebenso für das DSG im privaten Bereich anwendbar ist. Die Grenzen zur datenschutzrechtlichen Persönlichkeitsverletzung, wie sie durch die Verarbeitungsgrundsätze resp. ihre Verletzung markiert werden, bleiben damit bis heute vage.

791 Indem nun am Anfang von Datenverarbeitungsprozessen infolge der prinzipiellen Freiheit der Datenbearbeitung in der Regel die bearbeitenden Stellen stehen, wird ihnen, soweit die strukturierende Lehre und Rechtsprechung fehlt, die Interpretationshoheit über die allgemeinen Verarbeitungsgrundsätze zugewiesen. Sie sind indes aufgrund ihrer eigenen Interessen nicht die geeigneten Personen zur «treuhänderischen» Interpretation der Bearbeitungsgrundsätze. Von ihnen zu verlangen, ihre Handlungen auf die Einhaltung rechtlicher Vorgaben hin zu überprüfen, deren Interpretation selbst den Rechtsexpertinnen und -experten schwerfällt, überzeugt nicht, zumal sich teilweise anspruchsvolle Auslegungsfragen stellen. An dieser Stelle akzentuiert sich die Kritik am generalklauselartigen Regelungsregime für den privaten Bereich, der mit einer bislang schwachen Rechtsdurchsetzung und Durchdringung in der Lehre dazu führte, dass die datenschutzgesetzlichen Vorgaben im privaten Bereich lange im Wesentlichen nur auf dem Papier galten.[1072]

792 Was die Auslegung der allgemeinen Verarbeitungsgrundsätze gemäss Art. 4 DSG resp. Art. 6 nDSG anbelangt, vereinfacht ein gewisser Wertungswiderspruch die Aufgabe nicht: Gemäss Art. 1 (n)DSG ist Zweck des Gesetzes, die Persönlichkeit zu schützen. Eine hieraus abgeleitete Auslegungsregel, wonach das DSG und dessen Generalklauseln stets zugunsten des Datensubjektes und zulasten der Datenbearbeitenden auszulegen sind, überzeugt dennoch nicht. Vielmehr scheint aufgrund der Rechtslage, wonach das DSG für den privaten Sektor den Grundsatz der freien Datenbearbeitung mit Schranken vorsieht und erst die qualifizierte Verarbeitungshandlung eine Persönlichkeitsverletzung auslöst, eine andere Folgerung angezeigt: Für die Auslegung der generalklauselartigen Verarbeitungsgrundsätze ist ihre Einbettung in das Persönlichkeitsrecht angezeigt. Demnach figuriert der Grundsatz der Freiheit der Datenbearbeitung als Prioritätsregel, die Beschränkung ist die Ausnahme.[1073]

793 An dem beschriebenen Konzept gemäss Art. 12 Abs. 2 DSG wird mit Art. 30 Abs. 2 nDSG festgehalten. Damit implementiert die Totalrevision in einem Kernpunkt ein von der DSGVO abweichendes Regime, obschon eine Annäherung an

1072 Zum Vollzugsdefizit, das ein Einhaltungs- wie Durchsetzungsdefizit umfasst, dritter Teil, VII. Kapitel, wobei mit den datenschutzrechtlichen Neuerungen, wie sie die DSGVO und die Totalrevision des DSG bringen, davon auszugehen ist, dass die datenschutzrechtlichen Vorgaben markant an Effizienz gewinnen werden; zu diesen vgl. dritter Teil, VIII. Kapitel, A.

1073 Zur Prioritätsregel Pfaffinger, ZSR 2011, 417 ff.

das Datenschutzrecht der EU erreicht werden sollte.[1074] Art. 6 DSGVO geht auch für private Stellen von einem Verarbeitungsverbot mit Erlaubnistatbeständen aus, wobei die Datenschutzkonformität der Verarbeitungshandlungen zusätzlich an die Einhaltung der Verarbeitungsgrundsätze gemäss Art. 5 DSGVO gebunden wird. Insofern lässt sich sagen, dass die DSGVO ein *zweistufiges Schrankensystem* verankert, auch im privaten Bereich. Das DSG implementiert für den privaten Bereich ein *einstufiges Modell*.

1.2. Allgemein zugänglich gemachte Personenangaben, kein Widerspruch

794 *Die zweite Gruppe von Verarbeitungshandlungen,* für die nach schweizerischem Recht ebenso wenig von einer Persönlichkeitsverletzung ausgegangen wird, ist diejenige nach Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG. Die Totalrevision hält an der Konstellation fest. Demnach wird keine Persönlichkeitsverletzung qua Personendatenverarbeitung begangen, wenn Personendaten bearbeitet werden, die von der sie betreffenden Person *allgemein zugänglich gemacht* wurden, und die Person eine Bearbeitung *nicht ausdrücklich untersagt hat*.

795 Zum ersten Tatbestandselement hält das Bundesverwaltungsgericht im Entscheid Money-House vom 18. April 2017 fest:

> «Im Übrigen bleibt festzuhalten, dass die gesetzliche Vermutung von Art. 12 Abs. 3 DSG, wonach keine Persönlichkeitsverletzung vorliegt, wenn die betroffene Person die Daten allgemein zugänglich gemacht hat, so dass eine unbestimmte Zahl von Personen sie ohne wesentliche Hindernisse in Erfahrung bringen kann, ohne die Bearbeitung ausdrücklich zu verbieten, vorliegend nicht greift. Hierfür wäre erforderlich, dass die betroffene Person ihre Daten mit Wissen und Willen allgemein zugänglich gemacht hat oder durch einen Dritten zugänglich machen liess. Blosses Dulden der Handlung eines Dritten, ohne etwas zum Zugänglichmachen beizutragen, genügt indes nicht. Weiss etwa eine Person, dass sie betreffende Personendaten allgemein zugänglich gemacht werden sollen, z. B. in Form eines Zeitungsberichts, bleibt sie aber passiv, findet Art. 12 Abs. 3 DSG keine Anwendung (Urteil des BVGer A-7040/2009 vom 30. März 2011 E. 9.3 und Rosenthal, a. a. O., Art. 12 DSG Rz 54 ff., insbesondere Rz 59). Weder betreffend die Handelsregisterdaten noch die auf anderen Plattformen wie www.local.ch publizierten Daten stellt die Beklagte nämlich auf eine Einwilligungserklärung der darin genannten Personen ab. Die strittigen Daten werden somit nicht von den betroffenen Personen selber i. S. v. Art. 12 Abs. 3 DSG wissentlich und willentlich auf der Plattform der Beklagten allgemein zugänglich gemacht. Dieser Ausschlussgrund für das Bestehen einer Persönlichkeitsverletzung kommt demnach nicht zum Tragen (vgl. mit Bezug auf die Handelsregisterdaten Urteil des BVGer A-4086/2007 vom 26. Februar 2008 E. 5.1.2). Daran ändert auch ein allfälliges, nicht wahrgenommenes Widerspruchsrecht nichts, da passives Dulden wie soeben erwähnt nicht genügt.»[1075]

1074 Botschaft 2017–1084, 1 ff., 3 ff.
1075 BVGer, A-4232/2015 – Moneyhouse, Urteil vom 18. April 2017, E 5.4.1.

Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG sind bereits theoretisch betrachtet interessant. Die Norm *fusioniert* zwei für das Recht der Privatheit und das Datenschutzrecht *traditionsreiche Paradigmen*: Kombiniert wird eine Idee der *Selbstbestimmung* mit derjenigen des sphärentheoretisch begründeten Zweikammersystems, das zwischen öffentlich und privat differenziert. 796

Die Bestimmung integriert *zum einen* unübersehbar die *Sphärentheorie* mit einem Binärcode von «öffentlich» sowie «privat» in das Datenschutzgesetz.[1076] Charakteristisch für diese ist ein zwiebelartig, statisch gedachtes Modell von konzentrischen Kreisen, die um die Person angelegt sind, deren Lebenswelt sich in eine Geheim-, eine Privat- und eine Gemeinsphäre gliedern soll.[1077] An dieser Stelle ist nicht der erste Dualismus, der öffentlich i. S. v. staatlich und privat i. S. des Bereiches zivilgesellschaftlicher Beziehungen differenziert, gemeint. Es geht um eine dichotome Strukturierung innerhalb des privaten Sektors, wobei mit der Figur der allgemein zugänglich gemachten Personendaten ein öffentlicher Bereich strukturiert wird, demgegenüber ein privater Bereich abgegrenzt wird.[1078] Damit zeigt sich das DSG als *doppelt duales Gesetz*. 797

Dieser Fingerabdruck der *Sphärentheorie im DSG* gemäss Art. 12 Abs. 3 DSG (expliziter zu finden in Art. 12 Abs. 2 lit. b DSG) und wie er selbst nach Totalrevision mit Art. 30 Abs. 3 nDSG beibehalten wird erstaunt. Denn die Erkenntnis, wonach die Sphärentheorie erhebliche Schwächen unter dem Regime moderner Verarbeitungstechnologien aufweise, trieb die Erarbeitung eines *DSG* mit einem Regelungskorpus auch für den privaten Bereich an.[1079] Die Sphärentheorie gilt seit Dezennien als untaugliches Konzept, die Herausforderungen der Informationsverarbeitungstechnologien zu bewältigen.[1080] Dasselbe gilt für eine daran anknüpfende abstrakte Kategorisierung von Personendaten als gewöhnlich oder besonders schutzwürdig. Gleichwohl hinterlässt die Sphärentheorie bis heute ihre Spuren im DSG, so in Art. 12 Abs. 3 DSG und Art. 30 Abs. 3 nDSG. 798

Zum anderen importiert Art. 12 Abs. 3 DSG die *Idee eines selbstbestimmt handelnden Datensubjektes*. Es handelt sich dabei um eine Figur, der in jüngerer Zeit das Potential zur Bewältigung der datenschutzrechtlichen Herausforderungen zugemessen wird.[1081] Nach Art. 12 Abs. 3 DSG ist es das Datensubjekt, das seine Angaben *allgemein zugänglich macht und damit des Datenschutzes quasi verlustig geht*. Den Datenschutz kann es aktivieren, indem es die Verarbeitung explizit verbietet. Folglich weist die Norm, zumindest theoretisch, eine starke Orientie- 799

1076 Vgl. zu dieser m. w. H. Aebi-Müller, N 512 ff.
1077 Vgl. m. w. H. Dies., N 512 ff.
1078 Vgl. zum ersten Dualismus und zum Privaten im Privaten erster Teil, III. Kapitel, B.
1079 Vgl. BBl 1988 II 414 ff., 418 f.
1080 Vgl. m. w. H. Aebi-Müller, N 512 ff.
1081 Kritisch hierzu Barocas/Nissenbaum, 1 ff., 4.

rung an einer *Idee der Autonomie und Selbstbestimmung des Datensubjektes* auf.[1082]

800 Nicht abschliessend geklärt scheint bezüglich Art. 12 Abs. 3 DSG die Frage, ob für den Fall eines Widerspruches, der ein Verarbeitungsverbot etabliert, eine Verarbeitung aufgrund eines übertrumpfenden anderen Rechtfertigungsgrundes, insb. eines überwiegenden Interesses, zulässig sein kann. Der Widerspruch wäre dann keine «unüberwindbare Barriere» resp. «kein letztes Wort». Vielmehr würde das überwiegende Interesse zu einer Art «Über-Generalklausel».[1083] Weil sich Art. 12 Abs. 3 DSG hierzu nicht äussert, fragt sich, ob es sich um ein qualifiziertes Schweigen oder eine Lücke handelt. Nimmt man eine Lücke an («analog» zu Art. 12 Abs. 1 lit. b DSG und der insofern herrschenden Interpretation) und lässt eine Rechtfertigung zu, wird der Wille des Datensubjektes abgeschwächt. Umgekehrt stärkt eine restriktive Zulassung überwiegender Interessen, die das Verbot des Datensubjektes überwiegen, die Selbstbestimmung.[1084]

801 Diese *zweite Gruppe der nicht persönlichkeitsverletzenden Verarbeitungshandlungen* galt lange als unproblematisch, da sie zum einen an die tradierte Denkweise anknüpft, wonach ein öffentlicher Bereich ungeschützt bleiben soll, zum anderen jener Konstellation auch ein implizites Willenselement des Datensubjektes, das seine Personendaten allgemein zugänglich gemacht hat, innewohnt. Allerdings konterkariert die besagte Regelung den Datenschutz allem voran im Online-Bereich in empfindlicher Weise.[1085] Sie wird aufgrund der Realitäten moderner Informationsverarbeitungstechnologien und damit der faktischen Entwicklungen auf den Prüfstand gestellt.

802 Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG überzeugt bereits aus Praktikabilitätserwägungen nicht: Im Lichte des in der Schweiz beliebten pragmatischen Ansatzes kann nicht davon ausgegangen werden, dass geprüft wird, ob die «allgemein zugänglichen Daten» – wie es das Gesetz verlangt – von der Person *selbst* allgemein zugänglich gemacht wurden. Ob die Einhaltung dieser Voraussetzung in der Realität erstellt wird, ist oftmals zweifelhaft.[1086] Ebenso faktisch an Grenzen stösst die Widerspruchslösung, mit welcher die vorab in den öffentlichen

1082 Insofern wird das Private nicht mit dem Gegenbegriff des Öffentlichen konstruiert, sondern mit der Autonomie verbunden. Die Relation von Privatheit und Autonomie hat namentlich Rössler herausgearbeitet, 83 ff.; vgl. auch Hotter, 29 ff.

1083 Vgl. zu den entsprechenden Termini Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien Kommentar, N 33 und N 45.

1084 Hierzu auch Radlanski, der ebenso darauf hinweist, dass bei Annahme eines Alternativverhältnisses die Datenmacht der Subjekte einschlägig zurückdividiert wird und im Ergebnis aufseiten der Subjekte eine Rechtsposition suggeriert wird – das Recht der Selbstbestimmung –, das so selbst nicht im deutschen System kompromisslos umgesetzt wird, 203.

1085 So auch Rampini, BSK-DSG, Art. 12 N 17; zu Datenverarbeitungen im Online-Bereich vgl. auch Tinnefeld/Buchner/Petri, 387 ff.

1086 Zum Vollzugsdefizit allgemein und vertiefend dritter Teil, VII. Kapitel, A.–C.

Raum entlassenen Personendaten in die Beachtlichkeit der Datenschutzbestimmung zurückverwiesen werden sollen.[1087]

Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG ist allem voran aber konzeptionell problematisch. Die Norm bleibt in einer dichotomen Kategorisierung verwurzelt. Letztere dürfte als Paradigma eines wirksamen Datenschutzrechts überholt sein. Die Bestimmung schränkt den Datenschutz empfindlich ein: Personendaten, die allgemein zugänglich gemacht wurden, gelten quasi als öffentlich und verlieren damit zumindest partiell den datenschutzrechtlichen Rahmen. Damit erstaunt auch nicht, dass von der Lehre insofern beschränkende Auslegungen präsentiert werden.[1088] Ebenso nachvollziehbar ist, dass eine mit Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG vergleichbare Bestimmung der DSGVO *fremd* ist. 803

Die Norm hat mit den Entwicklungen des Internets spezifische Brisanz erlangt. Damit drängt sich die Frage auf, ob ebenda zugänglich gemachte Personendaten nach DSG überhaupt als allgemein zugänglich gemachte Angaben taxiert werden sollen und können. Insofern Rampini: 804

> «Gedacht wurde dabei an allgemein zugänglich gemachte Daten wie die Personalien einer Person, ihre Berufsbezeichnung, Adresse, Telefonnummer usw. sowie an Daten und Meinungen, welche die Person in einer öffentlichen Veranstaltung oder in den Medien über sich selber bekannt gibt […]. Die Bestimmung hat durch die Entwicklung des Internets neue Aktualität und Brisanz erlangt. Im Internet wird – oft sorglos – eine Vielzahl von persönlichen Daten veröffentlicht […]. Einmal veröffentlicht sind die Daten jedermann und weltweit einsehbar.»[1089]

Für das Internet läuft man über Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG Gefahr, das «Netz» als potentiell quasi-öffentlichen Bereich zu taxieren, womit Bearbeitungen von ebenda durch das Datensubjekt zugänglich gemachten Personenangaben vermutungshalber als nicht persönlichkeitsverletzend beurteilt werden.[1090] 805

Die Problematik der Bestimmung kann zudem über eine systematische Auslegung abgefedert werden: Von Gesetzes wegen nicht klar ist das Verhältnis von Art. 12 806

1087 Zu den Schwächen von Einwilligungs- und Widerspruchskonzeptionen im Lichte der datenschutzrechtlichen Realitäten unter Hinweis namentlich auf Radlanski vertiefend, insb. 12 ff., 210 ff.

1088 Hierzu namentlich Meier, N 1581 ff.

1089 Rampini, BSK-DSG, Art. 12 N 16 f.

1090 Bezüglich Twitter und sozialen Plattformen im Internet vgl. BGer, 5A_195/2016, 4.7.2016, E 5.3.; Bull, NVwZ 2011, 257 ff., 262; kritisch zu einer solchen Konzeption Zulauf/Sieber, AJP 2017, 548 ff., wobei die Autorinnen sowohl auf Nissenbaums Theorie zur «Privacy in Context», die Empfehlungen des Presserates sowie die Rechtsprechung des EGMR eingehen, der den Schutz einer privaten Zone auch im öffentlichen Raum verbürgt, 551 ff.; zur Lehre und Rechtsprechung mit Blick auf Fotos im Internet Fankhauser/Fischer, in: Fankhauser/Reusser/Schwander (Hrsg.), 193 ff., 195; vertiefend zu den Risiken und Herausforderungen von Social Media Coen, *passim*; illustrativ zu einer solchen Auffassung, wonach im Internet publizierte Informationen öffentlich zugänglich gemachte Informationen seien, Geiser, in: Gschwend/Hettich/Müller-Chen u. a. (Hrsg.), 373 ff., 377; vgl. für Deutschland auch Diercks, PinG 2016, 30 ff. und Göpfert/Wilke, NZA 2010, 1329 ff.

Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG und Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Bleiben die allgemeinen Verarbeitungsgrundsätze einschlägig für den Fall, dass eine Person die sie betreffenden Angaben allgemein zugänglich gemacht und keinen Widerspruch für weitere Verarbeitungen angebracht hat? Oder werden die allgemeinen Verarbeitungsgrundsätze obsolet, weil die Person ihre Daten selbst unwidersprochen «in die Allgemeinheit» entlassen hat? Mehrere Autoren vertreten hierzu zutreffenderweise, dass Art. 12 Abs. 3 DSG nicht von der Einhaltung weiterer datenschutzgesetzlicher Vorgaben, namentlich auch der allgemeinen Verarbeitungsvorgaben gemäss Art. 4 DSG resp. Art. 6 nDSG entbinde.[1091] Mit einer solchen Interpretation wird Art. 12 Abs. 3 DSG resp. Art. 30 einiges von seiner Spannungshaftigkeit, die der Artikel im Lichte der jüngsten technologischen Entwicklungen erlangt hat, genommen. Die Verarbeitung von allgemein zugänglich gemachten Personendaten ist somit im Anwendungsbereich von Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG nicht frei; vielmehr müssen die allgemeinen Verarbeitungsgrundsätze i. S. v. Art. 4 DSG resp. Art. 6 nDSG als Minimalstandard berücksichtigt werden. Im Ergebnis führt die Ansicht, wonach die allgemeinen Verarbeitungsgrundsätze weiterhin beachtlich sind, zu einer weitgehenden Korrektur von Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG. Mit Fug und Recht fragt sich sodann, inwiefern der Bestimmung noch ein eigenständiger Bereich verbleibt.

807 An dieser Stelle ist die Linse zu öffnen und Art. 12 Abs. 3 DSG systematischer innerhalb einer erweiterten Landschaft zu reflektieren: Allem voran die Analyse zum Zweckbindungsgrundsatz hat ergeben, dass sowohl die *Basierung datenschutzrechtlicher Normierung in einem Dualismus von öffentlich versus privat* als auch die *Beschränkung des Datenschutzrechts auf den Subjektschutz* zu kurz greift. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG führt dazu, dass der private Bereich einer dualistischen und stark sphärentheoretisch orientierten Sichtweise verhaftet bleibt. Als Resultat wird der Datenschutz gegenüber öffentlich resp. allgemein zugänglich gemachten Angaben herabgesenkt.[1092] Zugleich stellt die Bestimmung in zentraler Weise auf den Willen des Subjektes ab, das einerseits seine Angaben «allgemein zugänglich gemacht hat» und andererseits einer Verarbeitung (nicht) widersprochen hat. Im Laufe dieser Studie wurde an mehreren Stellen herausgearbeitet, dass die *datenschutzrechtlichen Herausforderungen mehrdimensional sind*. Das Datenschutzrecht hat über den *Subjektschutz hinaus*, so eine Schlussfolgerung nach einer Analyse des Volkszählungsurteils des Bundesverfassungsgerichts, die Funktion zu erfüllen, die *Integrität spezifischer resp. pluraler Verarbeitungszusammenhänge*, *Bereiche resp. Systeme zu schützen*.

1091 So Rosenthal, HK-DSG, Art. 12 N 53; vgl. weiter Baeriswyl, digma 2009, 99; Meier, N 1577.
1092 Ein Teil der Lehre stellt sich gegen eine solche Lockerung, indem für die Anwendbarkeit und Beachtlichkeit der allgemeinen Verarbeitungsgrundsätze plädiert wird.

Vor diesem Hintergrund greift es zu kurz, das Internet als monolithischen öffentlichen Bereich zu qualifizieren, wobei Datensubjekte mit der Nutzung quasi ihre Einwilligung für (weitgehend unbeschränkte) weitere Verarbeitungshandlungen geben. Ein solches Konzept ist aus einer Datenschutzperspektive *nicht tragfähig*. Im Ergebnis scheinen genau dies auch die Ansichten zu adressieren, die dafür eintreten, dass Art. 12 Abs. 3 DSG nicht von der Einhaltung der allgemeinen Datenschutzvorgaben dispensiert. 808

Für das Internet generiert die unter Treu und Glauben erläuterte Doktrin der «*reasonable expectations of privacy*» Erkenntnisse.[1093] Sie lassen sich zu einer Hypothese verdichten, wonach im Internet und z. B. auf Facebook mit Freunden und Verwandten *zwecks* Beziehungspflege ausgetauschte Angaben *nur zu diesem Zweck geteilt werden*. Ebendies dürfte mit einer vernünftigen Erwartung verbunden sein, wonach diese *Informationen aus dem persönlichen Lebensbereich nicht für einen anderen gesellschaftlichen oder staatlichen Bereich genutzt, beispielsweise nicht für und im privaten oder öffentlichen Arbeitskontext* ausgewertet werden.[1094] Im Ergebnis ist Rampini beizupflichten, der dafür plädiert, dass weitere Personendatenverarbeitungen von im Internet veröffentlichten Personenangaben nur dann nicht persönlichkeitsverletzend sind, wenn sich diese «im Rahmen des aus den Umständen ersichtlichen Verarbeitungszwecks» bewegen.[1095] 809

1.3. Resümee

Für das DSG sind *zwei Hauptkonstellationen* hervorzuheben, in denen die Tatbestandsmässigkeit der Persönlichkeitsverletzung grundsätzlich nicht angenommen wird. Anders gewendet: Das DSG beurteilt die fraglichen Arten von Personendatenverarbeitungen als nicht dergestalt qualifiziert, dass sie die Intensität einer Persönlichkeitsverletzung erreichen würden. Keine Persönlichkeitsverletzung liegt nach Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG grundsätzlich vor, wenn die Verarbeitungshandlung in Einklang mit den allgemeinen Verarbeitungsgrundsätzen steht. Keine Persönlichkeitsverletzung soll zudem vorliegen, wenn gemäss Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG Personendaten vom Da- 810

1093 Vgl. hierzu zweiter Teil, V. Kapitel, B.2.3.

1094 Dazu, dass auf Social Network Sites geteilte Angaben «freiwillig einer breiten Öffentlichkeit präsentiert werden» EDÖB, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien/erlaeuterungen-zu-sozialen-netzwerken.html> (zuletzt besucht am 30. April 2021); anders dagegen OGH-Beschluss vom 30. März 2016, 6 Ob 14/16a – Manipuliertes Facebook-Foto/Strandfoto, wonach das Veröffentlichen von (Personen-)Bildnissen in sozialen Netzwerken wie Facebook regelmässig nur eine bestimmte, vom Betroffenen gewünschte Öffentlichkeit bewirke; zum Thema Datenschutz und Facebook auch Buchner, DuD 2015, 402 ff.; vgl. in diesem Zusammenhang auch Rudin, digma 2010, 48 f.; beachte insofern auch EGMR Nr. 61496/08 – Bârbulescu/Romania, Urteil vom 12. Januar 2016; allgemein zum Recht am eigenen Bild auch BGE 127 III 481; BGE 129 III 715; BGE 138 II 346.

1095 Rampini, BSK-DSG, Art. 12 N 18.

tensubjekt allgemein zugänglich gemacht wurden und dieses einer Verarbeitung nicht widersprochen hat.

811 Beide Konstellationen von Personendatenverarbeitungen, die von Gesetzes wegen als *nicht* persönlichkeitsverletzend taxiert werden, speisen *verschiedene datenschutzrechtliche Konzepte in das DSG ein*.[1096] Mit der Totalrevision wird an diesen festgehalten.

812 Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG lehnt konsequent am Regelungskonzept gemäss Art. 28 ZGB an: Das Regime wird, da es erst *qualifizierte Verarbeitungshandlungen* als persönlichkeitsverletzend beurteilt, als *Integritätsschutz* charakterisiert. Gleichermassen akkurat dürfte eine *Chiffrierung als Missbrauchsgesetzgebung* sein. Die Regelungsmechanik verzichtet auf eine Kategorisierung von öffentlich versus privat und formuliert Vorgaben, die auf den *fairen, redlichen Umgang mit Personendaten abzielen*. Es sind die grossen Verarbeitungsgrundsätze, die als Minimalstandard einzuhalten sind und mit deren Einhaltung die Persönlichkeit der Datensubjekte nicht verletzt wird. Die Verarbeitenden stehen in der Pflicht, diese Regelkonformität sicherzustellen. Mit der Totalrevision wird die *proaktive Rechtseinhaltung durch mehrere Umsetzungsinstrumente akzentuiert. Damit rückt die defensivrechtliche und retrospektive Perspektive, wie sie dem Persönlichkeitsschutz eigen ist, von Gesetzes wegen in den Hintergrund*. Zugleich wird gegenüber der Sphärentheorie ein Perspektivenwechsel vollzogen. Der Fokus liegt auf den Verarbeitenden und der Gewährleistung von Prozessen, die einen Katalog an Mindestanforderungen, ausgedrückt mit den Verarbeitungsgrundsätzen, zu achten haben.

813 Demgegenüber steht Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG konzeptionell in einem Kontrast zu dem beschriebenen prozesshaft gedachten Integritätsschutz. Die Regelung beruht auf einem sphärentheoretisch begründeten dualen wie subjektverhafteten Konzept. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG trägt mit der als untauglich geltenden Kategorisierung von «öffentlich» und «privat» einen Ansatz in das DSG, der in empfindlicher Weise dessen Schutz preisgibt. Insofern ist eine Auslegung, wonach sämtliche im Internet vom Datensubjekt zugänglich gemachten Personendaten als allgemein zugänglich gemacht resp. öffentlich gelten und damit vom Datenschutz exkludiert werden, kritisch. Entsprechend wurden korrigierende Interpretationen vorgeschlagen, wonach selbst im Anwendungsbereich von Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG kein Dispens von der Einhaltung der allgemeinen Datenschutzvorgaben gilt. Die DSGVO kennt keine vergleichbare Regelung. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG wird uns an späterer Stelle nochmals beschäftigen, wo gezeigt werden

1096 Zum einen diejenigen, welche die allgemeinen Verarbeitungsgrundsätze einhalten, zum anderen die Verarbeitung von allgemein zugänglich gemachten Personendaten bei fehlendem Widerspruch.

wird, weshalb das Internet gerade *nicht als einheitlicher öffentlicher Bereich* taxiert werden sollte.

Zusammenfassend vereinigt das DSG bei der Definition von Personendatenbearbeitungen, bei denen die Grenze zur Persönlichkeitsverletzung *nicht* überschritten wird, *verschiedene Regelungsmechaniken*. Nach ihrer Betrachtung ist auf die eingangs zitierten Umschreibungen zurückzukommen. Meinungen, wonach jede Personendatenverarbeitung eine Persönlichkeitsverletzung begründe, wonach das Datensubjekt ein «Herrschaftsrecht» über seine Personendaten habe, wonach Personendatenverarbeitungen stets der Einwilligung des Datensubjektes bedürften oder wonach jedermann grundsätzlich selbst über die Verwendung «seiner» Personendaten befinden könne, haben im DSG *keine* Grundlage. Diese Klarstellung ist relevant, zumal andernfalls selbst gegenüber der Allgemeinheit ein Rechtsbestand suggeriert wird, der nach DSG nicht verbürgt wird.[1097] Eine unmittelbare Folge sind enttäuschte Erwartungen, was für ein Rechtsgebiet, das in besonderer Weise auf die Kategorie des Vertrauens angewiesen ist,[1098] besonders schwer wiegt. 814

2. Persönlichkeitsverletzende Verarbeitungen nach DSG

2.1. Vorbemerkungen

Die vorangehende Darstellung der *nicht* persönlichkeitsverletzenden Verarbeitungen befasste sich *indirekt resp. e contrario* zugleich mit den persönlichkeitsverletzenden Handlungen. Es ging um deren Abgrenzung und den entsprechenden Grenzverlauf. Daraus resultieren folglich teilweise Redundanzen. Sie werden zugunsten der Klärung vor dem Hintergrund der facettenreichen Umschreibungen zur Funktionsweise des DSG im privaten Bereich in Kauf genommen. 815

Persönlichkeitsverletzende Personendatenverarbeitungen sind insb. in Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG niedergelegt. In den lit. a–c werden nicht abschliessend die Tatbestände der Persönlichkeitsverletzung konkretisierend umschrieben. 816

Mit der Totalrevision werden Struktur und Inhalt von Art. 12 f. DSG weitgehend übernommen, vgl. Art. 30 f. nDSG. Insofern ist immerhin auf zweierlei hinzuweisen: Der erste Hinweis gilt einer *Bereinigung*. Neu wird die Rechtfertigungsmöglichkeit konsequent aus den Umschreibungen der persönlichkeitsverletzenden 817

1097 Zutreffend Rudin, BJM 1998, 113 ff., 115, der es als unglücklich bezeichnet, dass die Schweizer Lehre auf das Recht auf informationelle Selbstbestimmung i. S. des Volkszählungsurteils und i. S. eines Kontrollrechts referiert.

1098 Hierzu bereits zweiter Teil, V. Kapitel, B.2.; Druey, Rechtswissenschaftliche Abteilung der Universität St. Gallen (Hrsg.), 525 ff.

Tatbestände ausgegliedert. Die Totalrevision führt somit nach, was unter bisherigem DSG zur herrschenden Lehre und Rechtsprechung geworden war. Bot der noch in Kraft stehende Gesetzestext vorab Anlass zu Unsicherheiten, konsolidierte sich eine Auslegung, wonach entgegen der uneinheitlichen Integration von Rechtfertigungsgründen in den drei Literae solche stets zuzulassen sind.[1099] Die zweite Neuerung ist materieller Natur, indem bislang an den Begriff der Bearbeitung von «Persönlichkeitsprofilen» geknüpfte Vorgaben im Rahmen des Themas Profiling einer eigenständigen und anderen Normierung zugeführt werden.

818 Zur Persönlichkeitsverletzung nach DSG vor seiner Totalrevision prägnant Rampini:

> «Wann eine Persönlichkeitsverletzung vorliegt, d. h. wann die Datenbearbeitung die Persönlichkeit der Betroffenen verletzt, wird durch Art. 12 Abs. 2 und Abs. 3 DSG konkretisiert (vgl. die Marginalie), einerseits positiv (Abs. 2), andererseits negativ (Abs. 3). Diese Konkretisierung bleibt notwendigerweise vage.»[1100]

819 Ungeachtet dieser «Vagheit» scheint in einem Punkt Konsens zu bestehen: Der Massstab für die Beurteilung, ob ein Verstoss gegen eine Bearbeitungspflicht nach Art. 12 Abs. 2 lit. a–c DSG eine Persönlichkeitsverletzung begründe, sei ein *objektiver*.[1101] Das subjektive Empfinden der Datensubjekte oder Verantwortlichen sei nicht relevant.

820 Dies vorausgeschickt werden nun die Hauptkonstellationen der Persönlichkeitsverletzung, wie sie der Gesetzgeber nicht abschliessend in Art. 12 Abs. 2 lit. a–c DSG resp. Art. 30 Abs. 2 lit. a–c nDSG aufführt, beleuchtet.

2.2. Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG en détail

821 Innerhalb des Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG werden in den lit. a–c (nicht abschliessend, vgl. den Ingress «insbesondere») drei Tatbestände persönlichkeitsverletzender Personendatenverarbeitung definiert. Die beiden Konstellationen von lit. a und lit. c haben primär einen objektiven Charakter, lit. b hat eher subjektive Qualität.

- Lit. a widmet sich den *allgemeinen Verarbeitungsgrundsätzen*, deren Nichteinhaltung als Persönlichkeitsverletzung gilt. Insofern ist auf das V. Kapitel dieses zweiten Teils hinzuweisen.
- Lit. b gewährleistet ein *Widerspruchsrecht* des Datensubjektes.

1099 BGE 136 II 205; Auslegungshilfe des BJ; vgl. Rampini, BSK-DSG, Art. 12 DSG N 9b.
1100 Rampini, BSK-DSG, Art. 12 N 3.
1101 Rosenthal, HK-DSG, Art. 4 N 3 und Art. 12 N 3 ff.; Haas, N 68; vgl. Meili, BSK-ZGB, Art. 28 ZGB N 42; Rampini, BSK-DSG, Art. 12 DSG N 6.

Lit. c widmet sich einer spezifischen Bearbeitungshandlung, der *Weitergabe* von «qualifizierten Datenbeständen», insb. von *besonders schützenswerten Personendaten und Persönlichkeitsprofilen an Dritte*.

822 Die vom DSG umschriebenen persönlichkeitsverletzenden Verarbeitungshandlungen kombinieren und fusionieren – wie zu zeigen sein wird – in sich in eindrücklicher Weise unterschiedliche Stossrichtungen und Ansätze: ein Konzept des *Integritätsschutzes*, einen *Autonomieansatz* sowie die *Idee der Sphärentheorie*.[1102]

823 Vorauszuschicken ist: Art. 12 Abs. 2 lit. a DSG lässt sich als «Auffangtatbestand» in dem Sinne bezeichnen, dass er stets dann greift, wenn kein Widerspruch vorliegt oder wenn keine besonders schutzwürdigen Personendaten resp. Persönlichkeitsprofile an Dritte weitergegeben werden. Da es bei den letzteren beiden Konstellationen um spezifische Konstellationen geht, greift über weite Strecken das Regime von Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Insofern lässt sich der Absatz – *auch wenn er gewissermassen eine Auffangordnung bildet – als die Grundsatzordnung qualifizieren*. Folglich dürfte die Funktionsweise von Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG für eine Qualifizierung des DSG im privaten Bereich im Vordergrund stehen. Der überwiegende Teil der Personendatenverarbeitungen im privaten Bereich wird von den materiellrechtlichen Vorgaben, wie sie Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG formuliert, datenschutzgesetzlich strukturiert.

2.2.1. lit. a – Regime des Integritätsschutzes

824 Hinsichtlich Art. 12 Abs. 1 lit. a DSG stand lange eine Frage im Zentrum der Überlegungen: Handelt es sich bei der Nichterwähnung möglicher Rechtfertigungsgründe um einen Lapsus des Gesetzgebers oder um eine Stärkung des Datenschutzes? Insofern etablierte sich im Anschluss an eine Stellungnahme vonseiten des Bundesamtes für Justiz eine herrschende Lehre und Praxis: Rechtfertigungsgründe sind prinzipiell zuzulassen, allerdings mit Zurückhaltung.[1103] Die Totalrevision bringt mit Art. 30 Abs. 1 lit. a nDSG eine entsprechende Bereinigung.

825 Zur *konzeptionellen Tragweite der Bestimmung*: In einem System der prinzipiellen Verarbeitungsfreiheit, wie es die Schweiz im DSG für den privaten Bereich vorsieht, kommt der *Schrankendefinierung vorrangige Bedeutung* zu. In Bezug auf diese Schranken stehen gemäss Art. 12 Abs. 2 lit. a DSG die allgemeinen Ver-

1102 Letztere sollte mit dem DSG bekanntermassen überwunden werden, vgl. insofern BBl 1988 II 414 ff., 420 f.; Aebi-Müller, m. w. H., N 512 ff.

1103 Vgl. BGE 136 II 508, Regeste und E 5; entsprechend auch EDÖB, Schlussbericht PostFinance, 6, 23.

arbeitungsgrundsätze, vgl. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG, an erster Stelle. Die Totalrevision verweist in Art. 30 Abs. 2 lit. a nDSG auf Art. 6 und Art. 8 nDSG.

826 In beiden Fassungen sind es erst und nur *qualifizierte Personendatenverarbeitungen*, welche die Schranken einer prinzipiell freien Verarbeitung durchbrechen und eine Persönlichkeitsverletzung begründen. An dieser Stelle liegen die Schranken der allgemeinen Verarbeitungsfreiheit in einer Missachtung der materiellrechtlichen Datenschutzvorgaben, der *allgemeinen, weitgehend generalklauselartigen Verarbeitungsgrundsätze*. Sie markieren prinzipiell die Persönlichkeitsverletzung.

827 Die Schweiz regelt im DSG für den privaten Bereich die datenschutzrechtlichen Vorgaben mit einem *einstufigen Schrankenmodell*. Ebendies gilt auch nach Totalrevision. Anders definiert die DSGVO sowohl für den öffentlichen als auch für den privaten Bereich ein *zweistufiges Schrankenmodell*. Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG weist damit zunächst eine *materiellrechtliche Schrankenfunktion* auf.

828 Zusätzlich haben Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG eine *Verweisungs- und Koppelungsfunktion*. Die Bestimmung referiert vorab auf die wichtigsten Grenzen der prinzipiellen Verarbeitungsfreiheit, die allgemeinen Verarbeitungsgrundsätze, vgl. insb. Art. 4 DSG und Art. 6 nDSG. Die Verletzung der allgemeinen Verarbeitungsgrundsätze wird an die zivilrechtliche Persönlichkeitsverletzung angekoppelt.

829 Schranken der grundsätzlich freien Verarbeitung resp. persönlichkeitsverletzende Handlungen im privaten Bereich finden sich damit materiellrechtlich in erster Linie *innerhalb* des DSG. Art. 12 Abs. 1 lit. a DSG besagt, dass «insbesondere» die Verletzung bestimmter allgemeiner Verarbeitungsgrundsätze eine Persönlichkeitsverletzung begründe, wobei auf die Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG verwiesen wird. Art. 30 Abs. 2 lit. a nDSG verweist auf Art. 6 und Art. 8 nDSG. Nach DSG sind es die allgemeinen, teilweise generalklauselartigen *Bearbeitungsvorgaben*, die als zweites Strukturmerkmal in diesem zweiten Teil dargestellt wurden, die den *Grenzverlauf zwischen nicht persönlichkeitsverletzender und persönlichkeitsverletzender Personendatenverarbeitung markieren*. Allerdings handelt es sich hierbei, wie das Wort «insbesondere» deutlich macht, um keine abschliessende Ordnung.

830 Art. 12 Abs. 2 lit. a DSG wird als *«Fiktion»*[1104] resp. *«unwiderlegbare Vermutung»*[1105] qualifiziert. Beide Rechtsfiguren, so wird es vertreten, dienen der Über-

1104 So Steinauer, in: Schweizer (Hrsg.), 43 ff., 45.
1105 So Peter, 125.

brückung faktischer Ungewissheit.[1106] Die Qualifizierung liegt wohl in der Vorstellung begründet, wonach quasi «naturgegeben» bestimmte (Verarbeitungs-)Handlungen persönlichkeitsverletzend sein sollen. Der Gesetzgeber hat diese als «naturgegebenes Faktum» freizulegen und abzubilden. Allerdings erschöpft sich die Funktion von Vermutung resp. Fiktion nicht in einem solchen Element. Vielmehr dienen sie dem Gesetzgeber regelmässig als *Qualifikations- und Definitionsinstrument*. Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG, mit welchem der Datenschutzgesetzgeber die Verletzung der allgemeinen Verarbeitungsgrundsätze explizit als Persönlichkeitsverletzung taxiert, hat weniger zum Ziel, faktische Ungewissheit zu überwinden. Vielmehr handelt es sich bei Art. 12 Abs. 1 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG um eine gesetzgeberische Konkretisierung einer Generalklausel, hier der Persönlichkeit und deren Verletzung durch Personendatenverarbeitungen.[1107] Folglich überzeugt die Qualifizierung der Konstruktion im Sinne einer beweisrechtlichen Figur nur teilweise. In erster Linie handelt es sich bei der Gesetzgebung um die generell-abstrakte Konkretisierung eines Rechtsbegriffes, hier der Persönlichkeit.

Der Beweis der *Persönlichkeitsverletzung* und insofern Nichteinhaltung der Ver- 831
arbeitungsgrundsätze durch die Verantwortlichen obliegt gemäss der Regel von Art. 8 ZGB dem Datensubjekt. In der heutigen datenschutzrechtlichen Realität ist ein solcher Beweis indes kaum führbar. Und selbst wenn einem Datensubjekt der Beweis gelingt, dass die allgemeinen Verarbeitungsgrundsätze durch eine Bearbeitungshandlung verletzt wurden, erscheint dies in Anbetracht der Bedeutung von Personendatenverarbeitungen in der heutigen Zeit als Tropfen auf den heissen Stein, der in keiner Weise geeignet ist, das Datenschutzrecht und dessen Einhaltung zu effektuieren.[1108]

Im noch in Kraft stehenden DSG bildet den Kern(tat)bestand der Persönlichkeits- 832
verletzung qua Personendatenverarbeitung die Verletzung der weitgehend *generalklauselartigen, gemeinsamen resp. allgemeinen Verarbeitungsgrundsätze*, Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG, vgl. Art. 30 Abs. 2 lit. a nDSG.

Allerdings wurde an früherer Stelle gezeigt, dass sich ihre konturierende und 833
beschränkende Wirkung faktisch wie theoretisch nur teilweise zu entfalten vermochte. Der Befund wird im dritten Teil unter dem Titel des *Vollzugsdefizites*

1106 Schulbeispiel insofern ist die Vaterschaftsvermutung resp. -fiktion. Vermutungen figurieren auf der Stufe des Beweises und beziehen sich auf strittige Tatsachen; vgl. hierzu die einschlägige Kommentarliteratur.

1107 Indem das Datenschutzrecht am Persönlichkeitsrecht anknüpft, trägt auch diese Anknüpfung den generalklauselartigen Charakter in das Datenschutzrecht; zum Persönlichkeitsrecht mit seiner generalklauselartigen Unbestimmtheit Ehmann, Juristische Schulung, Zeitschrift für Studium und praktische Ausbildung 1997, 193 ff., 193; zur Notwendigkeit von klaren und konsistenten Datenschutzvorgaben Solove, Stan. L. Rev. 2001, 1393 ff., 1461.

1108 Betreffend Vollzugsdefizit dritter Teil, VII. Kapitel.

vertieft. Ursächlich für das sog. Vollzugsdefizit ist auch die generalklauselartige Regelung, angeknüpft an den Grundsatz der Freiheit der Datenbearbeitung.[1109] Neben dieser materiellrechtlichen Problematisierung ist weiter die prozessrechtliche Situation mitverantwortlich dafür, dass das DSG weitgehend ein «Papiertiger» blieb:[1110] Personendatenverarbeitungen werden noch heute selten auf ihre Rechtmässigkeit hin überprüft, da Persönlichkeitsverletzungen kaum je von den Datensubjekten geltend gemacht werden.[1111] Zugleich hat der EDÖB – die Funktionen von Datenschutzbeauftragten wurden von der Gesetzgebung gerade auch als Instrument der Kompensation für ein generalklauselartiges Regelungsregime vorgesehen – nur beschränkte Kompetenzen (die immerhin mit der Totalrevision erweitert werden). Hinzu tritt die über lange Zeit eher schwache wissenschaftliche Durchdringung des DSG namentlich für den privaten Bereich. Eine Folge hiervon ist, dass die so wichtige Konkretisierung der allgemeinen Verarbeitungsgrundsätze als Schranke der grundsätzlich freien Personendatenverarbeitung durch Lehre und Praxis erst ansatzweise bewerkstelligt ist.[1112] Immerhin: Mit der Totalrevision dürfte die eine oder andere Schwäche durch die Schaffung neuer Umsetzungsinstrumente sowie der verschärften Instrumente zur Rechtsdurchsetzung abgemildert werden.

834 Gemäss Art. 12 Abs. 2 lit. a DSG Ingress begründen nicht nur Verstösse gegen die Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG eine «Persönlichkeitsverletzung»; vielmehr ist die Aufführung aufgrund der Wendung «insbesondere» nicht abschliessend. Dieselbe Regelung findet sich in Art. 30 nDSG. Damit kommt der Frage, welche weiteren Verstösse gegen datenschutzrechtliche Vorgaben eine Persönlichkeitsverletzung begründen, zumindest theoretisch betrachtet nicht unwesentliche Bedeutung zu.

835 Welche weiteren Verstösse gegen Vorgaben des DSG als Persönlichkeitsverletzung zu qualifizieren sind, ist nicht abschliessend geklärt. Die Problematik soll anhand von Art. 6 DSG nachgezeichnet werden. Die Bestimmung befasst sich mit den Voraussetzungen des rechtmässigen Transfers von Personendaten ins Ausland.[1113]

1109 Zum hohen Preis der Ansammlung von Generalklauseln im Datenschutzgesetz Simitis, Nomos-Komm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien Kommentar, N 20; zur schwachen Effektivität des Datenschutzrechts Ders., Symposium, 1 ff., 1.

1110 Vgl. Huber, recht 2006, 205 ff.; Drechsler, AJP 2007, 1471 ff.; beispielhaft auch Gogniat, Jusletter vom 20. Juni 2016, N 3, wonach im Rahmen von Personendatenverarbeitungen zahlreiche Persönlichkeitsverletzungen stattfinden; vgl. auch Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.1.

1111 Vgl. dritter Teil, VII. Kapitel, A.2.

1112 Hierzu zweiter Teil, V. Kapitel.

1113 Zur Rechtsanwendung bei internationaler Datenbearbeitung durch Private grundlegend Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.10; vgl. zu den jüngsten verschärfenden Entwicklungen im Zusammenhang mit dem Transfer von Personendaten in die USA <https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/medienmitteilungen.msg-id-80318.html> (zuletzt besucht am 3. Juni 2021).

Die Totalrevision baut insofern die Vorgaben aus, vgl. Art. 16 ff. nDSG und insb. Art. 61 lit. a nDSG, wo eine strafrechtliche Sanktionierung verankert wird.

Art. 6 DSG fehlt in der Aufzählung von Art. 12 Abs. 2 lit. a DSG. Auch die Totalrevision nimmt Verletzungen der Pflichten im Zusammenhang mit dem Auslandstransfer nicht explizit in den Katalog der Persönlichkeitsverletzung auf. Die fehlende ausdrückliche Qualifizierung von Verstössen gegen die entsprechenden Vorgaben als Persönlichkeitsverletzung ist in Anbetracht der Tatsache, dass Personendaten heute kaum mehr lokal innerhalb der Ländergrenzen verarbeitet werden und das Schlagwort der Globalisierung Hand in Hand mit jenen der Digitalisierung und der Informationsgesellschaft geht, bemerkenswert.[1114] Dass Daten isoliert lokal bearbeitet werden, wird zur Ausnahme; in der Regel agieren diverse Verarbeiter als Verantwortliche und Auftragsverarbeitende in einer Art Netzwerkstruktur über Landesgrenzen, ja die Grenze des Erdballes hinweg.[1115] 836

Art. 6 DSG definiert Vorgaben an den Datentransfer ins Ausland, wobei ein spezifisches Instrumentarium zum Schutz der Datenbearbeitungs*pflichten* beim Transfer ins Ausland und der Überprüfung ihrer Einhaltung vorgesehen wird. Zudem greifen die strafrechtlichen Sanktionsmöglichkeiten nach Art. 34 DSG bei einem Verstoss gegen die Meldepflicht. 837

Spricht dieses besondere Schutzinstrumentarium dafür, dass der individualrechtliche Rechtsschutz qua Persönlichkeitsrecht ausgeschlossen wird? 838

Passadelis scheint für eine solche Interpretation einzutreten, indem er die Bestimmung von Art. 6 DSG (vgl. Art. 16 ff. nDSG) als *öffentlich-rechtliche Norm* qualifiziert. Der Rechtsweg wäre daran anknüpfend nicht derjenige über das Zivilgericht. Anders dagegen wohl Maurer-Lambrou/Steiner mit den Worten: 839

> «[…] [D]as Fehlen einer Datenschutzgesetzgebung, welche einen angemessenen Schutz gewährleistet, gilt gesetzlich als eine schwerwiegende Persönlichkeitsverletzung (Art. 6 Abs. 1 DSG).»[1116]

Wertungsmässig scheint m. E. die Gravität der Verletzungen der Vorgaben über den Auslandstransfer äquivalent zu den Verletzungshandlungen nach Art. 4, Art. 5 und Art. 7 DSG zu sein, womit ohne Weiteres auf eine Persönlichkeitsverletzung zu schliessen wäre. Diese Ansicht vertritt nach meinem Verständnis ebenso Rampini.[1117] Um die weiteren, nicht explizit enumerierten persönlichkeitsverletzenden Handlungen als Persönlichkeitsverletzung zu taxieren, dürfte neben der 840

1114 Illustrativ insofern Hoffmann-Riem, AöR 1998, 513 ff., 533 f.
1115 Ders., a. a. O., Rz 6.1 f.; die DSGVO anerkennt die «Grenzenlosigkeit» von Personendaten nicht zuletzt durch ihr vereinheitlichendes Regime wie den extraterritorialen Anwendungsbereich, vgl. Art. 3 DSGVO; vgl. zur sog. Deterritorialisierung als eine Aporie des Informationsrechts Hoeren, 20 f.
1116 Maurer-Lambrou/Steiner, BSK-DSG, Art. 6 N 11.
1117 Rampini, BSK-DSG, Art. 12 N 9a.

Frage nach der qualitativen Äquivalenz namentlich eine *funktionelle Betrachtung* resp. eine Fokussierung auf die Auswirkung einschlägig sein. Im Zuge der jüngsten Revisionswelle, aber auch den jüngsten Entwicklungen zu den Privacy Shields aufgrund der erfolgreichen Initiativen des Datenschutzaktivisten Max Schrems gewinnen internationale Datentransfers und die damit einhergehenden datenschutzrechtlichen Risiken markant an Bedeutung.[1118] Mit dem Transfer von Personendaten in ein «unsicheres Drittland» kann der Datenschutz weitgehend unterlaufen werden. Aufgrund dieser Auswirkungen dürfte ausser Frage stehen, dass die Verletzung der Vorgaben im Zusammenhang mit dem Auslandstransfer eine Persönlichkeitsverletzung begründet. Anders dagegen dürfte namentlich die Verletzung von neuen Datenschutzpflichten, die eine (interne) Hilfsfunktion haben, so das Bearbeitungsverzeichnis oder die Dokumentationspflicht, nicht direkt zur Annahme einer Persönlichkeitsverletzung führen.

841 Die Frage, welche Pflichtverstösse, die nicht explizit zu den enumerierten Bearbeitungsgrundsätzen nach Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. nDSG gehören, als persönlichkeitsverletzend zu gelten haben, ist im Übrigen weitgehend ungeklärt und soll an dieser Stelle auch keiner umfassenden Klärung zugeführt werden.[1119]

842 Es handelt sich indes – wegen der nicht griffigen Rechtsdurchsetzung – um eine weitgehend theoretische Frage. Je grosszügiger Verstösse gegen das DSG als Persönlichkeitsverletzung qualifiziert werden, desto stärker wird – theoretisch und formell betrachtet – die individualrechtliche Position der Datensubjekte ausgestaltet. Weil allerdings Persönlichkeitsverletzungen infolge Personendatenverarbeitung kaum je von den Individuen moniert werden, ist mit der grosszügigen Inklusion von Datenschutzverstössen in die Persönlichkeitsverletzung nicht viel für die Wirksamkeit des DSG gewonnen. Selbst eine *grosszügige Inklusion* von Verstössen gegen Verarbeitungsvorgaben im DSG in die Persönlichkeitsverletzung gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG führt *faktisch nicht zu einer nennenswerten Effektuierung des Datenschutzgesetzes* im privaten Bereich.

843 Damit präsentiert sich ein paradoxer Befund: Ein Regime, das auf den Schutz der Persönlichkeit abzielt, erfährt keine merkliche Stärkung durch eine grosszügige Auslegung und Ausweitung der nicht abschliessend aufgeführten persönlichkeitsverletzenden Tatbestände gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Im Gegenteil – das Gesetz schafft weitere Unsicherheiten über dieje-

1118 Vgl. insofern <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-80318.html> (zuletzt besucht am 20. September 2021).

1119 Fraglich insb. betr. die Meldepflicht gemäss Art. 6 DSG, die Informationspflicht gemäss Art. 14 DSG, die Einhaltung der Vorgaben nach Art. 8, Art. 10a, Art. 11a Abs. 3 oder Art. 35 DSG; m. w. H. Rosenthal, HK-DSG, Art. 4 N 2 sowie Art. 12 N 3 und N 14.

nigen hinausgehend, die das generalklauselartige Regime ohnehin in ein Regime hineinträgt.

Als Kernbefund für Art. 12 Abs. 2 lit. a DSG – und damit als Kernbefund für das DSG im privaten Bereich selbst – ist festzuhalten: Innerhalb des DSG haben datenverarbeitende Stellen im privaten Bereich die allgemeinen Verarbeitungsgrundsätze namentlich gemäss Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG zu beachten, um *keine* Persönlichkeitsverletzung mittels ihrer Datenverarbeitungshandlungen zu begehen, vgl. Art. 12 Abs. 1 lit. a DSG. Bei Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG handelt es sich um die Implementierung eines *Integritätsschutzes* – ebendies erscheint als die treffende Bezeichnung des Regimes. Nicht jede Personendatenverarbeitung ist gemäss dem schweizerischen Querschnittsgesetz persönlichkeitsverletzend, vielmehr ist es erst die *qualifizierte Verarbeitung*, die als Persönlichkeitsverletzung gilt. Die Demarkationslinie wird von den allgemeinen Verarbeitungsgrundsätzen und deren Verletzung gezogen. Sie bilden die Schranken der freien, sprich unterhalb der Persönlichkeitsverletzung liegenden Datenverarbeitung. An dieser Konzeption hält die Totalrevision mit Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG weitgehend fest. 844

Die allgemeinen Verarbeitungsgrundsätze – im privaten Sektor eingebettet in den Persönlichkeitsschutz – sollen *faire und angemessene Verarbeitungsprozesse sowie Datenflüsse gewährleisten*.[1120] Damit geht es im *privaten Bereich*, mangels abweichender Vorgaben durch spezifische Regelungen, auch um eine Art der Sicherstellung der *Lauterkeit im Umgang* mit Personendaten, die Verhinderung übermässiger Personendatenverarbeitungsprozesse, die Gewährleistung allgemeinster Grundsätze der Redlichkeit oder auch Fairness im Umgang mit Personenangaben. 845

Folglich ist der für das Informations- und Datenschutzrecht so enge Bezug zum Vertrauen, zu Art. 2 ZGB, aber auch zum Wortlaut von Art. 13 Abs. 2 BV mit seinem Gegenbegriff hergestellt. Diese als allgemeines Regime greifende Konzeption der Vorgaben bei Personendatenverarbeitungen im *privaten Bereich* lässt nun wiederum – trotz der Ankoppelung an die subjektivrechtliche Persönlichkeitsverletzung – ebenso für individualrechtlich geschulte Juristinnen und Juristen die Strukturierung eines gesellschaftlichen Bereichs, eines *privaten Lebensbereiches* sichtbar werden. Indem der *Integritätsschutz* gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG derjenige ist, der im Sinne einer «Grundordnung» mangels Anwendbarkeit einer besonderen Regelung greift (vgl. zu Art. 12 846

1120 Zu diesem Konzept grundlegend Nissenbaum, 1 ff., 129 ff. Eine Betrachtungsweise, die sich auf Datenflüsse bezieht, lässt sich in der Schweiz bei Gächter/Egli, Jusletter vom 6. September 2010, N 90 ff., erkennen; auch Gogniat, Jusletter vom 20. Juni 2016, N 16 verwendet das Bild vom Datenstrom; den Datenfluss als Betrachtungsgegenstand der datenschutzrechtlichen Analyse zu definieren, schlägt auch Helfrich, 29 f., vor.

Abs. 2 lit. b und lit. c DSG resp. Art. 30 Abs. 2 lit. b und lit. c nDSG sogleich), ist die Begrifflichkeit geeignet, eine akkurate Titulierung der Grundsatzregelung für den privatrechtlichen Datenschutz zu liefern.

847 Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG regelt *nicht abschliessend* die allgemeinen Schranken der prinzipiell freien Personendatenverarbeitung, deren Missachtung eine Persönlichkeitsverletzung begründen. Damit ist es angezeigt, auch *Vorgaben ausserhalb des DSG* in die Betrachtung zu integrieren. In Erinnerung zu rufen sind datenschutzrechtlich zentrale, abweichende Bestimmungen, namentlich die *Geheimhaltungspflichten*, deren Verletzung strafbewehrt ist, vgl. insb. Art. 35 DSG und Art. 320 ff. StGB resp. Art. 62 nDSG.

848 Spezialgesetzliche Geheimhaltungspflichten betreffend den Umgang mit Personendaten korrigieren den gemäss DSG als Querschnittsgesetz gewählten Ausgangspunkt der prinzipiellen Verarbeitungsfreiheit für den privaten Bereich. Sie werden regelmässig als Verletzung des Rechtmässigkeitsprinzips, Art. 4 Abs. 1 DSG resp. Art. 6 Abs. 1 nDSG, präsentiert, womit sie über Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG in das persönlichkeitsrechtliche System einfliessen. Sie gelten insb. für Personen bestimmter Berufsgattungen wie der Ärzteschaft, Anwaltschaft usf. Gerade in den *kontext-, branchen- und bereichsspezifischen Geheimhaltungspflichten* – die sich als Ausnahmen der prinzipiell freien Datenbearbeitung mit Schranken gemäss DSG für den privaten Sektor lesen lassen und deshalb hier erwähnt werden – bestätigt sich die herausgearbeitete *dynamische, systemische sowie akzessorische Dimension* des Datenschutzrechts.[1121]

849 Geheimhaltungspflichten, wie sie *ausserhalb des DSG* statuiert werden, *derogieren die grundsätzlich freie Personendatenverarbeitung* im privaten Bereich mit Schranken für qualifizierte Verarbeitungen. Es genügt nicht, die Verarbeitung unter Einhaltung der allgemeinen Verarbeitungsgrundsätze vorzunehmen. Vielmehr bedarf es vorab einer Legitimation für die Bearbeitung, z. B. in Gestalt einer Einwilligung des Datensubjektes. Anders gewendet: Geheimhaltungspflichten schotten Datenflüsse für spezifische Bereiche bzw. Systeme ab resp. formulieren strengere Vorgaben an eine «Transmission». Geheimhaltungspflichten können somit als Staudämme beschrieben werden, die den Fluss von Personendaten aus einem System, in welchem die Personen in spezifischen Rollen agieren, beispielsweise als Ärztin und Patientin, in ein anderes System verhindern sollen. Damit ein entsprechender Personendatenfluss rechtmässig erfolgt, bedarf es der Erfüllung zusätzlicher datenschutzrechtlicher Vorgaben. In der Nomenklatur von Nissenbaum, die einen richtungsweisenden Beitrag zur Überdenkung datenschutzrecht-

1121 Herausgearbeitet im Rahmen der Analyse des Zweckbindungsgrundsatzes sowie der Argumentation im Volkszählungsurteil des Bundesverfassungsgerichts, vgl. zweiter Teil, V. Kapitel, 4.

licher Konzepte vorgelegt hat, handelt es sich bei den Geheimhaltungspflichten um eines von mehreren sog. *Transmissionsprinzipien*.[1122]

Mit diesem Terminus erfasst die Wissenschaftlerin die nuancierten Möglichkeiten zur Gestaltung von Informationsflüssen – Freiwilligkeit und Einwilligung, Gegenseitigkeit, Anonymisierung usf. –, wobei Transmissionsprinzipien definieren, unter welchen Bedingungen Personendaten von einer Partei zu einer anderen Partei eines bestimmten Kontextes transferiert werden sollen oder nicht.[1123] Die *ratio* von Geheimhaltungspflichten beschränkt sich indes nicht isoliert auf den Schutz der Persönlichkeit, wie im Rahmen der Analyse des Volkszählungsurteils und des Statistikgeheimnisses gezeigt wurde. Auch das Arztgeheimnis dient nicht einzig dem Schutz der Persönlichkeit des konkreten Patienten oder der Vertrauensbeziehung zwischen einer konkreten Ärztin und dem Patienten. Vielmehr dient dieses zugleich dem Schutz der Funktionstüchtigkeit, der Integrität des Gesundheitssektors selbst. Denn die ärztliche Versorgung und die Gesundheit als allgemeines Gut können nur dann effizient und sinnvoll sichergestellt werden, wenn Patienten vertrauensvoll ihre gesundheitlichen Themen mit der Ärztin teilen können.[1124] Wird dies nicht garantiert, riskiert man z. B., dass hochansteckende Krankheiten unbehandelt bleiben und sich ausbreiten, einzig und allein, weil jemand mangels Gewährleistung der Diskretion durch den Arzt eine Konsultation meidet. 850

Indem Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG ein nicht abschliessendes Regel-Ausnahme-Regime bezüglich der prinzipiellen Verarbeitungsfreiheit und ihrer Schranken sowie bezüglich der Persönlichkeitsverletzung vorsieht, wird erneut der Facettenreichtum des schweizerischen Datenschutzrechts – jeglicher Fokussierung auf die Persönlichkeitsverletzung und der Qualifizierung der «Basiskonstruktion» des DSG für den privaten Bereich als Integritätsschutz zum Trotz – in den Blick genommen. Kontextspezifische Geheimhaltungspflichten korrigieren die prinzipielle Verarbeitungsfreiheit gemäss DSG für den privaten Bereich und grenzen ausdifferenzierte Subsysteme im «privaten Bereich» aus informationeller Perspektive ab. Auch der «private Bereich» entpuppt sich als nicht als homogener Bereich. 851

Um das Bild zu vervollständigen, ist auf eine Entwicklung hinzuweisen, wie sie die jüngsten datenschutzrechtlichen Neuerungswellen bringen. Im Rahmen der Analyse von Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a DSG wurden mehrere Schwächen des materiellrechtlichen Kernstückes des DSG für den privaten Bereich thematisiert. Das generalklauselartige, in den Persönlichkeitsschutz eingebettete Regime lässt Griffigkeit vermissen. An diesem Defizit setzen die datenschutzrechtlichen Neuerungen an: Neu werden die Verarbeitenden *proaktiv in* 852

1122 Vgl. Nissenbaum, 145 f.
1123 Vertiefend zur Konstruktion sowie zum Konzept dritter Teil, IX. Kapitel.
1124 Vgl. Nissenbaum, insb. 171 ff., aber auch 159 f.

die Pflicht zur Einhaltung der Vorgaben genommen. Die DSGVO verankert explizit einen Ansatz der *Accountability*.[1125] Den Verarbeitenden werden umfassende Dokumentations- und Rechenschaftspflichten auferlegt. Sie müssen jederzeit belegen können, dass ihre Personendatenverarbeitungen *in Einklang mit den rechtlichen Vorgaben*, auch den allgemeinen Verarbeitungsgrundsätzen, stehen.

853 Gerade mit Blick auf die faktische Einhaltung der allgemeinen Verarbeitungsgrundsätze ist deshalb auch das neue Basisinstrument in Erinnerung zu rufen: Das Verarbeitungsverzeichnis, Art. 30 DSGVO resp. Art. 12 nDSG. Mit diesem wird die Landschaft der Verarbeitungsprozesse abgebildet. Es ermöglicht Transparenz sowie die Überprüfbarkeit der Verarbeitungsprozesse auf ihre Konformität mit den Verarbeitungsgrundsätzen und -vorgaben. Insofern werden an *erster Stelle* die Verarbeitenden in die Pflicht genommen. Parallel werden mit den neuen Datenschutzerlassen die behördlichen Prüfungs- und Interventionsmöglichkeiten ausgebaut.

854 Mit den skizzierten Neuerungen wird die im zivilrechtlichen Deliktsrecht, defensivrechtlich, abwehrrechtlich strukturierten Persönlichkeitsrecht basierende Konzeption bisheriger Datenschutzgesetzgebung in *markanter Weise ergänzt*. Der Datenschutzgesetzgeber fokussiert nicht mehr ausschliesslich auf die Eingriffs- und Verletzungshandlung sowie eine darauffolgende Abwehrhandlung des Datensubjektes in Gestalt eines zivil- und individualrechtlichen Rechtsschutzes wegen datenschutzrechtlicher Persönlichkeitsverletzung, vgl. hierzu Art. 15 DSG und Art. 32 nDSG. Vielmehr setzen die datenschutzrechtlichen Neuerungen früher an. Das Augenmerk richtet sich quasi vorgeschaltet verstärkt auf die Sicherstellung der Einhaltung der Verarbeitungsvorgaben, wofür die Verarbeitenden in der Pflicht stehen. Die Einhaltung des materiellrechtlichen Herzstückes des Datenschutzes wird abgesichert über mehrere neue Umsetzungsinstrumente.

855 Ein Verarbeitungsverzeichnis, das gerade auch die Konformität der Verarbeitungshandlungen mit den *allgemeinen und abstrakten Verarbeitungsgrundsätzen effektuiert*, ist dort von besonderer Relevanz, wo diese *allgemeinen Verarbeitungsgrundsätze* die einzige Schranke der prinzipiellen Verarbeitungsfreiheit darstellen, vgl. Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG. Im zweistufigen Regime der DSGVO dient das Verarbeitungsverzeichnis dazu, die Einhaltung *beider Schranken* – das Vorliegen eines Legitimationsgrundes sowie die Einhaltung der allgemeinen Verarbeitungsgrundsätze – zu gewährleisten und durch die Verarbeitenden wie durch die Behörden überprüfbar zu machen.

856 *Zusammenfassend* ist zu statuieren, dass Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8

1125 Vgl. Art. 24 und Art. 30 DSGVO.

nDSG einen *Integritätsschutz* implementiert. Für den privaten Bereich gilt gemäss DSG kein allgemeines Verarbeitungsverbot. Vielmehr findet die prinzipielle Verarbeitungsfreiheit ihre wichtigsten Schranken anhand der allgemeinen Verarbeitungsgrundsätze. Persönlichkeitsverletzend sind *qualifizierte Verarbeitungshandlungen*, mithin diejenigen, welche die allgemeinen Verarbeitungsgrundsätze, vgl. insb. Art. 4 DSG, aber auch Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG, resp. Art. 6 und Art. 8 nDSG missachten.

857 Die grosszügige Inklusion von Verstössen gegen Vorgaben des DSG in die nicht abschliessend enumerierten Tatbestände der Persönlichkeitsverletzung gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG bauen den Datenschutz *nur in theoretischer Hinsicht* aus. Weil Persönlichkeitsverletzungen durch qualifizierte Personendatenverarbeitungen nicht nur von den Datensubjekten kaum je festgestellt werden, ist über die Integration weiterer Verstösse gegen Datenschutzvorgaben in die Persönlichkeitsverletzung nicht viel gewonnen. An einem solchen konzeptionellen Schwachpunkt scheinen die datenschutzrechtlichen Neuerungen anzusetzen, welche konkrete Umsetzungsinstrumente vorsehen, wie das Verarbeitungsverzeichnis oder allgemeine Dokumentations- und Rechenschaftspflichten.[1126]

858 Mit ihnen vollzieht sich ein Perspektivenwechsel, denn der Fokus richtet sich nicht «erst» auf die «persönlichkeitsverletzende Datenverarbeitung». Vielmehr werden die Verarbeitenden *früher* durch *konkrete Umsetzungsinstrumente* in die Pflicht genommen, womit die Einhaltung der Datenschutzvorgaben effizienter gewährleistet werden soll. Ebendies ist für ein Regime von besonderer Bedeutung, das von einer prinzipiellen Verarbeitungsfreiheit ausgeht und die Schranken in erster Linie generalklauselartig definiert, vgl. Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG. In entsprechenden Neuerungen deutet sich ein Sichtwechsel an, indem primär die Verarbeitenden für ihre Handlungen in die Pflicht genommen werden. Neu sind verschiedene prozedurale und organisatorische Massnahmen durch diese zu ergreifen, um dem materiellrechtlichen Kernbestand des Datenschutzes proaktiv Nachachtung zu verschaffen. Die isolierte materiellrechtliche, persönlichkeitsrechtliche Fokussierung auf einen abwehr- und deliktsrechtlich gedachten Subjektschutz wird aufgeweicht resp. ergänzt. Das bisherige materiellrechtlich basierte Datenschutzrecht für den privaten Bereich lastete in erster Linie auf einem abwehrrechtlich begründeten Persönlichkeitsschutz. Neu wird der Schutz des Individuums auf organisatorische wie prozedurale Instrumente umgelagert, was auch der faktischen Verwirklichung der Verarbeitungsgrundsätze dienen soll.

1126 Hierzu dritter Teil, VIII. Kapitel, A.2.6.

859 Eine differenzierte Sicht auf das Schweizer Datenschutzregime wurde nicht nur anhand eines Blicks auf seine jüngsten Entwicklungen sichtbar. Vielmehr konnte bereits anhand des geltenden Regimes nach Art. 12 Abs. 2 lit. a DSG die hohe Differenziertheit des Gesetzes nachgewiesen werden. Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG schaffen zwar die *Grundsatzkonstruktion* des schweizerischen Datenschutzrechts. Sie verankern für den privaten Bereich die prinzipielle Verarbeitungsfreiheit mit Schranken in den allgemeinen Verarbeitungsgrundsätzen, deren Missachtung eine Persönlichkeitsverletzung begründen. Dieser sog. «Integritätsschutz» findet seine wohl einschlägigste Abweichung in spezifischen Geheimhaltungspflichten. Die bereichs- und kontextspezifischen Geheimhaltungspflichten, welche die prinzipielle Verarbeitungsfreiheit des DSG durchbrechen, zeigen eindrücklich, dass das schweizerische Datenschutzrecht keineswegs isoliert die Person vor unfairen Verarbeitungshandlungen schützt. Vielmehr zielen solche, die Basiskonstruktion des DSG derogierende Geheimhaltungspflichten über den Schutz der Person hinausgehend auf den Schutz der Funktionstüchtigkeit resp. Integrität spezifischer gesellschaftlicher Bereiche, beispielsweise des Gesundheitsbereiches, ab. Gleichwohl sind Art. 12 Abs. 2 lit. a DSG, weniger ausgeprägt Art. 30 Abs. 2 lit. a nDSG, als Kernbestimmungen und Basiskonstruktionen des DSG zu sehen, indem die Schranken der grundsätzlichen Verarbeitungsfreiheit durch allgemeine Verarbeitungsgrundsätze markiert werden, deren Missachtung eine Persönlichkeitsverletzung begründet. Für diese datenschutzgesetzliche Basiskonstruktion des privaten Bereichs wird die Charakterisierung als *Integritätsschutz* vorgeschlagen.

2.2.2. lit. b – Widerspruchslösung

860 Eine Persönlichkeitsverletzung liegt nach dem allgemeinen Regime des DSG für den privaten Bereich zudem dann vor, *wenn Personendaten entgegen dem ausdrücklichen Willen der betroffenen Person bearbeitet werden*. Die noch geltende Fassung gemäss Art. 12 Abs. 2 lit. b DSG integriert den Passus «ohne Rechtfertigungsgrund» und wählt die Formulierung «entgegen dem ausdrücklichen Willen».

861 Mit der Totalrevision wird auf die Integration der Rechtfertigungsgründe in Art. 30 Abs. 2 lit. b nDSG verzichtet: Während sich Art. 30 nDSG konsequent mit der Tatbestandsmässigkeit befasst, sind die Rechtfertigungsgründe in Art. 31 nDSG niedergelegt. Der «zivilrechtliche resp. individualrechtliche» Rechtsschutz für den Datenschutz im privaten Bereich findet sich in Art. 32 nDSG. Neu wird in Art. 30 Abs. 2 lit. b nDSG von einer der Personendatenbearbeitung «entgegengestellten ausdrücklichen Willenserklärung» gesprochen. Nachfolgend wird nicht im Detail auf die mit der Totalrevision einhergehenden Veränderungen in Bezug

auf die Anforderungen betreffend einen gültigen Widerspruch eingegangen. Die Neuerungen im Zusammenhang mit den Willenserklärungen, welche die Totalrevision bringt, bedürfen einer eigenständigen Untersuchung. An dieser Stelle erfolgt eine konzeptionelle Analyse, um Erkenntnisse für den in dieser Studie entwickelten Paradigmenwechsel zu generieren.

862 Mit Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG findet der *Wille des Datensubjektes* in die allgemeine Datenschutzgesetzgebung Eingang. Gleichwohl handelt es sich dabei namentlich nach Totalrevision des DSG nicht um die einzige Norm, die an diesem subjektiven Element, dem Willen des Datensubjektes, anknüpft.

863 Nach Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG führt eine Verarbeitung entgegen einem *Widerspruch des Datensubjektes zu einer Persönlichkeitsverletzung*. Eine *Persönlichkeitsverletzung* liegt gemäss Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG dann vor, wenn eine Datenbearbeitung *gegen den ausdrücklichen Willen* (resp. neu entgegen ausdrücklicher Willenserklärung) der betroffenen Person erfolgt. Allerdings kann diese gerechtfertigt werden, sofern Rechtfertigungsgründe ausserhalb des Willens des Datensubjektes dessen Widerspruch überwiegen, vgl. Art. 13 DSG resp. Art. 31 nDSG.

864 Diese *Widerspruchslösung* für den privaten Sektor im schweizerischen DSG ist eine logische Folge des gewählten Ansatzes. Sie ist eine *konsequente Umsetzung des gewählten Ausgangspunktes der Freiheit der Datenbearbeitung*, die beschränkt wird: Dies geschieht basierend auf die lit. b der besagten Bestimmungen aufgrund eines Widerspruchs des Datensubjektes.

865 Die Widerspruchslösung dürfte durchaus als Selbstbestimmungsansatz qualifiziert werden. Denn mit ihr wird der Wille des Datensubjektes zu einem Kriterium der (un)zulässigen Personendatenverarbeitung. Gleichwohl ist zu betonen, dass das Recht auf informationelle Selbstbestimmung untrennbar mit dem Volkszählungsurteil des Bundesverfassungsgerichts einhergeht. Mit einem «Recht auf informationelle Selbstbestimmung», bei welchem der Widerspruch die prinzipielle Verarbeitungsfreiheit durchbricht, ist ein *anderes Konzept verbunden,* als es mit dem im Volkszählungsurteil geprägten Grundrecht auf informationelle Selbstbestimmung der Fall ist. In beiden Konstruktionen kommt zwar dem Willen resp. der Selbstbestimmung des Datensubjektes Relevanz zu. Nach DSGVO sowie verfassungsgerichtlicher Rechtsprechung allerdings bildet die Einwilligung einen Erlaubnistatbestand zur Durchbrechung eines prinzipiellen Verarbeitungsverbotes. Die strukturellen Differenzen wurden in der Schweiz lange nicht hinreichend gewürdigt. Erst die intensivierte Auseinandersetzung, wie sie von den datenschutzrechtlichen Neuerungswellen angestossen wurde, führt zu treffliche-

ren Beschreibungen des Konzepts des DSG. Insofern ist auch auf die Studie von Fasnacht aus dem Jahr 2017 hinzuweisen.[1127]

866 Die «informierte Einwilligung» hat in Europa nicht nur im Datenschutzrecht Hochkonjunktur, sondern ebenso im Bereich des (Bio-)Medizinrechts.[1128] Anders gewendet: Juristisch gewinnt ein Konzept der Selbstbestimmung dort an Einfluss, wo es um die Emanzipation des Menschen von den Technologien geht. Fasnacht gibt unter dem Titel «Datenschutzgrundrecht» und Art. 13 Abs. 2 BV einen systematischen Überblick über das weite Spektrum an Auslegungen – von Missbrauchsordnungen bis zum Recht auf informationelle Selbstbestimmung.[1129] Im Ergebnis schliesst er sich der Ansicht an, wonach Art. 13 Abs. 2 BV als Recht auf informationelle Selbstbestimmung zu lesen sei: «Der Einzelne soll grundsätzlich selbst bestimmen können, wer seine Personendaten wie bearbeitet.»[1130] Da es sich um ein Grundrecht handle, das bekanntlich nicht direkt im Privatrecht gelte, entfalte das Recht auf informationelle Selbstbestimmung gemäss Art. 35 BV über den zivilrechtlichen Persönlichkeitsschutz Wirkung. Die datenschutzrechtliche Einwilligung fungiere hier als Rechtfertigungsgrund: Sie rechtfertige eine Persönlichkeitsverletzung.[1131] Die Aussage ist nicht falsch. Sie expliziert indes die konzeptionellen Differenzen in Bezug auf die Rolle des Willens des Datensubjektes nicht hinreichend. Hierzu daher einige klärende Ausführungen.

867 Das Volkszählungsurteil des Bundesverfassungsgerichts hat die datenschutzrechtlichen Entwicklungen in Deutschland, ja in Europa nachhaltig geprägt.[1132] Hervorzuheben sind *zwei Aspekte*: Erstens hat das Volkszählungsurteil verfassungsrechtliche Vorgaben für den Umgang mit *Personendaten im öffentlichen Bereich*, also durch *staatliche Stellen*, formuliert. Zweitens wurde mit dem Volkszählungsurteil und seinen Ausführungen zum Recht auf informationelle Selbstbestimmung ein Systemwechsel vollzogen: Ein bisher auf die Verhinderung von missbräuchlichen Personendatenverarbeitungen gerichteter Datenschutz wurde

1127 Fasnacht, *passim*; zur datenschutzrechtlichen Einwilligung auch Heuberger, N 267 ff.; allgemein zur Einwilligung im System des Persönlichkeitsschutzes gemäss Art. 28 ZGB Haas, *passim*; zu rechtsdogmatischen Fragen der rechtfertigenden Einwilligung vgl. Kothe, AcP 1985, 105 ff.

1128 Vgl. Barocas/Nissenbaum in ihren verschiedenen Beiträgen; zur informierten Einwilligung als Ausdruck des verfassungsrechtlich verbürgten Selbstbestimmungsrechts im Kontext des Biomedizinrechts eine Übersicht über die Lehrmeinungen Karavas, Körperverfassungsrecht, 222 ff.; zur Frage, ob Selbstbestimmung im Zeitalter der Biotechnologie überhaupt möglich ist, vgl. Fateh-Moghadam, BJM 2018, 215 ff.; zur informierten Einwilligung gemäss DSG insb. Bühlmann/Schüepp, Jusletter vom 15. März 2021; Vasella, Jusletter vom 16. November 2015.

1129 Fasnacht, N 96 ff.

1130 Ders., N 206.

1131 Ders., N 217 ff.

1132 Vgl. Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 27 ff., der das Urteil als Zäsur beschreibt; Buchner, 31 f.; kritisch zur Staatszentrierung Vesting, in: Ladeur (Hrsg.), 155 ff.

ersetzt durch ein prinzipielles Verarbeitungsverbot mit Schranken.[1133] Der Schutz von Personendaten wurde zur Regel, der staatliche Zugriff zur Ausnahme. Gesetzgeberisch umgesetzt mündete dies in ein grundsätzliches Verarbeitungsverbot mit Erlaubnistatbeständen.[1134]

Heute wird dieses Regime des prinzipiellen Verarbeitungsverbots mit Erlaubnistatbeständen in der DSGVO *gleichermassen* für Personendatenverarbeitungen durch öffentliche Stellen *wie private Verantwortliche vorgesehen, vgl. Art. 6 DSGVO*. Jegliche Personendatenverarbeitung, nicht nur die qualifizierte, bedarf eines Erlaubnistatbestandes. Zudem sind die Verarbeitungsgrundsätze gemäss Art. 5 DSGVO sowie weitere neuen Vorgaben einzuhalten. Die Gültigkeit des Prinzips des Verarbeitungsverbotes mit Erlaubnistatbestand, wie es ursprünglich für den öffentlichen Bereich entwickelt wurde, wird auf den privaten Bereich ausgedehnt. Mangels anderweitigen Ermächtigungsgrundes fällt als Erlaubnistatbestand für die Personendatenverarbeitung gemäss Art. 6 Abs. 1 lit. a DSGVO die *Einwilligung* der betroffenen Person in Betracht. Gleichzeitig operiert auch die DSGVO mit dem Instrument des Widerspruches, mittels dessen eine aufgrund eines anderen Erlaubnistatbestandes vorab legitimierte Personendatenverarbeitung qua Widerspruch des Subjektes zu einer unrechtmässigen Verarbeitung wird: So hat die Kommission Personendatenverarbeitungen zum Direktmarketing als «legitimate interest» im Sinne von Art. 6 Abs. 1 lit. f DSGVO anerkannt.[1135] Die in diesem Sinne zulässige Personendatenverarbeitung kann indes durch einen Widerspruch des Datensubjektes verboten werden. Folglich wird eine Personendatenverarbeitung zum Zwecke des Direktmarketings definitiv unzulässig. 868

Ebendies entspricht nicht dem Ansatz des DSG, auch nicht nach seiner Totalrevision. Die Einwilligung figuriert gemäss DSG im privaten Bereich gerade nicht als Erlaubnistatbestand für prinzipiell verbotene Verarbeitungshandlungen. Vielmehr dreht das Widerspruchsrecht gemäss Art. 12 Abs. 2 lit. b DSG resp. Art. 30 869

1133 Vgl. Buchner, 27 ff., insb. 43; von Gallwas, NJW 1992, 2785 ff., 2788 ff. wird der entscheidende Wandel darin verortet, dass das Subjekt mit der Anerkennung eines Rechts auf informationelle Selbstbestimmung grundsätzlich Herr über die es betreffenden Personendaten ist, ihm ein prinzipielles Entscheidungsrecht zusteht; Eberle, in: Wilhelm (Hrsg.), 113 ff., 114 ff., der vom Prinzip «in dubio pro securitate» spricht, weil prinzipiell jede Personendatenverarbeitung als Gefährdung des Persönlichkeitsrechts taxiert wird; die vom Autor präsentierte These, wonach das Grundrecht auf informationelle Selbstbestimmung erst aus dem jeweiligen Gesellschaftsbereich heraus seine Struktur erhalte, stiess auf Widerstand, vgl. ebenda, 123.

1134 Vgl. Buchner, 43.

1135 Hierzu dritter Teil, VIII. Kapitel, A.; erläuternd zur Direktwerbung auch die Orientierungshilfe der deutschen Datenschutzkonferenz (DSK), abrufbar unter: <https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Entschliessungen_Datenschutzkonferenz/Inhalt/96_-Konferenz/Orientierungshilfe-der-Aufsichtsbehoerden-zur-Verarbeitung-von-personenbezogenen-Daten-fuer-Zwecke-der-Direktwerbung-unter-Geltung-der-Datenschutz-Grundverordnung-_DS-GVO_/OH_Werbung_Stand_07_11_2018.pdf> (zuletzt besucht am 30. April 2021); zur Direktwerbung als datenschutzrechtlich relevante Form der Werbung früh Schineis, 119 ff.

Abs. 2 lit. b nDSG den gesetzgeberischen Entscheid für die prinzipielle Verarbeitungsfreiheit einzelfallbezogen in ein Verbot um.[1136]

870 Unbestritten wird mit einem Widerspruch ebenso ein «Selbstbestimmungsrecht» des Datensubjektes adressiert. Es handelt sich indes nicht um das identische Konzept, wie es mit dem Volkszählungsurteil des Bundesverfassungsgerichts hervorging und wie es heute gemäss DSGVO auch für den privaten Bereich gilt. Ein «Recht auf informationelle Selbstbestimmung» ist untrennbar mit dem Volkszählungsurteil des Bundesverfassungsgerichts und dessen Gehalt verknüpft. Eine Folgerung war die Implementierung eines prinzipiellen Verarbeitungsverbotes mit Erlaubnisvorbehalten.

871 Somit überzeugt es nicht, wenn für das schweizerische Datenschutzrecht pauschal für den privaten Bereich vom Recht auf informationelle Selbstbestimmung gesprochen wird.[1137] Die konzeptionellen Unterschiede werden damit ignoriert, zumal es die Einwilligung ist, die genuin mit dem Recht auf informationelle Selbstbestimmung assoziiert wird.[1138] Zugleich wird ein Rechtsbestand suggeriert, der so im schweizerischen Datenschutzrecht nicht gewährleistet wird. In der Schweiz kommt gemäss Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG dem Widerspruch (und gerade nicht der Einwilligung), entsprechend dem Konzept der Freiheit der Datenbearbeitung, die Funktion eines *Verbotstatbestandes* zu. Immerhin: Auch in der Schweiz weisen Spezialbestimmungen der Einwilligung die Funktion eines Erlaubnistatbestandes zu, insb. die beruflichen Geheimhaltungspflichten. Weiter ist der Wille des Datensubjektes als Rechtfertigungsgrund relevant, Art. 13 Abs. 1 DSG und Art. 31 Abs. 1 nDSG, insb. bei persönlichkeitsverletzenden Handlungen nach Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG.

872 Die Schweiz integriert folglich den *Willen des Datensubjektes in nuancierter Weise* in das DSG. Dies geschieht indes *nicht* in Gestalt eines Erlaubnistatbestands für dem Grundsatz nach verbotene Personendatenverarbeitungen. Wenn das Datensubjekt mit einem Widerspruch nach Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG die grundsätzlich erlaubte Personendatenverarbeitung *verbieten* kann, mag man darin die Verbürgung eines «Selbstbestimmungsrechts» se-

1136 Vgl. für Deutschland dazu, dass primär der Gesetzgeber aufgerufen ist, zwischen einem Verbot mit Einwilligungsvorbehalt und einer Erlaubnis mit Widerspruchsmöglichkeiten zu entscheiden, Ohly, 195.

1137 Ungeachtet dieser grundlegenden Differenzen ist eine Praxis zu problematisieren, unter der gewissermassen zur Sicherheit die datenschutzrechtliche Einwilligung eingeholt wird, obschon eine Verarbeitungshandlung dieser nicht bedürfte. Nach DSGVO für den Fall, dass ein anderweitiger Legitimationsgrund vorliegt, nach DSG für den Fall, dass die Personendatenverarbeitung innerhalb der Schranken stattfindet. Die datenschutzrechtliche Einwilligung zur «Sicherheit» einzuholen, ist problematisch, da sie eine «Selbstbestimmung» des Datensubjektes suggeriert, obschon die Verantwortlichen auch ohne diese verarbeiten dürften.

1138 Vgl. Radlanski, 271.

hen. Dies mit dem Argument, dass es im Ergebnis das Datensubjekt ist, das mittels Verbotes darüber entscheidet, wer welche Personendaten über es bearbeitet. Mehrere Punkte sind zu ergänzen:

Erstens besteht – wie gesagt – eine markante Differenz zwischen einem Recht auf informationelle Selbstbestimmung, das mittels eines Systems des grundsätzlichen Verarbeitungsverbotes umgesetzt wird, und einem System der grundsätzlichen Verarbeitungsfreiheit mit Schranken und darin eingebetteter Widerspruchslösung. Es handelt sich – konsequent implementiert – um diametral auseinandergehende Ansätze. 873

Diese Klarstellung wird anhand eines *Exkurses* in das Transplantationsrecht erhärtet: Das Zustimmungserfordernis ist fester Bestandteil des Transplantationsgesetzes, vgl. insb. Art. 5, Art. 8 Abs. 2, Art. 13 Abs. 3, Art. 39 f., Art. 48 Abs. 1 Ziff. 1 und Ziff. 2 Transplantationsgesetz.[1139] Organe oder sonstige Körpersubstanzen zu Transplantationszwecken zur Verfügung zu stellen, bedarf in der Schweiz *de lege lata* der erklärten, informierten Einwilligung des «Organträgers». Dies kann beispielsweise durch einen Spenderausweis dokumentiert werden. Die Knappheit an Spenderorganen hat hierzulande die Debatte um die Abkehr vom Zustimmungsmodell und die Hinwendung zu einem Widerspruchsmodell ausgelöst. Sie setzte sich nicht durch: Der Nationalrat schloss sich einer Empfehlung des Bundesrates an und verwarf am 5. März 2015 eine entsprechende Änderung.[1140] Damit werde – so der Fernsehbericht – auf einen Systemwechsel verzichtet.[1141] Im Bereich des Transplantationsrechts wird selbst in der allgemeinen Medienberichterstattung und nicht nur in der Fachliteratur der *grundlegende Unterschied zwischen einer Einwilligungs- und der Widerspruchslösung* unmissverständlich thematisiert. 874

Ganz anders im Bereich des Datenschutzgesetzes, wo diese Systemdifferenz lange nicht adäquat erfasst wurde. Ein Systemwechsel, wie er in der Schweiz für das Transplantationsgesetz diskutiert wurde – wenn auch in die entgegengesetzte Richtung –, stand hierzulande selbst mit der Totalrevision des DSG nicht zur Debatte. Er wurde nicht diskutiert, obschon mit ihm eine Annäherung an die 875

1139 Bundesgesetz über die Transplantation von Organen, Geweben und Zellen vom 8. Oktober 2004, SR 810.21.

1140 Parlament, Transplantationsgesetz, Teilrevision, Bern 2015, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20130029> (zuletzt besucht am 30. April 2021); vgl. Tagesanzeiger, Parlament lehnt automatische Organspende ab, Zürich 2015, <https://www.tagesanzeiger.ch/schweiz/standard/Parlament-lehnt-automatische-Organspende-ab/story/26647013> (zuletzt besucht am 30. April 2021).

1141 SRF, Organspende: Nationalrat gegen Widerspruchslösung, Zürich 2015, <http://www.srf.ch/news/schweiz/session/organspende-nationalrat-gegen-widerspruchsloesung> (zuletzt besucht am 30. April 2021).

DSGVO erreicht werden sollte. Letztere sieht für den privaten Bereich das prinzipielle Verarbeitungsverbot vor, vgl. Art. 6 DSGVO.[1142]

876 *Zweitens*: In einem System mit Ausgangspunkt der Verarbeitungsfreiheit mit Widerspruchslösung ist die *Erkennbarkeit der Datenverarbeitung* und damit die Transparenz notwendige Vorbedingung der Funktionstüchtigkeit einer Widerspruchslösung. Theoretisch und formalgesetzlich greifen insofern Grundsätze der Transparenz resp. Erkennbarkeit, wobei eine Vorgabe der angemessenen Informierung über ein Widerspruchsrecht ebenso anerkannt wird.[1143] Dessen ungeachtet können mit Blick auf die datenschutzgesetzliche Widerspruchslösung die *faktischen Rahmenbedingungen und damit die datenschutzrechtliche Realität* nicht ausgeblendet werden: Kaum ein Datensubjekt überschaut, wer wann welche Personendaten über es verarbeitet. Hieran werden auch die mittels Totalrevision ausgebauten Informations- und Transparenzvorgaben nicht viel ändern. Zwar wird über viel mehr informiert werden, doch die Informiertheit der Datensubjekte wird damit nicht zwangsläufig angehoben. Somit dürfte in Bezug auf die Transparenz, die das Widerspruchsrecht faktisch effektuieren soll, von Defiziten ausgegangen werden.[1144] Das Widerspruchsrecht bleibt bei Lichte betrachtet über weite Strecken eine kühne Fiktion.[1145]

877 *Drittens* soll – entgegen einem Widerspruch des Datensubjektes – eine Verarbeitung gleichwohl zulässig sein, sofern hierfür ein anderweitiger Rechtfertigungsgrund vorliegt.[1146] Dies dürfe zwar nur ganz ausnahmsweise der Fall sein.[1147] Weil indes namentlich das konturlose überwiegende Interesse oftmals die beschränkende Wirkung vermissen lässt, schwächt das Schweizer Recht die Bedeutung des Willens des Datensubjektes in Gestalt eines Widerspruchs ab. Es wäre angezeigt, dass der *Gesetzgeber selbst* entsprechende, einen *Widerspruch* übertrumpfende Interessen *konkreter definiert* würde.[1148]

878 Die Widerspruchslösung und ihre konkretisierende, einbettende Rechtsgestaltung ist folglich kein Garant und Regime, das eine Titulierung als «Recht auf informationelle Selbstbestimmung» in überzeugender Weise trägt. Dies gilt *a fortiori* in Anbetracht der Unübersichtlichkeit durchgeführter Datenbearbeitungen in einem

1142 Botschaft 2017–1084, 1 ff., 3 ff.
1143 Hierzu Rosenthal, HK-DSG, Art. 12 N 26.
1144 Vertiefend zum Vollzugsdefizit dritter Teil, VII. Kapitel, A. und B.; zur mangelnden Effektivität vgl. Simitis, Symposium, 1 ff.
1145 Ein Befund, der übrigens ebenso für die informierte Einwilligung gilt, vgl. insofern vertiefend dritter Teil, VIII. Kapitel, A.4.2.2.
1146 Vgl. Art. 12 Abs. 2 lit. b DSG, der explizit die Rechtfertigung zulässt; Rampini, BSK-DSG, Art. 12 N 13.
1147 Vgl. BGE 136 III 508, Regeste.
1148 Nach DSGVO gilt gemäss Kommission das Direktmarketing als «legitimate interest» und Erlaubnistatbestand. Ein Widerspruch des Datensubjektes allerdings macht eine entsprechende Verarbeitung per se verboten; eine wiederum übertrumpfende Rechtfertigung ist nicht denkbar.

System mit prinzipieller Verarbeitungsfreiheit, der Tatsache defizitärer Rechtseinhaltung ebenso in Bezug auf die Transparenz sowie eine Rechtslage, wonach ein Widerspruch durch gesetzlich nicht präzis umrissene «überwiegende Interessen» beiseitegeschoben werden kann.

879 Unter dem Titel des Widerspruchsrechts sind abrundend die Anglizismen «*opt-out*» und «*opt-in*» zu thematisieren.[1149] Das Begriffspaar *opt-in und opt-out* wird zur Systembezeichnung für das Einwilligungs- oder Widerspruchsmodell, womit der jeweils gewählte prinzipielle Ausgangspunkt korrigiert wird, verwendet.[1150] Für diese konzeptionellen Grundsatzdimensionen wird die Bezeichnung *opt-in und opt-out im weiteren Sinne* vorgeschlagen.[1151] Das Begriffspaar von *opt-out und opt-in im engeren Sinne* adressiert damit zusammenhängend die Art und Weise, wie eine datenschutzrechtliche Willenserklärung *formularmässig* erklärt wird resp. wie ein (elektronisches) Formular auszugestalten ist.[1152]

880 Das Schweizer System wird neuerdings regelmässig als eines des *opt-out* beschrieben.[1153] Mit Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG dürfte es als *opt-out im weiteren Sinne* zu qualifizieren sein. Weil selbst der Widerspruch im Rahmen des Systems prinzipieller Verarbeitungsfreiheit mit Schranken «übertrumpft» werden kann, sollte das Regime des DSG für den privaten Bereich präzisierend als ein *relatives opt-out im weiteren Sinne taxiert werden.* Die *Widerspruchslösung* gemäss DSG verlangt die *ausdrückliche* Erklärung, was m. E. ein aktives Verhalten bedingt. Ein konkludentes oder passives Verhalten scheint nicht geeignet, um einen gültigen Widerspruch anzubringen. In diesem Zusammenhang ist zudem zu beachten, dass die datenbearbeitenden Stellen einen Hinweis auf das Widerspruchsrecht anzubringen haben, womit dessen Wahrnehmung in angemessener Weise durch die betroffene Person eingeräumt wird.[1154]

881 Für *Rechtsordnungen mit Einwilligungsmodell und -erfordernis* werden hinsichtlich formulartechnischer Gestaltungsmöglichkeiten verschiedene Versionen diskutiert: Als *opt-in im engeren Sinne* wird im elektronischen Kontext eine Erklärungsmodalität bezeichnet, in welcher neben dem einschlägigen Text ein Kästchen angebracht ist, das leer ist. Das Datensubjekt hat durch aktives Setzen eines Häkchens seine Einwilligung zu erklären. Das *opt-out im engeren Sinne* dagegen erfolgt dergestalt, dass eine Checkbox leer ist und das Leerlassen als «vermutete

1149 Insofern auch Buchner, DuD 2015, 402 ff., 403; Fasnacht, N 398 ff.; hierzu ebenso Langhanke, 65 ff.; sodann Hoeren, LMK 2008, 65 f.
1150 Hierzu Radlanski, 18; für dieses System Art. 6 DSGVO.
1151 Ders., 18 f.
1152 Zum Ganzen Rogosch, 32 ff., 132; Radlanski, 19, m. w. H.; Heuberger, N 189 ff.; Fasnacht, N 398 ff.; Buchner, DuD 2010, 52.
1153 So Hussein, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.114; Fasnacht, N 402 ff.
1154 Vgl. Rosenthal, HK-DSG, Art. 12 N 26.

Einwilligung» gilt. Das Setzen eines Häkchens gilt als verweigerte Einwilligung. Es finden sich auch Mischformen. Einschlägiges Kriterium für die Qualifizierung ist das Aktivwerden des Datensubjektes im Rahmen seiner Einwilligungserklärung, wobei nur das Tätigwerden der betroffenen Person als *opt-in im engeren Sinne* gilt.[1155]

882 Die Unterscheidung von *opt-in und opt-out im engeren Sinne* ist nicht bloss begrifflicher oder theoretisch-formeller Natur. Sie ist hoch relevant aufgrund eines statistisch belegten Befundes: Demnach verhält sich ein grosser Teil der Menschen gerade im Internet hinsichtlich Formulareinwilligungen *passiv*: Eine Voreinstellung wird in aller Regel nicht geändert.[1156] Anders gewendet bedeutet dies, dass eine Einwilligung *proaktiv* deutlich seltener erteilt wird als eine *passive Einwilligung*, bei der die «Einwilligung» voreingestellt ist und das Datensubjekt diese aktiv beseitigen müsste. Vor diesem Hintergrund erstaunt nicht, dass im Anwendungsbereich der DSGVO verlangt wird, dass Verantwortliche die «erteilte Einwilligung» nachweisen können müssen, wobei es einer bestätigenden Handlung bedarf. Sie wird elektronisch durch *Anklicken* eingeholt.[1157]

883 Die Herausforderungen von Einwilligungskonstruktionen erschöpfen sich indes nicht darin. Denn selbst bei ausdrücklich zu erteilenden Zustimmungen zeichnet sich ab, dass diese oft rein *schematisch* erfolgen. Die Erfüllung der Gültigkeitsvoraussetzungen – Informiertheit und Freiwilligkeit – stehen damit auf dem Spiel. Die Situation präsentiert sich dergestalt, dass die unmittelbar verfolgten Interessen resp. das primäre Ziel, aufgrund dessen das Datensubjekt beispielsweise das Internet nutzt – Bestellung einer Sache, Suche nach Informationen –, mittelbare Interessen gänzlich absorbieren und datenschutzrechtliche Erwägungen verdrängen. Wer im Internet ein Hotel betrachten möchte, will nicht Einwilligungserklärungen studieren; wer ein Buch bestellen will, klickt sich durch die datenschutzrechtlichen Erfordernisse durch, um dieses Ziel möglichst effizient zu erreichen. Paradoxerweise rückt damit faktisch die von den Menschen erklärte hohe Bedeutung, die sie dem Datenschutz zuweisen, in den Hintergrund.

884 Damit ist ein datenschutzrechtlicher Brennpunkt offensichtlich: Die Tragfähigkeit von Einwilligungskonstruktionen als Lösungsansatz für datenschutzrechtliche Herausforderungen wird – obschon gesetzgeberisch eine Kernstrategie – kritisch beleuchtet.[1158] Entsprechende Studien stammen aus Rechtskreisen mit jeweils an-

1155 M. w. H. Radlanski, 19.

1156 Rogosch, m. w. H., 13; Buchner, DuD 2010, 39 ff. und DuD 2010, 52; Radlanski, 20; vgl. zur Ineffizienz von Opt-out-Lösungen im Internet Solove, Stan. L. Rev. 2001, 1393 ff., 1458.

1157 Jüngst insofern DSK, Kurzpapier Nr. 20, Einwilligung nach der DSGVO, <https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz-Grundverordnung/Kurzpapiere_der_DSK_als_Auslegungshilfen_zur_DSGVO/DSK_KPNr_20_Einwilligung.pdf> (zuletzt besucht am 30. April 2021).

1158 Insb. durch Nissenbaum sowie Barocas/Nissenbaum, aber auch Radlanski.

derem Regime als dem schweizerischen – aus Deutschland und den USA. Mit der Berücksichtigung ihrer Erkenntnisse kann unter Umständen der Umweg über ein nicht effektives Rechtsinstrumentarium (namentlich: Selbstbestimmungs- resp. informed consent-Lösungen) vermieden werden. Vorab ist indes das Bild des schweizerischen datenschutzgesetzlichen Systems zu vervollständigen.

2.2.3. lit. c – Sphärentheoretische Relikte

Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG werden primär konzeptionell dargelegt. Anknüpfend an die Analyse zu Art. 12 Abs. 2 lit. a und lit. b DSG resp. Art. 30 Abs. 2 lit. a und lit. b nDSG lässt sich einleitend feststellen, dass Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG die beiden beleuchteten Regelungsansätze bestätigen: Nach DSG für den privaten Bereich begründet erst die *qualifizierte Verarbeitungshandlung* eine Persönlichkeitsverletzung. Gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG erfolgte die Qualifizierung anhand der Verarbeitungs*handlung,* die *grundsatzwidrig vorgenommen wurde.* Das Qualifizierungsmerkmal ist ein *objektives*. In Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG erfolgt die Qualifizierung durch den *Widerspruch*, womit das subjektive Qualifizierungskriterium greift. Das Qualifikationskriterium gemäss Art. 12 Abs. 2 lit. c DSG wird primär in einer bestimmten *«Natur und Kategorisierung von Personendaten»* verortet: Es geht um besonders schutzwürdige Personendaten oder Persönlichkeitsprofile, Art. 3 lit. c und lit. d DSG, wobei diese *Dritten* nicht bekannt gegeben werden dürfen. Art. 12 Abs. 2 lit. c DSG erklärt somit eine spezifische Verarbeitungshandlung, die *Weitergabe* von *besonders schutzwürdigen Personenangaben* oder *Persönlichkeitsprofilen an Dritte*, vgl. Art. 3 lit. c und lit. d DSG, als persönlichkeitsverletzend. Mit der Totalrevision wird das sog. Persönlichkeitsprofil fallen gelassen. Stattdessen werden das Profiling und die automatisierte Einzelfallentscheidung eingeführt, worauf nicht spezifisch eingegangen wird. Art. 30 Abs. 1 lit. c nDSG beschränkt sich neu auf besonders schutzwürdige Personenangaben i. S. v. Art. 5 lit. c nDSG. 885

Die Kategorie der sog. «besonders schutzwürdigen Personendaten» hat eine lange Tradition. Seit jeher knüpfen datenschutzrechtliche Erlasse an die Verarbeitung solcher spezifischer Personendaten erhöhte Schutzvorgaben, wobei die Kataloge sowie die hieran angeknüpften rechtlichen Konsequenzen teilweise variieren.[1159] Das DSG misst bestimmten Personendaten eine spezifische Qualität i. S. einer erhöhten Sensitivität zu, womit ein grösseres Risiko für die Beeinträch- 886

1159 Vgl. Art. 3 lit. c DSG und nach Totalrevision ergänzt Art. 5 lit. c Ziff. 1–Ziff. 6 nDSG; Art. 6 der Europarats-Konvention Nr. 108; zur Definierung spezifischer Personendaten, ohne von besonders schützenswerten Daten zu sprechen, Art. 4 Ziff. 13–Ziff. 15 DSGVO.

tigung der Persönlichkeit und Grundrechte korreliert wird. Folglich sieht das Gesetz besondere Schutzvorkehrungen vor.[1160] Während im öffentlichen Bereich die rechtmässige Verarbeitung einer gesetzlichen Grundlage im formellen Sinne bedarf, liefern die besonders schützenswerten Personendaten im privaten Bereich ein Anknüpfungskriterium für die Definierung der Persönlichkeitsverletzung, sofern diese Dritten weitergegeben werden. In Bezug auf die Kategorie werden mehrere Begründungsansätze und Herangehensweise beschrieben.[1161]

887 Indem das DSG nicht jede Verarbeitung qualifizierter Personendaten oder Personendatenbestände verbietet, hält es konsequent an seinem Grundsatzentscheid der prinzipiell freien Personendatenverarbeitung fest. Es rückt von diesem nur für eine spezifische *Verarbeitungshandlung, die «Bekanntgabe an Dritte», ab*. Damit vereint die Bestimmung *mehrere Facetten*:

888 Vorab findet sich das *traditionsreiche Konzept einer abstrakten und statisch angelegten Sphärentheorie*. Demnach soll bestimmten Personendaten abstrakt eine spezifische Qualität eigen sein. Gewisse Angaben gelten, wenn auch in Art. 3 lit. c DSG resp. Art. 5 lit. c nDSG aufgeführt, quasi naturgegeben und abstrakt als intim, persönlich, privat, sensitiv oder – in den Worten des DSG – «besonders schutzwürdig».[1162] Folglich implementiert das DSG für solche Angaben ein spezifisches Regime. Die *Weitergabe* von *besonders schutzwürdigen Daten* (und DSG vor seiner Totalrevision: Persönlichkeitsprofilen) an *Dritte* gilt als Persönlichkeitsverletzung.

889 In der Regelung lässt sich damit zugleich die *dynamische Dimension des Datenschutzes* nachweisen: Es geht um Datenflüsse, die einer Ordnung zuzuführen sind. Die Sichtweise ist gerade für eine Norm wie Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG bemerkenswert. *Prima vista* veranlassen die Regeln dazu, das Datensubjekt und das Objekt resp. Quasi-Objekt – die besonders schutzwürdige Personenangabe – als Anknüpfungskategorien zu sehen. Die Produktivität einer dynamischen Sichtweise für den Datenschutz, welche Personendatenflüsse in den Blick nimmt, wurde bisher an mehreren Stellen hervorgehoben – allem voran anhand der Geheimhaltungspflichten sowie dem Zweckbindungsgrundsatz. Zudem vollziehen die jüngsten datenschutzrechtlichen Neuerungen eine Abkehr von einem Konzept, welches das Datensubjekt und die Personenangabe als Quasi-Objekt ins Zentrum der Aufmerksamkeit rückt.

890 In Erinnerung gerufen seien die Erwägungen des Bundesverfassungsgerichts im Volkszählungsurteil. Es gelte zu verhindern, dass im Kontext der Volkszählung

1160 Epiney, in: Rumo-Jungo/Pichonnaz/Hürlimann-Kaup/Fountoulakis (Hrsg.), 97 ff., 97.
1161 Dies., a. a. O., 97 ff., 100 f., wobei die Autorin auf den öffentlichen Bereich fokussiert und attestiert, dass die Einwilligung als Surrogat einer gesetzlichen Grundlage nur in ganz engen Schranken zulässig ist.
1162 Hierzu Epiney/Hofstötter/Meier/Theuerkauf, 23 ff.

generierte Personendaten weiteren Verwaltungseinheiten zur Erfüllung ihrer Vollzugsaufgaben zufliessen. Wenn auch das Urteil den öffentlich-rechtlichen Bereich betrifft, lässt sich eine parallele Stossrichtung in Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG ausmachen: Mit der Bestimmung soll der «Übertritt» von Datenflüssen und Personendaten aus einem bestimmten Verarbeitungskreislauf bei einem bestimmten Verarbeiter, gebunden an einen bestimmten Zweck und Verarbeitungszusammenhang, in einen anderen Verarbeitungskreislauf zu einem *Dritten* beschränkt werden.

Prägend für Art. 12 Abs. 2 lit. c i. V. m. Art. 3 lit. c DSG resp. Art. 30 Abs. 2 lit. c i. V. m. Art. 6 lit. c nDSG bleibt der Abdruck der *Sphärentheorie*, obschon das DSG deren Schwächen überwinden wollte.[1163] Die Feststellung, wonach die Einteilung von Lebensäusserungen, Eigenschaften usf. in privat resp. geheim/intim und öffentlich zu kurz greife, gab einen Impetus zum Erlass spezifischer Datenschutzregulierungen. Denn die Auswertung vieler in der «Öffentlichkeit» zur Kenntnis genommener Angaben könnten zu einem Persönlichkeitsprofil verdichtet werden, woraus grundlegende Aussagen über eine Person mit entsprechenden Risiken resultieren. Diese Erkenntnis rezipiert Art. 12 Abs. 2 lit. c DSG mit seinen Schutzvorgaben betreffend *Persönlichkeitsprofile*. 891

Im Übrigen zeigt sich Art. 12 Abs. 2 lit. c DSG und Art. 30 Abs. 2 lit. c nDSG mit der Kategorie der *besonders schutzwürdigen Personenangaben* als Relikt der Sphärentheorie. Die sog. Sphärentheorie hatte sich ursprünglich zur Konkretisierung eines Persönlichkeitsgutes in Deutschland entwickelt. Sie wurde später in der Schweiz für den privatrechtlichen Bereich zur Konkretisierung von Art. 28 ZGB rezipiert.[1164] Aus zivilrechtlicher Perspektive ist es die Metapher der Zwiebel, nach welcher menschliche Lebensbereiche im Sinne konzentrischer Kreise in eine Gemeinsphäre resp. öffentliche Sphäre, eine Privatsphäre und eine Geheim- resp. Intimsphäre gegliedert werden. Das Bundesgericht bezieht sich bis heute auf dieses Konzept, neuerdings in BGE 142 III 263. Seine Regeste lautet: «Datenschutzgesetz, Art. 28 ff. ZGB; Videoüberwachung in einem Miethaus. Beurteilung der Zulässigkeit einer Videoüberwachungsanlage in einer Liegenschaft mit Mietwohnungen (E. 2).» Es ging um die Beurteilung der Zulässigkeit einer Videoüberwachung einer Mietliegenschaft in diversen Bereichen und Räumlichkeiten, unter anderem im Eingangsbereich. Die Parteien wie die Vorinstanzen erhoben die «Privatsphäre» zum Kernelement ihrer Argumentation. Die Erwägungen differenzieren hinsichtlich der Überwachung des Aussenbereichs und der Übergänge zu den Waschräumen gegenüber dem Innenbereich. Im Zusammenhang mit der Fortwirkung der Sphärentheorie über das 20. Jahrhundert hinaus ist sodann BGE 136 III 410 zu nennen: In dem Entscheid ging es um die Observation einer 892

1163 Vgl. BBl 1988 II 414 ff., 418 f.
1164 Vertiefend m. w. H. Aebi-Müller, N 512 ff.

versicherten Person durch einen Privatdetektiv, wobei das Bundesgericht mit E 2.2. auf die sog. Geheim- und Privatsphäre als Beurteilungskriterium abstellte.[1165] Illustrativ hinsichtlich der Anknüpfung auch zeitgenössischer Datenschutzbelange an die Idee des Privatsphärenschutzes – und der Ehre – ist ebenso der Beitrag von Rusch/Kummer aus dem Jahr 2015.[1166] In ihrem Aufsatz beleuchten sie die zivilrechtliche Relevanz des «forced outing». Die sexuelle Orientierung und die entsprechende Information mag als Inbegriff einer «natürlicherweise intimen» Personenangabe gelten. Folglich figurieren in Art. 3 lit. c Ziff. 3 DSG resp. Art. 6 lit. c Ziff. 3 nDSG die «Angaben über die Intimsphäre» unter den *besonders schützenswerten Personenangaben*. Auch Rusch/Kummer beziehen sich auf die Sphärentheorie als Persönlichkeitsgut i. S. v. Art. 28 Abs. 1 ZGB. Ihr gemäss werden die Geheim-, Privat-, und Öffentlichkeitssphäre abgegrenzt. Entsprechend der Zuweisung werden einer Angabe nuancierte Schutzvorgaben zugemessen. In einem Einzeiler behaupten auch Rusch/Kummer unter Berufung auf Aebi-Müller für das Datenschutzgesetz die Verbürgung eines Rechts auf informationelle Selbstbestimmung, aus dem ggf. ein Entscheidungsmerkmal für die subjektive Interpretation der Sphären gezogen werden könne. Dies ist nicht die Stelle, die erwähnten Entscheide oder das unfreiwillige Outing von Homosexualität vertieft zu analysieren. Die kurze Darstellung sollte illustrieren, inwiefern die Sphärentheorie noch heute ein Element für die Argumentation im Rahmen des (rechtlichen) Umgangs mit Personendaten ist.

893 Dass eine abstrakte Kategorisierung von Personendaten in gewöhnliche und besonders schutzwürdige sowie daran anknüpfend die Definierung der Datenschutzvorgaben nicht tragfähig ist, hielt das Bundesverfassungsgericht mit dem Volkszählungsurteil 1983 fest, indem es ausführte:

> «2. Die Verfassungsbeschwerden geben keinen Anlass zur erschöpfenden Erörterung des Rechts auf informationelle Selbstbestimmung. Zu entscheiden ist nur über die Tragweite dieses Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt. Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein belangloses Datum mehr.

1165 Die Problematik der Observation führte die Schweiz in einem sozialversicherungsrechtlichen Fall sogar vor den EGMR. In EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016 kommt der Europäische Gerichtshof für Menschenrechte (EGMR) mit 6 zu 1 Stimmen zu dem Schluss, dass die Schweiz Art. 8 der Europäischen Menschenrechtskonvention (EMRK) verletzt hat, weil im schweizerischen Recht eine hinreichend präzise rechtliche Grundlage für die Foto- und Videoüberwachung von Versicherten fehlt.

1166 Rusch/Kummer, AJP 2015, 916 ff.

> Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: […].»[1167]

Die Bedeutung des *Verwendungszusammenhanges* als einschlägiges Element zur Gestaltung datenschutzrechtlicher Vorgaben, die nicht isoliert auf den Schutz des Individuums gerichtet sind, stattdessen auch auf den Schutz gesellschaftlicher Institutionen und Kontexte mit ihren Zielen und Erwartungen, wird im letzten Teil dieser Arbeit zukunftsweisend vertieft.[1168] 894

Für Art. 12 Abs. 2 lit. c DSG lässt sich festhalten, dass er Relikte des sphärentheoretischen Konzepts aufweist. Es ist indes nicht die Verarbeitung von besonders schutzwürdigen Personenangaben per se, die eine Persönlichkeitsverletzung auslöst. Vielmehr vervollständigt erst die *Weitergabe an Dritte* den Tatbestand. Damit markiert das Gesetz, dass es zugleich der Datenfluss ist, der mitentscheidend für die datenschutzrechtliche Beurteilung ist. Die Bestimmung hat damit, ähnlich wie Art. 12 Abs. 3 DSG, einen hybriden Charakter. Entsprechend finden sich ebenso an dieser Stelle Impulse für die Entwicklung eines neuen paradigmatischen Ansatzes. Zunächst wurde gezeigt, dass eine abstrakte Definierung und Zuweisung eines gewissen Personendatums zu den «gewöhnlichen» Personendaten oder zu den besonders schützenswerten Personendaten nicht taugt: Wie Simitis für den Namen beschreibt, ist es ein Trugschluss, diesen pauschal als nicht besonders schützenswert zu taxieren – findet sich dieser auf der Liste eines Verbrecherringes ist die Verarbeitung des Namens mit hohen Risiken für die betroffene Person verbunden. Umgekehrt stammen die jeweils als besonders schützenswert definierten Personendaten stets aus einem gewissen Kontext: Es sind Angaben zur Gesundheit, zur Religion, zur Sexualität usf. Und indem die Schweiz die Weitergabe an Dritte – den Transfer – als persönlichkeitsverletzend definiert, erkennt und anerkennt das DSG, dass es nicht die abstrakte Natur einer gewissen Kategorie von Personendaten ist, die zu Risiken führt, sondern ihr Transfer in andere Bereiche. 895

3. Zusammenfassung zur Persönlichkeitsverletzung nach DSG

Es ist der Schutz der Persönlichkeit, Art. 1 (n)DSG, an welchem das DSG sein Regelungskonzept für den privaten Bereich mit Art. 12 f. DSG resp. Art. 30 ff. nDSG konsequent ausrichtet. Den Ausgangspunkt bildet für den privaten Bereich 896

1167 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 176 f.

1168 Richtungsweisend für den kontextuellen Ansatz Nissenbaum, *passim*; vgl. als Andeutung Murphy, Geo. L.J. 1996, 2381 ff., 2400 mit den Worten: «I raise the point because I believe it is related to a noneconomic justification for privacy – the concern that information can be „taken out of context" or „misused".»

die *prinzipielle Verarbeitungsfreiheit mit Schranken*. Ein grundsätzliches Verarbeitungsverbot, das von Erlaubnistatbeständen durchbrochen wird, ist dem DSG für den privaten Bereich fremd. Vielmehr setzt das DSG insofern an *qualifizierten Verarbeitungshandlungen* an, wobei die persönlichkeitsverletzenden Personendatenverarbeitungen mit Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG durch ein differenziertes Instrumentarium konkretisiert werden. Auf den vorangehenden Seiten wurden die Verarbeitungshandlungen beleuchtet, die das DSG explizit, wenn auch nicht abschliessend, vgl. Ingress zu Art. 12 DSG und Art. 30 nDSG, als *persönlichkeitsverletzend* definiert. Während in Abs. 2 lit. a–c drei Konstellationen vom Gesetzgeber als Persönlichkeitsverletzung vordefiniert werden, ist bis heute nicht abschliessend geklärt, welche weiteren Rechtsverstösse eine Persönlichkeitsverletzung begründen.

897 *E contrario* wurden vorab zwei Hauptgruppen von Verarbeitungshandlungen umrissen, die *unterhalb* der Demarkationslinie zur Persönlichkeitsverletzung liegen. Erstens diejenigen, welche die allgemeinen Verarbeitungsgrundsätze einhalten, vgl. Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Zweitens gelten nach Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG Verarbeitungen von Personendaten, die das Datensubjekt selbst allgemein zugänglich gemacht hat, nicht als persönlichkeitsverletzend, sofern das Datensubjekt die Verarbeitung nicht ausdrücklich untersagt hat. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG lässt sich als Hybrid bezeichnen, der Aspekte der Sphärentheorie wie die Idee einer Selbstbestimmung inkludiert. Die Verarbeitung von Personendaten, die das Subjekt selbst allgemein zugänglich gemacht hat, beurteilt das Gesetz als grundsätzlich nicht persönlichkeitsverletzend, es sei denn, es läge ein Verbot durch das Datensubjekt vor. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG ist in verschiedener Hinsicht problematisch. Konzeptionell liegt sein Defizit darin, dass er der dichotomen Vorstellung von öffentlich versus privat verhaftet bleibt. Eine Vorstellung, wonach im Internet zugänglich gemachte Personendaten gewissermassen öffentlich sind und folglich dem Datenschutz weitgehend entzogen werden, ist nicht haltbar.

898 In Bezug auf die *qualifizierten und damit persönlichkeitsverletzenden Verarbeitungshandlungen* wurde *Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG*, welcher die Verletzung der allgemeinen Verarbeitungsgrundsätze als persönlichkeitsverletzend taxiert, als Verbürgung eines *Integritätsschutzes* beschrieben. Die Tatbestandsmässigkeit der Persönlichkeitsverletzung wird objektiv bestimmt, die Qualifizierung der Eingriffsintensität liegt in der Verletzung der allgemeinen Verarbeitungsgrundsätze. Letztere lassen sich als Mindestanforderungen der fairen Personendatenverarbeitung beschreiben. Ihre Einhaltung resp. Verletzung markiert die Grenze resp. Schranke zur persönlichkeitsverletzenden Personendatenverarbeitung. Mit dieser Grundsatzregelung wird kein System informa-

tioneller Selbstbestimmung, das von einem prinzipiellen Verarbeitungsverbot ausgeht und in dem die allgemeinen Verarbeitungsgrundsätze eine zweite Schranke bilden, vorgesehen. Die jüngsten rechtlichen Neuerungen reagieren u. a. auch auf die ungenügende Griffigkeit generalklauselartiger Datenschutzvorgaben in der Praxis. Sie ergänzen die deliktsrechtliche Fokussierung des persönlichkeitsrechtlich basierten Datenschutzrechts, indem neu an erster Stelle die Verantwortlichen durch verschiedene konkrete Umsetzungsinstrumente sowie Dokumentations- und Rechenschaftspflichten früher und nachdrücklicher in die Pflicht genommen werden. Insofern wird ein Perspektivenwechsel vollzogen, wobei der Fokus von der deliktsrechtlichen, abwehrrechtlichen Konzeption einer Persönlichkeitsverletzung abgewendet und die Einhaltung der Datenschutzvorgaben zu einer genuinen und primären Aufgabe der Verarbeitenden wird. Neue organisatorische und prozedurale Instrumente ergänzen das bislang im Persönlichkeitsschutz basierte materielle Datenschutzrecht. Damit soll dieses faktisch effektuiert werden. Die Einhaltung des Datenschutzrechts wird zu einer Compliance- und Governance-Aufgabe.[1169]

899 *Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG* implementiert eine *Widerspruchslösung*. Der Tatbestand integriert ein subjektives Kriterium. Mit dem Widerspruch wird der von Gesetzes wegen geltende Ausgangspunkt der prinzipiell freien Personendatenverarbeitung für den Einzelfall umgekehrt. Das durch Widerspruch begründete Verarbeitungsverbot kann indes durch überwiegende Interessen der Verantwortlichen übertrumpft werden. Die Bestimmung wurde deshalb als Ansatz eines Autonomieschutzes bezeichnet. Es handelt sich um ein relatives *opt-out im weiteren Sinne*. Die Widerspruchslösung ist kongruent für ein System mit prinzipieller Verarbeitungsfreiheit. Von einem Recht auf informationelle Selbstbestimmung zu sprechen, das untrennbar mit dem Volkszählungsurteil des Bundesverfassungsgerichts assoziiert wird, vermag auch im Lichte dieser Bestimmung des DSG nicht zu überzeugen. Ebendies erhärtete ein vergleichender Blick auf das Transplantationsrecht.

900 Zu *Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG* wurde festgestellt, dass auch dieser Tatbestand an die qualifizierte Verarbeitung anknüpft. Hierbei begründet insb. die Weitergabe von besonders schutzwürdigen Personenangaben an Dritte eine Eingriffsintensität, welche die Persönlichkeitsverletzung des Datensubjektes markiert. Die Bestimmung zeigt Relikte der Sphärentheorie, indem sie an in abstrakter Weise kategorisierte, besonders schutzwürdige Personendaten anknüpft. Die Einschlägigkeit des Verarbeitungszusammenhanges für die Gestaltung der datenschutzrechtlichen Vorgaben wird damit nicht hinreichend anerkannt. Dennoch deutet sich in Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c

1169 Vgl. dritter Teil, VIII. Kapitel, A.2.6.; insofern insb. auch Art. 24 DSGVO.

nDSG eine *dynamische und potentiell systemische datenschutzrechtliche Betrachtungsweise* an. Angesetzt wird am Transfer von qualifizierten Personendaten an Dritte. Weil in der Norm gleichzeitig Relikte der Sphärentheorie wie auch Elemente ihrer Überwindung angelegt sind, hat sie einen hybriden wie transformativen Charakter.

901 Die Analyse des persönlichkeitsrechtlichen Regelungsregimes des DSG ergab, dass es stets darum ging, die Demarkationslinie zu konkretisieren, wobei es qualifizierte Verarbeitungshandlungen sind, die als Persönlichkeitsverletzung taxiert werden. Das DSG ist damit in seinen Kernbestimmungen im privaten Bereich konsequent dem *abwehr-, deliktsrechtlich und individualrechtlich konzipierten Persönlichkeitsrecht* verpflichtet. Die datenschutzrechtlichen Neuerungen liefern indes eine markante Ergänzung, indem zahlreiche neue Instrumente den Datenschutz weiter auf organisatorische und prozedurale Instrumente umlagern.

902 Datenverarbeitungen, welche die Qualifizierung als persönlichkeitsverletzend erlangen, ziehen die Frage nach der *Widerrechtlichkeit resp. Rechtfertigung* nach sich. Entsprechend der für das Persönlichkeitsrecht entwickelten Dogmatik begründet die Verletzung eines absolut geschützten Rechtsgutes die Widerrechtlichkeit; diese kann allerdings im Falle des Vorliegens eines *Rechtfertigungsgrundes* entfallen.[1170] Nachfolgend wird auf die einzelnen Rechtfertigungsgründe eingegangen, wobei der rechtfertigenden Einwilligung besonderes Augenmerk gilt. Im Ergebnis kann aufgrund der fundierten Betrachtung des Rechtfertigungssystems eine noch präzisere Charakterisierung des DSG für den privaten Sektor erfolgen. Es geht an dieser Stelle nicht darum, eine weitere Theorie beispielsweise zur Frage, ob die Rechtfertigungsgründe tatbestandsausschliessend oder rechtfertigend wirken, anzufügen.[1171] Ebenso wenig geht es um eine grundsätzliche Analyse der Rechtfertigungsgründe. Vielmehr sollen diese spezifisch hinsichtlich ihrer Funktion im Datenschutzrecht beleuchtet werden, um hieraus Anhaltspunkte zur Gestaltung eines wirksamen Datenschutzrechts zu gewinnen.

4. Rechtfertigungsregime gemäss DSG

4.1. Ausgangslage – Text- und Wertungsdifferenzierung

903 Einleitend ist auf die Diskrepanz in der Gesetzesredaktion mit Blick auf die noch in Kraft stehende Version des DSG und die Erwähnung des Rechtfertigungsmechanismus einzugehen. Ebendiese wird zwar mit der Totalrevision bereinigt, indem Art. 30 Abs. 2 und Abs. 3 nDSG konsequent nur die persönlichkeitsverletzende Verarbeitung adressieren. Die Rechtfertigungsgründe werden einzig in

1170 Vgl. Art. 13 DSG.
1171 Vgl. Haas, 33 ff.; grundlegend zur Einwilligung im Privatrecht Ohly, *passim*.

Art. 31 nDSG niedergelegt. Dennoch sind die Ausführungen zum bisherigen DSG aufschlussreich, auch für die Zeit nach dem Inkrafttreten der Totalrevision.

Art. 12 Abs. 2 lit. a DSG und Art. 12 Abs. 3 DSG sehen bei ihrer Umschreibung des Tatbestandes der Persönlichkeitsverletzung durch Datenverarbeitung die Möglichkeit einer Rechtfertigung nicht vor. Dagegen verweisen Art. 12 Abs. 2 lit. b und lit. c DSG explizit auf diese. Als Rechtfertigung fungieren die Einwilligung, überwiegende private oder öffentliche Interessen sowie gesetzliche Rechtfertigungsgründe, vgl. Art. 13 DSG und Art. 28 Abs. 2 ZGB. Wie allerdings sind diese gesetzgeberischen Differenzen zu verstehen? Die Frage hat während längerer Zeit die datenschutzrechtliche Auseinandersetzung absorbiert. In die Sprache der Methodenlehre übersetzt, handelt es sich um eine Auslegungsfrage. Klärungsbedürftig ist, ob es sich um eine echte Lücke, qualifiziertes Schweigen oder ein redaktionelles Versehen handelt. Bevor Art. 12 Abs. 2 DSG mit der Teilrevision von 2008 angepasst wurde, lautete Art. 12 Abs. 2 lit. a DSG: «Er darf insbesondere nicht ohne Rechtfertigungsgrund Personendaten entgegen den Grundsätzen der Artikel 4, 5 Absatz 1 und 7 Absatz 1 bearbeiten.» In der geltenden Fassung lautet Art. 12 Abs. 2 lit. a DSG, Stand 1. Januar 2008: «Er darf insbesondere nicht Personendaten entgegen den Grundsätzen der Artikel 4, 5 Absatz 1 und 7 Absatz 1 bearbeiten.» 904

Über die Bedeutung der Streichung der Passage «ohne Rechtfertigungsgrund» entbrannte eine intensive Debatte: Der EDÖB verortete darin, dass die Rechtfertigungsgründe aus dem Text von Art. 12 Abs. 2 lit. a DSG gestrichen wurden, nicht aber aus lit. b und ebenso wenig aus lit. c, eine datenschutzrechtliche *Stärkung*. Er vertrat infolge der differenzierenden Formulierungen in den drei Literae, dass Verstösse gegen Datenbearbeitungsgrundsätze nach der damaligen Teilrevision *nicht* mehr rechtfertigungsfähig wären.[1172] Anders die Position eines namhaften Teils der Lehre.[1173] Das Bundesamt für Justiz sah sich in der Folge veranlasst, am 10. Oktober 2006 eine Auslegungshilfe zu publizieren: Es interpretierte den Willen des Gesetzgebers dahingehend, dass eine Rechtfertigung von Persönlichkeitsverletzungen infolge Verletzung der Bearbeitungsgrundsätze nicht grundsätzlich ausgeschlossen sei. Vielmehr habe der Gesetzgeber verdeutlichen wollen, dass die Rechtfertigung von Verstössen gegen die enumerierten Grundsätze nicht vorschnell angenommen werden dürfe.[1174] Dieser Auslegung folgte das Bundesgericht in BGE 136 II 508, dem sog. *Logistep-Entscheid vom 8. September 2010*. Es hielt fest, dass *entgegen dem Wortlaut* von Art. 12 Abs. 2 lit. a DSG auch für die hier bezeichneten Konstellationen eine *Rechtfertigung* denkbar 905

1172 BGE 136 II 508, E 5.2. und E 6.3.

1173 Immerhin sei angemerkt, dass es sich bei den Schreibenden zum grossen Teil um praktizierende Anwälte in internationalen Wirtschaftskanzleien handelt.

1174 Vgl. Auslegungshilfe des BJ vom 10. Oktober 2006, Ziff. 3.1.

sei. Allerdings dürfe dies *nur mit grosser Zurückhaltung* angenommen werden.[1175] Im konkreten Fall beurteilte das Bundesgericht vorab IP-Adressen als personenbezogene Daten i. S. v. Art. 3 lit. a DSG. Sie wurden gesammelt, um eine Urheberrechtsverletzung verfolgbar zu machen. Da allerdings das Zusammentragen der Daten über P2P-Netzwerkteilnehmer für diese nicht erkennbar war, sah das Gericht darin eine Verletzung der Grundsätze der Erkennbarkeit sowie der Zweckbindung gemäss Art. 4 Abs. 3 und Abs. 4 DSG. Die damit begangene Persönlichkeitsverletzung beurteilte das Bundesgericht als widerrechtlich und *verneinte* das Vorliegen eines rechtfertigenden überwiegenden privaten oder öffentlichen Interesses.[1176] BGE 138 II 346, das sog. Google-Street-View-Urteil, bestätigte die zurückhaltende Zulassung von Rechtfertigungsgründen im Anwendungsbereich von Art. 12 Abs. 2 lit. a DSG: Zwar sei ein Verstoss gegen die Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 DSG gemäss Art. 12 Abs. 2 lit. a DSG als Persönlichkeitsverletzung zu taxieren, eine Rechtfertigung sei entgegen dem Wortlaut der Norm dennoch nicht ausgeschlossen. Sie dürfe indes nur äusserst zurückhaltend angenommen werden.[1177] Die Teilrevision des DSG von 2008, bei der aus Art. 12 Abs. 2 lit. a DSG der Passus «ohne Rechtfertigungsgrund» gestrichen wurde, änderte mithin an der Rechtslage – so das Bundesgericht und das Bundesamt für Justiz – nichts oder wenig: Der Gesetzgeber habe «nicht grundsätzlich vom heutigen System abweichen» wollen. Immerhin wurde eine Nuancierung anerkannt, indem Rechtfertigungsgründe bei Verletzungen der allgemeinen Verarbeitungsgrundsätze zwar nicht generell ausgeschlossen, aber doch nur ausnahmsweise denkbar seien. Damit wird die Bedeutung der allgemeinen Verarbeitungsgrundsätze als *minimal standard* der fairen Personendatenverarbeitung unterstrichen.

906 Mit der Totalrevision wird der Gesetzestext entsprechend angepasst, vgl. Art. 30 nDSG. In sämtlichen die Persönlichkeitsverletzung umschreibenden Tatbeständen gemäss lit. a–c wird auf eine Thematisierung der Rechtfertigungsgründe verzichtet. Sie werden in Art. 31 nDSG geregelt. Die Totalrevision sieht folglich eine Bereinigung dergestalt vor, dass sie für sämtliche persönlichkeitsverletzenden Handlungen, auch diejenigen entgegen den Grundsätzen, die Rechtfertigung zulässt, was in konsequenter Weise die Umsetzung des Systems von Art. 28 ff. ZGB darstellt.

907 Ob an der Auslegung, wonach Rechtfertigungsgründe *bei Verletzungen der allgemeinen Bearbeitungsgrundsätze zurückhaltend zuzulassen sind*, festgehalten wird, wird sich erst weisen. M. E. sprechen hierfür gewichtige Argumente: Vorab

1175 Vgl. BGE 136 II 508, Regeste und E 5; entsprechend auch EDÖB, Schlussbericht PostFinance, 6, 23.
1176 BGE 136 II 808, E 6.
1177 BGE 138 II 364, E 7.2.

handelt es sich bei der Präzisierung, wonach erhöhte Anforderungen an die Stichhaltigkeit von Rechtfertigungsgründen zu verlangen sind, um eine gefestigte Praxis. Ein Abweichen hiervon scheint mit der Neufassung des DSG nicht beabsichtigt und die Praxisänderung müsste entsprechend gut begründet sein. Hinzu tritt ein gewichtiges materiellrechtliches Argument: Der Ansatz, wonach die allgemeinen Bearbeitungsgrundsätze die bedeutsamste Schranke der prinzipiell freien Datenbearbeitung im privaten Bereich definieren, wurde als *Integritätsschutz* bezeichnet. Er implementiert Mindestanforderungen an faire resp. nicht missbräuchliche Personendatenverarbeitungen. Insofern lassen sie sich als Minimalstandard beschreiben, dessen Verletzung – weil es sich um Basiselemente einer Integritätsgesetzgebung handelt – *nur ausnahmsweise gerechtfertigt* werden soll. Namentlich das überwiegende private Interesse (i. d. R. als wirtschaftliches Interesse), das allzu gerne und leicht ins Feld geführt wird, sollte restriktiv zugelassen werden. Entsprechend wird hier dafür plädiert, dass die Zurückhaltung bei der Anerkennung von Rechtfertigungsgründen bei der Konstellation der Persönlichkeitsverletzung gemäss Art. 30 Abs. 2 lit. a nDSG weiterhin gilt. Aus der Eliminierung der Rechtfertigungsverweise aus sämtlichen Literae resultiert keine Nivellierung in der Zulassung von Rechtfertigungsgründen.

908 Erhärtet wird die Begründung für diese Interpretation wegen der *systemischen Dimension des Datenschutzrechts*. Die Einhaltung der Bearbeitungsgrundsätze gemäss Art. 4 ff. DSG resp. Art. 6 und Art. 8 nDSG resp. deren Verletzung hat *nicht* nur eine individual- und subjektivrechtliche Dimension. Wie anhand des Zweckbindungsgrundsatzes herausgearbeitet wurde, zielen diese wie das Datenschutzrecht im Allgemeinen zugleich darauf ab, die *Angemessenheit von Datenflüssen* zu steuern. Dazu gehört, dass ein Datenfluss in einem bestimmten Flussbett verläuft und dieses nicht resp. nur unter Einhaltung bestimmter Vorgaben verlässt, und dass Personendaten nicht zu einem anderen Zweck in ein anderes Flussbett umgeleitet werden. Damit wird, über den Schutz des Subjektes hinaus, der Schutz der Integrität von Systemen und Subsystemen gewährleistet.[1178] Einen Verstoss gegen den Zweckbindungsgrundsatz als Kernprinzip der allgemeinen Verarbeitungsgrundsätze aufgrund primär individual- und subjektivrechtlich geprägter Interessen der Datenverarbeitenden zu rechtfertigen, bedeutet nichts anderes, als einen elementaren datenschutzrechtlichen Ansatz, dessen vollständiger Bedeutungsgehalt indes bislang nur ungenügend zur Kenntnis genommen wurde, auszuhöhlen.

909 Indem die Verarbeitungsgrundsätze einen *materiellrechtlichen Mindeststandard* gewährleisten und *nicht nur dem Subjektschutz, sondern auch dem Systemschutz* dienen, sollen rein individuell ausgerichtete Eigeninteressen der verarbeitenden

1178 Richtungsweisend für eine solche Konzeption die Beiträge von Nissenbaum.

Stellen als Rechtfertigung von grundsatz- und damit persönlichkeitsverletzenden Verarbeitungshandlungen nur angenommen werden, wenn die Integrität der jeweiligen Bereiche, in welche die Personendatenverarbeitungen eingebettet sind, dennoch gewahrt wird. Gerade die Rechtfertigung von Verstössen gegen datenschutzrechtliche Minimalstandards, die in einem System mit grundsätzlicher Verarbeitungsfreiheit – anders als im System des prinzipiellen Verarbeitungsverbots – die einzige Schranke definieren, sollte auch in der totalrevidierten Fassung weiterhin zurückhaltend zugelassen werden.

910 Weitere gewichtige Fragen zu den Rechtfertigungsgründen, die einen Einfluss auf die Steuerungswirkungen und das Schutzniveau im Datenschutzrecht haben, sind damit nicht geklärt: Eine Kernfrage ist, ob ebenso bei den Tatbeständen von Art. 12 Abs. 2 lit. b und lit. c DSG Zurückhaltung geboten ist. Offen ist sodann, ob persönlichkeitsverletzende Verarbeitungen nach Art. 12 Abs. 3 DSG, wenn das Datensubjekt die Verarbeitung von zuvor allgemein zugänglich gemachten Personendaten ausdrücklich verbietet, namentlich durch überwiegende Interessen gerechtfertigt werden kann oder ob der Widerspruch als eine Art Vorrecht zur unüberwindbaren Schranke der Verarbeitung wird. Der Tatbestand äussert sich hierzu, ähnlich wie Art. 12 Abs. 2 lit. a DSG, nicht. Die Zulassung von Rechtfertigungsgründen für diesen Tatbestand entspräche der Regelung von Art. 12 Abs. 2 lit. b DSG. Letztere Bestimmung lässt eine Bearbeitung gegen den Widerspruch der Person zu, sofern ein Rechtfertigungsgrund vorliegt. Die Regelungsmechanismen weisen denn auch Parallelen auf. Allgemein entspricht eine generelle Rechtfertigungsmöglichkeit persönlichkeitsverletzender Handlungen dem Konzept von Art. 28 ZGB. In Anbetracht dieser Ausgangslage scheint die Zulassung von gesetzlichen Rechtfertigungsgründen ausser Frage zu stehen. Die Herausforderung allerdings liegt in der Koordination des eine Verarbeitung verbietenden Willens des Datensubjektes mit Interessen der Verarbeitenden. Der Wille in Gestalt des Widerspruches des Datensubjektes kann nicht prinzipiell das einzige und allein ausschlaggebende Kriterium für die Unzulässigkeit einer Personendatenverarbeitung sein. Ebenso wenig allerdings sind Interessen der Verarbeitenden (oft wirtschaftliche Interessen) per se geeignet, einen Entscheid des Datensubjektes zu übertrumpfen. Denn stets ist ebenso zu berücksichtigen, dass der Datenschutz nicht nur eine individualrechtliche, sondern auch eine systemische Schutzdimension aufweist. Letztere wird uns vertieft im dritten Teil dieser Arbeit beschäftigen.

911 Eine Kernherausforderung zeigt sich somit in der Koordination des Willens des Datensubjektes mit den von den verarbeitenden Stellen angerufenen überwiegenden eigenen Interessen.[1179] Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG führen

1179 Vgl. in diesem Zusammenhang auch Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 33 ff und N 44 ff.; zum Facettenreichtum dieser Interessen, wobei hierbei sehr oft

einen Katalog von Konstellationen auf, in denen potentiell ein überwiegendes Interesse der Verarbeitenden angenommen wird.

912 Eine interessante Lösung hat sich im Rahmen der DSGVO herausgebildet. Im Rahmen ihres grundsätzlichen Verarbeitungsverbotes mit Erlaubnistatbeständen, vgl. Art. 6 DSGVO, soll im Kontext des sog. Direktmarketing folgende Mechanik gelten: Das nicht qualifizierte Direktmarketing kann prinzipiell über das *legitimate interest* datenverarbeitender Verantwortlicher erlaubt sein; eine Einwilligung wird für den fraglichen Verarbeitungszweck und die entsprechende Verarbeitungstätigkeit nicht generell vorausgesetzt. Sofern allerdings ein Datensubjekt einen Widerspruch einlegt, ist die Personendatenverarbeitung zu Marketingzwecken *endgültig verboten*.[1180]

913 Umgekehrt steht ausser Frage, dass Personendatenverarbeitungen aus bestimmten Gründen ungeachtet des Willens des Datensubjektes zulässig sind: Bereits aus dem Anwendungsbereich von Art. 28 ZGB ist die Situation bekannt, wonach aufgrund überwiegender Informationsinteressen ein Bericht in der Presse veröffentlicht wird, selbst wenn keine Einwilligung resp. kein Widerspruch vorliegt.[1181] Vor diesem Hintergrund sollten auch für die Konstellation von Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG Verarbeitungen entgegen einem Widerspruch des Datensubjektes – wenn auch zurückhaltend resp. aus gewichtigen Gründen – zulässig sein (hierzu vertiefend sogleich). Damit wird Kongruenz zur Interpretation von Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG geschaffen. Ein solcher Auslegungsentscheid wird untermauert vom Grundsatzentscheid des DSG für den privaten Sektor mit seiner prinzipiellen Verarbeitungsfreiheit. Zusammenfassend ist für Art. 12 Abs. 3 DSG eine analoge Interpretation, wie sie für Art. 12 Abs. 2 lit. a DSG vom Bundesamt für Justiz sowie vom Bundesgericht formuliert wurde und die eine parallele Regelung in Art. 12 Abs. 2 lit. b DSG findet, anzunehmen.

914 Ob für die datenschutzgesetzlichen Tatbestände der Persönlichkeitsverletzung allgemein und auch nach Totalrevision Zurückhaltung in Bezug auf die Zulassung von Rechtfertigungsgründen angezeigt ist, ist damit nicht abschliessend geklärt. Namentlich das überwiegende Interesse der Verarbeitenden stellt ein neuralgisches Element für die Gewährleistung eines effizienten Datenschutzrechts dar. Dies gilt *a fortiori* für die Schweiz in ihrem DSG für den privaten Bereich, wo

wirtschaftlich motivierte Effizienzerwägungen im Vordergrund stehen, allerdings auch weitere Interessen auszumachen sind, dritter Teil, IX. Kapitel.

1180 Hierzu ebenso Art. 21 Abs. 2 und Art. 6 lit. f DSGVO; DSGVO ErwG 47; Buchner/Petri, Beck-Komm.-DSGVO, Art. 6 N 176; vgl. auch Helfrich, NomosKomm-DSGVO, Art. 21 N 44; Datenschutzkonferenz DSK, Kurzpapier Nr. 3 vom 29. Juli 2017, 1 ff.; WP 29/217, legitimate interests, 18 ff.

1181 Vgl. BGE 143 III 297, E 6.3.; BGE 127 III 481, E 3; zum Entscheid und den Figuren der absoluten und relativen Person der Zeitgeschichte auch Vogt/Wiget, in: Arter/Jörg (Hrsg.), 129 ff., 150 f.

aufgrund des Ausgangspunktes und der Konstruktion, wonach erst qualifizierte Verarbeitungen eine Persönlichkeitsverletzung begründen, materiellrechtlich ein niedriges Schutzniveau vorgesehen wird. Ebendieses kann immerhin gehalten werden, wenn die Rechtfertigungsgründe für sämtliche Tatbestände der datenschutzgesetzlichen Persönlichkeitsverletzung und nicht nur für Art. 12 Abs. 2 lit. a DSG restriktiv eröffnet werden. Umgekehrt führt die grosszügige Zulassung von Rechtfertigungsgründen auch für Art. 12 Abs. 2 lit. b, lit. c und Art. 12 Abs. 3 DSG zu einer weiteren substantiellen Absenkung des Schutzes der Datensubjekte in ihrer Persönlichkeit.

915 Ebendies sollte, wie zu zeigen sein wird, insb. nicht allein aus überwiegenden wirtschaftlichen Interessen der Verarbeitenden zugelassen werden. Vielmehr sollten *kontextuelle Erwägungen* ein Kernelement der Evaluation bilden.[1182] Nach diesen grundlegenden strukturellen Erwägungen ein kurzer Blick auf die einzelnen Kategorien von Rechtfertigungsgründen bei persönlichkeitsverletzenden Verarbeitungshandlungen durch Private. Das Regime entspricht vor wie nach Totalrevision des DSG demjenigen von Art. 28 ZGB.

4.2. Gesetzliche Rechtfertigungsgründe

916 Die *gesetzlichen Rechtfertigungsgründe* bereiten theoretisch wie praktisch wenig Schwierigkeiten. Es ist der Gesetzgeber, der hier die Gewichtung und Abwägung vornimmt. Gesetzliche Bearbeitungspflichten und -rechte, die als Rechtfertigungsgründe für persönlichkeitsverletzende Personendatenverarbeitungen figurieren, finden sich in einer Vielzahl von Erlassen.[1183] Exemplarisch zu nennen sind Aufklärungs- und Bearbeitungspflichten gemäss Art. 3 ff. des Geldwäschereigesetzes oder Art. 28 ff. des Konsumkreditgesetzes, die Aufbewahrungspflicht gemäss Art. 985 OR, Offenlegungspflichten nach Gesellschaftsrecht, Art. 663c OR, oder gemäss Art. 20 und Art. 31 des Börsengesetzes, Auskunftspflichten, Zeugnispflichten usf.; erwähnenswert ist ebenso Art. 384 Abs. 1 ZGB.

917 Wiederum ist eine Reflexion im Lichte des Grundsatzentscheides für den Ausgangspunkt angezeigt: Bei einem System mit prinzipiellem Verarbeitungsverbot greift die Notwendigkeit eines Erlaubnisvorbehaltes in einem Gesetz auf «oberster Stufe» und für «gewöhnliche», sprich «jede» resp. «nicht qualifizierte» Verarbeitung. Anders im System der grundsätzlichen Verarbeitungsfreiheit mit Schranken, wie sie das DSG für den privaten Bereich vorsieht: Die gesetzliche Grundlage liefert im System der prinzipiellen Verarbeitungsfreiheit einen Rechtfertigungsgrund für qualifizierte, sprich persönlichkeitsverletzende Verarbeitungshandlungen. Trotz dieser Differenz verwebt sich in beiden Systemen über die Gesetzes-

1182 Vertiefend insofern dritter Teil, IX. Kapitel.
1183 Eine gute Übersicht bietet Rampini, BSK-DSG, Art. 13 N 18.

grundlage das allgemeine Regime mit einem jeweils spezifischen Regime, das Kontexten, Systemen usf. Rechnung trägt. Über die gesetzlichen Rechtfertigungsgründe, die nach DSG persönlichkeitsverletzende Verarbeitungshandlungen zu rechtmässigen Handlungen machen, vgl. Art. 13 DSG und Art. 31 nDSG werden namentlich *Spezialgesetzgebungen und sektor- oder branchenspezifische Erlasse* einschlägig. Die gesetzlichen Rechtfertigungsgründe sind damit gleichzeitig ein wichtiges und konkretes Instrumentarium zur *Gestaltung von Datenflüssen* sowie zur Koordinierung von verschiedenen Verarbeitungszusammenhängen, -kontexten sowie -prozessen. Insofern lassen sich die gesetzlichen Rechtfertigungsgründe als *Brücken* oder *Koordinationsstellen* bezeichnen. Die allgemeine Datenschutzgesetzgebung für den privaten Sektor wird damit an der Stelle der gesetzlichen Rechtfertigungsgründe neuerdings als *Teilordnung des Datenschutzrechts* positioniert. Sie ist, wie anhand des Rechtmässigkeitsprinzips dargestellt, in ein ausdifferenziertes Netz von weiteren Erlassen eingebettet.[1184] Anhand der gesetzlichen Rechtfertigungsgründe präsentiert sich der private Bereich des DSG erneut nicht als einheitlicher, monolithischer Bereich. Vielmehr konstituiert sich dieser sog. Privatbereich aus pluralen Subsystemen, wobei über die *gesetzlichen Rechtfertigungsgründe kontextspezifische Erwartungen*, die der Gesetzgeber für spezifische Regulierungsbereiche anerkannt hat, in das allgemeine Datenschutzregime integriert werden.

An dieser Stelle, an welcher der Fokus auf die Rechtfertigung einer Persön- 918
lichkeitsverletzung im Rahmen des Individualgüterrechtsschutzes gerichtet ist, bestätigt sich die systemische und dynamische Facette des Datenschutzrechts. Sie verändert eine Sicht, welche das Datensubjekt und das Personendatum als Quasi-Objekte ins Visier nimmt. Über die Rechtfertigungsgründe qua Gesetz werden Personendatenflüsse und -verarbeitungsprozesse innerhalb und zwischen verschiedenen Verarbeitungszusammenhängen und -kontexten als Gegenstand datenschutzrechtlicher Regulierung sichtbar.[1185] Auch anhand der gesetzlichen Rechtfertigungsgründe lässt sich selbst im schweizerischen DSG mit seiner konsequenten Anknüpfung im zivilrechtlichen Persönlichkeitsschutz eine Regelungskonzeption freilegen, die den Fluss von Personendaten normiert, die Flussbetten sowie das Delta in den Blick nehmen. Ladeur hat für dieses Delta den Begriff des *Knotenpunktes* geprägt und dessen Relevanz für den Datenschutz betont.[1186] Anhand der gesetzlichen Rechtfertigungsgründe zeigt sich – auch wenn diese

1184 Hierzu zweiter Teil, V. Kapitel, B.1.

1185 Eine solche Sichtweise wurde namentlich anhand des Zweckbindungsgrundsatzes herausgearbeitet, zweiter Teil, V. Kapitel, B.4.

1186 Ladeur, Vortrag, Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021); eine solche Perzeption drängt sich gerade auch mit Blick auf das Internet auf mit seiner netzwerkartigen und konnexionistischen Struktur, Vesting, in: Ladeur (Hrsg.), 155 ff., 162 f.

prima vista einzig und allein der konkreten Rechtfertigung einer spezifischen Persönlichkeitsverletzung dienen –, dass es gerade nicht isoliert um den Schutz der Persönlichkeit des Datensubjektes und allfälliger individueller Interessen der Verarbeitenden geht. Vielmehr werden dem Grundsatz nach persönlichkeitsverletzende Personendatenverarbeitungen *von Gesetzes wegen* gerechtfertigt, wobei bereichs-, kontext-, systemspezifische Erwartungen verfolgt und adressiert werden. Sie zielen darauf ab, die in den spezifischen Bereichen einschlägigen Ziele und Zwecke zu gewährleisten.

919 Eine solche Betrachtungsweise der gesetzlichen Rechtfertigungsgründe macht die *Relevanz der jeweiligen Rollen der Akteure* im *jeweiligen Verarbeitungskontext* sichtbar, wie sie selbst für das Datenschutzgesetz als Querschnittsgesetz einschlägig ist.[1187] Massgeblich ist im Rahmen der Verarbeitungsprozesse und der Prüfung allfälliger Rechtfertigungsgründe für persönlichkeitsverletzende Handlungen zum einen, ob die verarbeitende Person als *Arbeitgeber*, als *Kreditinstitut* resp. Finanzdienstleistungen anbietendes Institut, als *Verwaltungsrat*, als *Ärztin* usf. Personendaten verarbeitet. Zum anderen scheint das DSG selbst grob geschnitzt von der «Persönlichkeit», der natürlichen Person, dem Individuum für den «privaten Sektor» auszugehen.[1188] Das betroffene Datensubjekt erscheint auf den ersten Blick als eine «fixe und einheitliche Figur». Anhand der gesetzlichen Rechtfertigungsgründe allerdings zeigt sich dieses Subjekt in seinem Facettenreichtum und seinem «changierenden» Charakter. Es nimmt differenzierte Rollen ein, womit es auch datenschutzrechtlich um eine Persönlichkeit geht, die gewissermassen und wiederum «ausdifferenziert» anhand ihrer Rollen agiert. Es geht darum, dass eine persönlichkeitsverletzende Verarbeitungshandlung gegenüber einer Patientin, einem Versicherungsnehmer, einer Anlegerin usf. aufgrund einer gesetzlichen Grundlage gerechtfertigt werden kann. Mit anderen Worten wird ein *Konnex* zwischen einem vorab aufgrund des Querschnittsgesetzes des DSG als fix und undifferenziert beschriebenen Datensubjekt («Einheitssubjekt», «Persönlichkeit») und einem in ähnlicher Weise nicht nuanciert wahrgenommenen «Verarbeiter» zu den jeweils im Hintergrund stehenden und einbettenden Handlungsbereichen hergestellt. Im Rahmen der Geheimhaltungspflichten wurde zur Beschreibung dieser Ausgangslage der Begriff der *Akzessorietät* vorgeschlagen. Weiter gedacht heisst dies, dass beispielsweise die Weitergabe von

1187 Früh zur Ausdifferenzierung von Gesellschaftssystemen und zur Relevanz von hieran anknüpfenden Rollen auch für das Datenschutzrecht Mallmann, 36 ff.

1188 Für den öffentlichen Bereich wird grob vom «Bundesorgan» und von der «Bürgerin» ausgegangen, wobei hierbei das Legalitätsprinzip und die Notwendigkeit einer spezifischen gesetzlichen Grundlage Ausdifferenzierungen für den öffentlichen Bereich bringen, der ebenso wenig ein einheitlicher Bereich ist, sich stattdessen aus pluralen Unterbereichen konstituiert. Das Bundesverfassungsgericht hat dies mit seinem Volkszählungsurteil und seinen Erwägungen zum Zweckbindungsgrundsatz sichtbar gemacht; aufschlussreich zu Teilbereichen innerhalb der Persönlichkeit, die ihrerseits Systeme abbilden, Fried, Yale L.J. 1968, 475 ff., 478.

Gesundheitsangaben über eine Person an eine bestimmte Stelle durch einen Arzt, der grundsätzlich dem Arztgeheimnis untersteht, für den Fall von ansteckenden Krankheiten im Interesse der allgemeinen Gesundheit geboten sei.[1189] Eine solche Personendatenverarbeitung soll entsprechend zwecks Erfüllung eines allgemeinen gewichtigen Interesses, des allgemeinen Gesundheitsschutzes, unter Umständen selbst mangels Einwilligung des Datensubjektes unter Einhaltung allfälliger prozeduraler Vorgaben, möglich sein. Eine grundsätzlich persönlichkeitsverletzende Verarbeitungshandlung wird dann – zum Schutz kontextueller Integrität – von Gesetzes wegen gerechtfertigt.[1190]

920 Die persönlichkeitsverletzende Verarbeitungshandlungen *legitimierenden Gesetzestatbestände dienen folglich der Funktionstüchtigkeit und dem Schutz der Integrität jeweils spezifischer Kontexte mit den ebenda formulierten und zu gewährleistenden Zielen*.[1191] Indem Bewertungen und Interessen aus spezifischen Kontexten aufgrund einer generell-abstrakten Beurteilung als schutzwürdig anerkannt werden, lässt sich der gesetzliche Rechtfertigungsgrund als *Brücke* bezeichnen. Datenschutzrecht ist damit – trotz der allgemeinen Ordnung im DSG als sog. Querschnittsgesetz – bereits heute *systembezogenes Recht*.

4.3. Überwiegende Interessen

921 Die überwiegenden privaten wie öffentlichen Interessen werden als Rechtfertigungsgründe für Persönlichkeitsverletzungen qua Personendatenverarbeitungen allgemein in Art. 13 Abs. 1 DSG resp. Art. 31 Abs. 1 nDSG genannt. Konkretisiert werden Konstellationen potentiell überwiegender Interessen in den Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG. Die gesetzliche Enumerierung möglicher überwiegender Interessen entbindet nicht davon, ihr Vorliegen für den konkreten Fall zu belegen. Anders gewendet: Sie gelten nicht von Gesetzes wegen absolut.

922 Die Generalklausel der überwiegenden privaten und öffentlichen Interessen lädt zu grosszügigen Interpretationen vonseiten der Datenverarbeitenden ein. Datenschutzrechtlich wird namentlich das überwiegende private Interesse als *Blanko-Ermächtigung* kritisiert.[1192] Heute lassen sich vonseiten der Verantwortlichen für nahezu jede Personendatenverarbeitung Interessen anführen, die als überwiegend beurteilt werden könnten. An erster Stelle dürften wirtschaftliche Interessen figurieren, zumal Personendaten als das «Gold» resp. «Öl des 21. Jahrhunderts» gel-

1189 Nissenbaum, 173.
1190 Vgl. die Meldepflicht gemäss Art. 12 Abs. 1 des Bundesgesetzes über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiegesetz, EpG, SR 818.101).
1191 Nissenbaum, 173.
1192 Vgl. Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 33 ff und N 44 ff.

ten.[1193] Die Gesetzessystematik mag den datenverarbeitenden Stellen aufgrund des Grundsatzentscheides für die Freiheit der Datenbearbeitung mit Schranken durchaus rechtlich begründeten Anlass geben, von einer grosszügigen Interpretation zulässiger überwiegender privater Interessen auszugehen.[1194]

923 Immerhin sollen, *pro memoria*, Rechtfertigungsgründe für Persönlichkeitsverletzungen gemäss Art. 12 Abs. 2 lit. a DSG nur zurückhaltend angenommen werden. Dies hat spezifisch für die Figur des überwiegenden Interesses Relevanz. Eine solch zurückhaltende Annahme von Rechtfertigungsgründen ist ebenso nach Totalrevision zu fordern, insb. für die Konstellation gemäss Art. 30 Abs. 2 lit. a nDSG. Wie weit aber geht diese Zurückhaltung resp. worin finden sich orientierende Gewichtsteine resp. Evaluationskriterien, um zu bestimmen, welche überwiegenden privaten Interessen persönlichkeitsverletzende Verarbeitungshandlungen rechtfertigen? Lehre und Rechtsprechung äussern sich hierzu nicht vertieft. Anhaltspunkte liessen sich vorab aus den von Gesetzes wegen konkretisierten Konstellationen des überwiegenden Interesses gemäss Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG finden. Weitere Richtungshinweise finden sich in einem Befund, wonach die Gründe zur Rechtfertigung persönlichkeitsverletzender Personendatenverarbeitungen nicht isoliert individualrechtlicher Provenienz sind. Vielmehr ist in diesem Punkt die dynamische sowie systemische Dimension des Datenschutzrechts zu berücksichtigen. Ebendies soll für die *überwiegenden öffentlichen oder privaten Interessen* gelten. Unmittelbar sichtbar wird dies anhand von Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG, der *nicht abschliessend* denkbare überwiegende Interessen, die der Erfüllung spezifischer Verarbeitungszusammenhänge und -kontexte dienen, aufführt. Art. 31 Abs. 2 nDSG sieht gewisse Anpassungen im Vergleich zu Art. 13 Abs. 2 DSG, auf die indes an dieser Stelle nicht vertiefend eingegangen wird.

924 Eine Inspiration- und Interpretationsquelle lässt sich in Bezug auf die Interessenabwägungen anhand eines auf den ersten Blick vielleicht gewagten Exkurses in das Vereinsrecht finden. Im Vereinsrecht kommt Zweckerwägungen – ähnlich wie im Datenschutzrecht – eine hohe Bedeutung zu. Über einen vernetzten Blick auf Zweckerwägungen im Rahmen des Vereinsrechts lassen sich Richtungshinweise für das Datenschutzrecht generieren. Die beklagte Orientierungs- und Steuerlosigkeit des «überwiegenden Interesses» lässt durch eine Integration von Zweckerwägungen reduzieren. Mit anderen Worten: Das Defizit der Figur der «überwiegenden Interessen» wird datenschutzrechtlich durch eine

1193 Vgl. kritisch m. w. H. Hürlimann/Zech, sui-generis 2019, 89 ff., 90; Flückiger, NZZ vom 1. Februar 2016; Grassegger, 10; zum Gold, das aus Analysen von grossen Datenbeständen generiert wird, Beranek Zanon, in: Thouvenin/Weber (Hrsg.), 86 ff., 89; zum hohen wirtschaftlichen Wert von Personendaten Schmid, in: Schmid/Girsberger (Hrsg.), 151 ff., 151.

1194 Vgl. zweiter Teil, IV. Kapitel, B.3.2.

Ankoppelung von Zweckerwägungen abgeschwächt, wobei eben das Vereinsrecht für einen differenzierten Blick auf die Zweckrelevanz aufschlussreich ist. Konkreter geht es um die Herausforderung, das *Verhältnis zwischen mehreren verschiedenen Zwecken, zwischen mittelbarem und unmittelbarem Zweck*, zu koordinieren. Eine solche Zweckdifferenzierung ist für das Vereinsrecht typisch. Das Vereinsrecht wird geprägt von der Unterscheidung zwischen *ideellem und wirtschaftlichem* Zweck.[1195] Für einen rein wirtschaftlichen Zweck darf nicht die Vereinsform gewählt werden. Entsprechend konstanter Bundesgerichtspraxis liegt ein wirtschaftlicher Zweck dann vor, wenn ein Verein wirtschaftliche Vorteile generieren möchte *und* diese an die Mitglieder selbst zurückfliessen sollen.[1196] Es geht in dieser Konstellation um ein *isoliertes und eigenes Profitinteresse*, für welches das Gefäss des Vereins nicht zur Verfügung stehen soll. Die Vereinsform ist zulässig, wenn zwar ein Vorteil generiert wird, dieser allerdings Dritten und nicht dem Verein resp. seinen Mitgliedern selbst zufliesst.

Parallele Erwägungen lassen sich für den Datenschutz anstellen: Im Rahmen der Personendatenverarbeitung liegt es für die Verarbeitenden nahe, den *eigenen* Profit, der (vermeintlich) durch möglichst unbeschränkte Personendatenverarbeitungsprozesse erzielt werden kann, als «überwiegendes privates Interesse» anzuführen. Die Relevanz der Staffelung von Interessen und Zwecken wurde für das Datenschutzrecht anhand der Analyse des Zweckbindungsgrundsatzes herausgearbeitet.[1197] Im Rahmen der Beurteilung, wann aus einer Perspektive des Datenschutzes Interessen als überwiegend zu qualifizieren sind, liesse sich dieser für das Vereinsrecht längst bekannte, nuancierte Ansatz mit seiner Differenzierung zwischen primären Zwecken, Zielen und Interessen sowie oft dahinterstehenden wirtschaftlichen Interessen fruchtbar machen: Unter Umständen liesse sich die «Vermutung» erhärten, wonach eine persönlichkeitsverletzende Verarbeitungshandlung dann von einem überwiegenden Interesse getragen ist, wenn mit ihr der *unmittelbare Zweck und das primäre Ziel des Kontextes*, in den die Verarbeitungshandlung eingebettet ist, effizienter erreicht werden. Einzig und allein die Generierung von *wirtschaftlichem Gewinn und Profit in eigenem Interesse* vermag – isoliert betrachtet – hierzu namentlich dann nicht zu genügen, wenn sich die persönlichkeitsverletzende Verarbeitungshandlung nicht in einem rein ökonomischen Kontext vollzieht, sondern stattdessen Ziele und Zwecke weiterer gesellschaftlicher Bereiche auf dem Spiel stehen, in denen die Personendatenverarbeitungsprozesse eingebettet sind. Anders gewendet: Wirtschaftliche Interessen von Verantwortlichen, die mittels Personendatenverarbeitungen verfolgt werden, dürfen die Integrität weiterer gesellschaftlicher Kontexte mit ihren

925

1195 Vgl. Art. 52 Abs. 2, Art. 59 Abs. 2 und Art. 60 Abs. 1 ZGB; vgl. BGE 88 II 209; BGE 90 II 333.
1196 Vgl. m. w. H. Jakob, KuKo-ZGB, Art. 60 N 1 f.
1197 Vgl. hierzu zweiter Teil, V. Kapitel, B.4.

Zielen und Zwecken nicht untergraben. In einem solchen Sinne liessen sich die überwiegenden Interessen in einer für das Datenschutzrecht produktiven Weise strukturieren, kanalisieren und unter Umständen limitieren.

926 Die umrissene Stossrichtung wird im letzten Teil dieser Arbeit fundiert werden, wobei exemplarisch und spezifisch die Observation im Versicherungskontext zur «Beweisführung» herangezogen wird. Bei letzterer geht es darum, Leistungsbeziehende mittels Privatdetektivs geheim zu observieren, um einen allfälligen Betrug aufzudecken. Die Praxis, für die nunmehr eine gesetzliche Grundlage geschaffen wurde, stösst gleichwohl auf gesellschaftlichen Widerstand.[1198] Nissenbaum dienen die gesellschaftlichen Reaktionen des Widerstandes und des Empörens als Detektor oder Indikator, wonach kontextspezifische Erwartungen verletzt werden. Sie setzt diese als Instrumentarium für ihre Argumentation ein.[1199]

927 Eine ähnliche Konstellation wie in der geheimen Versicherungsobservation liegt den Logistep-Entscheiden zugrunde. Die Logistep AG, welche aufgrund einer von ihr entwickelten Software das Surfverhalten von Internetnutzerinnen und -nutzern trackte, verfolgte an erster Stelle ein *eigenes monetäres Interesse*. Die Ermittlung von Urheberrechtsverletzungen dagegen, so das Bundesgericht, sei Aufgabe staatlicher Behörden.[1200] Folglich liess das Bundesgericht ein überwiegendes Interesse nicht als Rechtfertigungsgrund zu.[1201] Der Entscheid ist damit ein Illustrationsbeispiel dafür, wie für das Datenschutzrecht der Schweiz – hier anhand der Rechtsprechung zu den überwiegenden Interessen als Rechtfertigungsgrund für eine persönlichkeitsverletzende Personendatenverarbeitung – die Einschlägigkeit *pluraler* Verarbeitungszusammenhänge sowie Gesellschaftsbereiche anerkannt wird. Die Relevanz des Schutzes von Systemen sowie Subsystemen mit ihren jeweiligen spezifischen Zwecken, Interessen, Akteuren und Rollen wird auch hier adressiert.

928 Dass diese Schutzrichtung trotz der dualistischen Struktur mit seiner persönlichkeitsrechtlichen Anknüpfung für den privaten Bereich im DSG angelegt ist, verdeutlicht zudem der Blick auf die vom Gesetzgeber konkretisierten potentiellen Konstellationen, in denen überwiegende Interessen angenommen werden: Sie beziehen sich auf jeweils spezifische Verarbeitungszusammenhänge und Kontexte, z. B. den Medienkontext oder die Forschung.

929 Nachdem über die gesetzliche Grundlage sowie die überwiegenden Interessen zur Rechtfertigung persönlichkeitsverletzender Personendatenverarbeitungen die

1198 Vgl. vertiefend dritter Teil, IX. Kapitel, B.
1199 Nissenbaum, 3; zur Welt der Gefühle im Zusammenhang mit (enttäuschten) Erwartungen Luhmann, Systeme, 370 ff.
1200 BGE 136 II 508, E 6.3.2.
1201 BGE 136 II 508, E 5 und E 6, insb. E 6.3.3.; beachte insofern die Teilrevision des URG.

Integration kontextspezifischer Erwägungen selbst im persönlichkeitsrechtlichen und damit subjektivrechtlich angeknüpften Datenschutzrecht resp. Datenschutzgesetz als Querschnittsgesetz sichtbar gemacht wurde, soll nunmehr auf die Bedeutung der Einwilligung des Datensubjektes als Rechtfertigungsgrund eingegangen werden. Da hinsichtlich der Bedeutung, Rolle und Funktion der datenschutzrechtlichen Einwilligungen Unsicherheiten und Fehlannahmen bestehen, widmen sich die folgenden Ausführungen diesen vertieft.

4.4. *Die rechtfertigende Einwilligung gemäss DSG*

4.4.1. *Einordnung*

930 Die Schweiz kennt in ihrem DSG für den privaten Bereich das Einwilligungserfordernis als Erlaubnistatbestand für prinzipiell verbotene Personendatenverarbeitungen *nicht*. Ebendies gilt auch nach Totalrevision und mit Blick auf Art. 6 Abs. 6 und Abs. 7 nDSG. Vielmehr spielt die Einwilligung im DSG die Rolle als Rechtfertigungsgrund für persönlichkeitsverletzende Personendatenverarbeitungen, vgl. auch Art. 13 Abs. 1 und Art. 31 Abs. 1 nDSG. Ein solches Einwilligungskonzept ist logische Konsequenz des Ausgangspunktes der generellen Verarbeitungsfreiheit mit Schranken, den das DSG für den privaten Bereich wählt.[1202] Schranken, deren Durchbrechung die Persönlichkeitsverletzung markieren, bilden namentlich die Verletzung der allgemeinen Verarbeitungsgrundsätze, der Widerspruch des Datensubjektes, die Weitergabe von besonders schutzwürdigen Angaben und Persönlichkeitsprofilen an Dritte, vgl. Art. 12 Abs. 2 DSG und Art. 30 Abs. 2 nDSG. Die Einwilligung des Datensubjektes figuriert gemäss DSG somit als Rechtfertigungsgrund für qualifizierte Verarbeitungshandlungen, die als persönlichkeitsverletzend taxiert werden und die nicht durch einen anderen Rechtfertigungsgrund legitimiert sind.[1203] Obschon punktuell nachgeschaltet zu den Rechtfertigungsgründen qua Gesetz oder überwiegendem Interesse gilt die Einwilligung faktisch als bedeutsam(st)er Rechtfertigungsgrund.[1204] Hierzu die folgenden Anmerkungen:

931 Einbettend ist unter Berücksichtigung des Dualismus zunächst zu erwähnen, dass die Einwilligung im öffentlichen Bereich von vornherein keine grosse Relevanz hat.[1205] Gesprochen wird dort, wo Personendaten zu einem «öffentlichen

1202 So auch Vasella, Jusletter vom 16. November 2015, N 1.
1203 Die jederzeitige Widerrufsmöglichkeit einer Einwilligung gemäss allgemeinen Grundsätzen wird nachfolgend nicht thematisiert.
1204 Rampini, BSK-DSG, Art. 13 N 3; Vasella, Jusletter vom 16. November 2015, N 2.
1205 Exemplarisch und spezifisch in Bezug auf besonders schützenswerte Informationen Epiney, in: Rumo-Jungo/Pichonnaz/Hürlimann-Kaup/Fountoulakis (Hrsg.), 97 ff., 101 ff., 105 ff., 110.

Zweck» und damit regelmässig basierend auf einer gesetzlichen Grundlage bearbeitet werden, von einer «Entprivatisierung» der Person.[1206]

932 Die Systematik des DSG ist nur teilweise überzeugend. Die Gültigkeitsvoraussetzungen der Einwilligung sind in den allgemeinen Verarbeitungsgrundsätzen niedergelegt, vgl. Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG. Ebendies kann zu der Annahme verleiten, wonach das Einwilligungserfordernis ein allgemeiner Verarbeitungsgrundsatz ist.[1207] Die Lektüre der Bestimmungen erhellt, dass sich die Bestimmung *einzig* mit den Gültigkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung beschäftigt, dort, wo eine Einwilligung geboten ist. Die Bestimmungen statuieren selbst kein Einwilligungserfordernis. Die Konstruktion weist gewisse Parallelen zu Art. 3 ZGB auf. Letzterer verbürgt keinen allgemeinen Gutglaubensschutz. Vielmehr stellt der Artikel eine Vermutung zum guten Glauben auf für den Fall, dass dieser von einer anderen Bestimmung als schutzwürdig taxiert wird.

933 Die Einbettung der Gültigkeitsvoraussetzungen für die datenschutzrechtliche Einwilligung innerhalb der allgemeinen Verarbeitungsgrundsätze, Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG, ist mindestens teilweise irreführend. Sie verleitet zu falschen Annahmen über die verbürgte Rechtsposition. Die Gesetzessystematik mag mitursächlich sein für eine Rezeption und schematische Qualifikation des schweizerischen Datenschutzrechts auch für den privaten Bereich als Regime der Selbstbestimmung. Zumindest in der Allgemeinheit wird ein falscher Eindruck hinsichtlich der Positionierung der Einwilligung nach schweizerischem DSG vermittelt. Die Gültigkeitsanforderungen gemäss Art. 4 Abs. 5 DSG beziehen sich nach dem System des DSG für den privaten Bereich prinzipiell auf die *rechtfertigende Einwilligung gegenüber qualifizierten Verarbeitungshandlungen*, vgl. Art. 12 f. DSG und Art. 30 f. nDSG. Die datenschutzrechtliche Einwilligung ist keineswegs Erfordernis zur Erlaubnis jedweder Personendatenverarbeitungen.

934 Relativierend ist immerhin auf Art. 6 Abs. 2 lit. b DSG resp. Art. 17 Abs. 1 lit. a nDSG hinzuweisen, wonach die Einwilligung des Datensubjektes im Einzelfall insb. für den Transfer von Personendaten in ein sog. unsicheres Drittland eingeholt werden soll.[1208]

935 Innerhalb des DSG für den privaten Bereich bewegt sich die Relevanz der datenschutzrechtlichen Einwilligung in den folgenden Schranken: Von vornherein

1206 Kilian, in: Garstka/Coy (Hrsg.), 195 ff., 197.

1207 Die Gültigkeitsvoraussetzungen für die Einwilligung nach der Totalrevision werden Anlass zu einigen Diskussionen in Lehre und Rechtsprechung nicht nur mit Blick auf die dogmatischen Details geben, vgl. insofern bereits zu den entsprechenden Aufsätzen.

1208 Zu den Entwicklungen im Zusammenhang mit dem US Privacy Shield <https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/medienmitteilungen.msg-id-80318.html> (zuletzt besucht am 3. Juni 2021).

nicht greift die rechtfertigende Einwilligung für persönlichkeitsverletzende Verarbeitungen gemäss Art. 12 DSG resp. Art. 30 nDSG. Für die Tatbestände nach Art. 12 Abs. 1 lit. b und Art. 12 Abs. 3 DSG sowie Art. 30 Abs. 1 lit. b und Art. 30 Abs. 3 nDSG ist der *Widerspruch* des Datensubjektes begründend für die Persönlichkeitsverletzung. In diesen Konstellationen kann der Einwilligung keine sinnvolle Rolle zukommen. Ihre Hauptbedeutung erlangt die datenschutzrechtliche Einwilligung für Datenverarbeitungen, welche die allgemeinen Verarbeitungsgrundsätze missachten und deshalb persönlichkeitsverletzend sind, Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG (was die Widerrechtlichkeit indiziert). Zudem kann sie ihre Relevanz entfalten im Zusammenhang mit der Weitergabe von besonders schutzwürdigen Daten und Persönlichkeitsprofilen an Dritte ohne anderweitigen Rechtfertigungsgrund nach Art. 12 Abs. 1 lit. c DSG.[1209] Art. 30 Abs. 1 lit. c nDSG adressiert nur noch die Weitergabe von besonders schutzwürdigen Angaben an Dritte; das Persönlichkeitsprofil wird aus der gesetzlichen Regelung entfernt.

936 Dass der datenschutzrechtlichen Einwilligung ungeachtet dieses normativ eher engen Rahmens *faktisch – sprich in der Praxis* – eine so hohe Relevanz zugewiesen wird, mag als Bestätigung gelesen werden, wonach der Autonomie und Selbstbestimmung des Datensubjektes hohes Gewicht beigemessen wird. Paradoxerweise allerdings ist die Aussage, wonach die Einwilligung in der Schweizer Unternehmenspraxis eine wichtige Rolle spielt, keineswegs nur als positive Aussage für den Datenschutz zu verstehen. Die Einwilligung dient primär zur Rechtfertigung eines Verstosses gegen das als Integritätsschutz bezeichnete Regime von Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Weil allerdings die allgemeinen Verarbeitungsgrundsätze als *Minimalstandard der fairen Personendatenverarbeitung* zu gelten haben und im schweizerischen System die Hauptschranke der Personendatenverarbeitung bilden, ist das hohe Gewicht, das der Einwilligung in der Datenschutzpraxis zugemessen wird, problematisch. Denn die Einhaltung der allgemeinen Verarbeitungsgrundsätze wird unter Umständen pauschal und blanko «gewaved». Eine solche rein formalistische Herangehensweise vermag allerdings dem Datenschutz nicht gerecht zu werden. Erhärtet wird diese Kritik durch den Befund, wonach die Verarbeitungsgrundsätze *systemische Schutzerwägungen* integrieren. Sie sollen nicht beliebig der breitangelegten, gleichwohl aber individualrechtlichen Dispositionsbefugnis anheimgestellt werden. Zudem ist in Erinnerung zu rufen, dass sich die Auslegung etabliert hat, wonach Rechtfertigungsgründe im Rahmen von Art. 12 Abs. 2 lit. a DSG nur mit Zurückhaltung zuzulassen sind. Es gibt folglich mehrere Einwände, die eine Prio-

1209 In diesem Sinne auch Vasella, Jusletter vom 16. November 2015, N 2.

risierung individualrechtlicher Dispositionsbefugnisse in einem nachteiligen Licht erscheinen lassen.[1210]

937 Spezifisch zu thematisieren ist eine in der Praxis verbreitete Vorgehensweise. Nach dieser wird die datenschutzrechtliche Einwilligung zur Absicherung und formellen Legitimierung von Personendatenprozessen selbst dort eingeholt, wo es von Gesetzes wegen gar keiner datenschutzrechtlichen Zustimmung bedürfte. Sei es, weil die Personendatenverarbeitung gar keine Persönlichkeitsverletzung begründet, sei es, weil eine persönlichkeitsverletzende Verarbeitungshandlung durch einen gesetzlichen Rechtfertigungsgrund oder überwiegende Interessen legitimiert ist. Dem Datensubjekt wird mit einem solchen Vorgehen suggeriert, dass es über die Verarbeitung der Personendaten bestimmen würde. Allerdings wäre im Lichte der Gesetzesordnung die Personendatenverarbeitung selbst ohne seine Einwilligung zulässig. Besagtes Vorgehen ist nicht nur nach DSG, sondern auch nach DSGVO problematisch. Nach DSGVO haben Verantwortliche bei Verstössen gegen die Vorgaben der Verordnung mit weit- und tiefgreifenden Massnahmen sowie Sanktionen vonseiten der Datenschutzbehörden zu rechnen, vgl. Art. 57 f. und Art. 83 f. DSGVO.[1211] Um entsprechende Risiken zu minimieren, liegt es nahe, quasi zur Sicherheit die Einwilligung des Datensubjektes als Erlaubnistatbestand einzuholen, vgl. Art. 6 Abs. 1 lit. a DSGVO. Selbst dann, wenn die Verarbeitung durch einen anderweitigen Erlaubnistatbestand gedeckt wäre, vgl. Art. 6 lit. b–f DSGVO, und insofern nur – aber immerhin – die Transparenzvorgaben einzuhalten wären, vgl. Art. 12 DSGVO. Im Ergebnis *degeneriert in einer solchen Praxis des «cover your action» durch eine «Sicherheitseinwilligung» die datenschutzrechtliche Einwilligung zu einer inhaltslosen und bedeutungsentleerten Formalität*. Sie suggeriert eine Selbstbestimmung des Datensubjektes, die es indes von Gesetzes wegen nicht hat. Entsprechend dürfte von einer *Pseudo-Selbstbestimmung* zu sprechen sein.

938 In Bezug auf die hohe Bedeutung, die der (rechtfertigenden) Einwilligung nach DSG im schweizerischen Schrifttum zugemessen wird, ist ein weiterer Hinweis angezeigt: Die akademische Auseinandersetzung mit dem Datenschutzgesetz für den privaten Sektor war in der Schweiz lange wenig intensiv.[1212] Zwar findet in der Schweiz das Datenschutzrecht nicht zuletzt im Zuge der Inkraftsetzung und Umsetzung der DSGVO sowie der Totalrevision des DSG gesteigerte Aufmerk-

1210 Zu den Schwächen datenschutzrechtlicher Einwilligungskonstruktionen vertiefend dritter Teil, VIII. Kapitel, B.2.2. und B.5.2.

1211 Hierzu z. B. Bergt, DuD 2017, 555 ff.

1212 Der grosse Teil der Beiträge zum DSG im privaten Bereich ist Kommentarliteratur, sodann Aufsätze von Praktikerinnen und Praktikern. Wissenschaftliche Monografien zum DSG für den privaten Bereich dagegen sind Raritäten, vgl. insofern früh Peters und Aebi-Müller, unlängst spezifisch zum Profiling Heuberger.

samkeit auch vonseiten der Wissenschaft.[1213] Von einer eigentlichen Debatte und Theoriebildung mit Blick auf den Ansatz informationeller Selbstbestimmung und damit die Rolle, Funktion und Funktionstüchtigkeit von Einwilligungskonstruktionen im Datenschutzrecht kann allerdings noch nicht gesprochen werden. Bis heute stammt das Gros der Beiträge zum Datenschutzgesetz für den privaten Sektor aus der Feder der *praktizierenden Anwaltschaft* (sowie der kantonalen Datenschutzbeauftragten). Wenn auch vonseiten der Anwaltschaft bedeutsame Beiträge, namentlich Kommentierungen zum geltenden Recht, verfasst wurden, prägt dieser Ursprung das Schweizer Datenschutzrecht mit. Die praktizierende und publizierende Anwaltschaft im Bereich des Datenschutzrechts ist oft für renommierte und international tätige Wirtschaftskanzleien tätig. Hierbei sind es datenschutzrechtlich meist grosse Unternehmen in Konzernstrukturen, welche die entsprechende Expertise benötigen.[1214] Der Rückgriff auf die datenschutzrechtliche Einwilligung dient dann der Minimierung von Datenschutzverstössen mit ihren Risiken und basiert auf einer Strategie des *cover your action*. Aus der Perspektive der beratenden Anwaltschaft mag folglich die *Relevanz der Einwilligung* als Rechtfertigungsgrund faktisch im Vordergrund stehen. Umgekehrt ist davon auszugehen, dass es unzählige Personendatenverarbeitungen gibt, die persönlichkeitsverletzend sind und für die mangels anderweitigen Rechtfertigungsgrundes eine rechtfertigende Einwilligung einzuholen wäre, auf deren Einholung allerdings verzichtet wird.[1215]

939 Bezogen auf die datenschutzrechtliche Einwilligung zeigt sich damit das Problem, dass diese einerseits eingeholt wird, obschon es ihrer nicht bedürfte, und dass diese andererseits nicht eingeholt wird, obschon es ihrer bedürfte.

940 Darin erschöpfen sich indes die Herausforderungen nicht. Vielmehr stehen zudem die *Gültigkeitsvoraussetzungen* der Einwilligung im Datenschutzrecht in Anbetracht der Realität auf dem Prüfstand. Ihnen widmen sich die nachfolgenden Ausführungen. Die Beschäftigung mit der noch grundsätzlicheren Frage, inwiefern Einwilligungskonstruktionen überhaupt geeignet sind, datenschutzrechtliche Aufgaben zu adressieren und Schutzziele zu erreichen, wird im dritten Teil dieser Arbeit vertieft. Die Frage mag erstaunen, zumal sich die Anerkennung und der Ausbau von Selbstbestimmungsrechten, in denen die *Einwilligung* als Ausdruck der Autonomie des Subjektes zum Kernelement der Gesetzgebung

1213 Jünger zur Einwilligung im Datenschutzrecht, allerdings mit Akzent auf den grund- und verfassungsrechtlichen Aspekt, Fasnacht, *passim*; jüngst beachte Kasper, *passim*; Amstutz, AcP 2018, 438 ff. und NZZ vom 5. September 2018, 10.

1214 Vgl. zur unterschiedlichen Maturität mit Blick auf die Umsetzung der datenschutzrechtlichen Vorgaben durch schweizerische KMU gegenüber den Grossunternehmen Ebert/Widmer, 19.

1215 Bolliger/Féraud/Epiney/Hänni, 41; in Deutschland hat namentlich Buchner problematisiert, dass viele Personendatenverarbeitungen an den «Datensubjekten vorbei» bearbeitet werden, vgl. 130 ff.

wird,[1216] als Entwicklungstendenz für Rechtsgebiete beschreiben lässt, die sich mit den Herausforderungen neuer Technologien zu befassen haben. Sie wird als «Rezept» zur Lösung von Herausforderungen, welche die neuen Technologien mit sich bringen, präsentiert.[1217] Dahinter scheint eine Vorstellung zu wirken, wonach der Mensch und seine Würde sowie sein Subjektstatus durch die neuen Technologien ausgehöhlt werden. Dem Subjekt droht durch die undurchschaubaren und unkontrollierbaren Technologien die Degradierung zum Objekt. Zu Recht wurde allerdings – und das ist für diese Studie richtungsweisend -früh davor gewarnt, mit der Identifizierung der Technologien als «Sündenbock» von den sozialen Konflikten und Problemen abzulenken.[1218] Ebendies gilt es über das Recht zu adressieren.

941 Einwilligungskonstruktionen als rechtliche Antwort im Kontext technologiebedingter Herausforderungen können vor diesem Hintergrund als «Emanzipationsansätze» bezeichnet werden. Sie werden mit den Kategorien und Gütern der «Selbstbestimmung» und «Autonomie» assoziiert.[1219] Zwar drängt sich an dieser Stelle erneut die Vermutung auf, dass eine Reduktion auf eine Dichotomie, in der die Technologie als Herrschaftstechnologie und Instrument der Unterwerfung des Menschen beschrieben wird – mit einer Degradierung des Menschen zum Objekt –, dem Facettenreichtum der Thematik nicht gerecht wird. So erstaunt es keineswegs, dass das komplexe Verhältnis zwischen Mensch und Technik auch anderweitig umschrieben wird, beispielsweise mit Begriffen wie «hybride Assoziationen» im Kontext des Internets.[1220]

942 Gleichwohl lässt sich im Zuge der Entwicklungen des Rechts die Strategie nachweisen, auf etablierte Figuren zurückzugreifen und mit Blick auf ein Datenschutzrecht, das zutiefst im Persönlichkeitsrecht verwurzelt ist, den *Subjektstatus zu stärken und auszubauen*.[1221] Ob damit datenschutzrechtlich ein wirksames und produktives Instrument etabliert werden kann, wird jüngst hinterfragt: Insofern werden die Tauglichkeit des Instrumentes in seiner funktionellen Stossrichtung an sich wie auch die bedeutungsvolle Griffigkeit der etablierten Gültigkeits-

1216 Exemplarisch zur Qualifikation von Einwilligungsvorschriften als Elemente des informationellen Autonomieschutzes Ingold, NomosKomm-DSGVO, Art. 7 N 33.

1217 Vgl. illustrativ insofern die zahlreichen datenschutzrechtlichen Monografien zur datenschutzrechtlichen Einwilligung sowie Zeitschriftenbeiträge sowohl im schweizerischen als auch im deutschen Schrifttum; sodann die Beiträge von Barocas/Nissenbaum; Karavas, Körperverfassungsrecht, 193 ff., insb. 199 ff., für den Bereich des Biomedizinrechts.

1218 Fiedler, in: Podlech/Steinmüller (Hrsg.), 179 ff., 193.

1219 Vgl. mit Blick auf das Online Behavioral Advertisement Barocas/Nissenbaum, 1 ff.; aufschlussreich zum Selbstbestimmungsrecht Fateh-Moghadam, BJM 2018, 205 ff., 213 ff.; vgl. insofern auch Litman, Stan. L. Rev. 2000, 1283 ff., 1292 f. mit den Worten «If ownership of private property is power, however, calling privacy rights „property rights" offers the promise of magically vesting the powerless with control over their personal data».

1220 Vgl. Karavas, Neue Zeitschrift für Sozialforschung 2010, 95 ff.

1221 Burkert, 158.

voraussetzungen datenschutzrechtlicher Einwilligungen im Lichte der Realität kritisch beleuchtet.[1222] Damit erscheint es *prima facie* als nicht nachteilig, dass man in der Schweiz bislang den Weg in Richtung Ausbau resp. Etablierung eines Regimes der Selbstbestimmung, in welchem die informierte Einwilligung ein Kerninstrumentarium darstellt, nicht beschritten hat: Zwar werden mit der Totalrevision die Transparenzvorgaben gegenüber dem Datensubjekt und die Betroffenenrechte ausgebaut. Im Übrigen allerdings soll die prinzipielle Bearbeitungsfreiheit mit Schranken beibehalten werden, womit der Wille des Datensubjektes weiterhin als Widerspruchsrecht (das oft eine Utopie bleibt) sowie als rechtfertigende Einwilligung von qualifizierten Verstössen figurieren. Prinzipiell dürfen Personendatenverarbeitungen im privaten Bereich auch nach der Totalrevision des DSG ohne Einwilligung erfolgen.[1223] Sehr viel effizienter zeigt sich eine andere Strategie: die Einführung von neuen Instrumenten, die das Datenschutzrecht faktisch verwirklichen sollen. Genau diesen Weg beschreiten auch die DSGVO sowie die Totalrevision des DSG.

943 Für den Fall, dass eine Einwilligung *zwecks Rechtfertigung* persönlichkeitsverletzender – weil qualifizierter – Personendatenverarbeitungen erforderlich ist, sind ihre *Gültigkeitsvoraussetzungen* zu beachten. Die *Gültigkeitsvoraussetzungen* der Einwilligung gemäss Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG beziehen sich *nicht* auf den *Widerspruch*, wie er in Art. 12 Abs. 2 lit. b DSG oder Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 2 lit. b und Art. 30 Abs. 3 nDSG niedergelegt wird. Dies ergibt bereits der Wortlaut – Einwilligung ist nicht gleich Widerspruch. Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG befassen sich ausdrücklich mit den Modalitäten für die gültige Einwilligung. Dem Widerspruch kommt eine andere Bedeutung und Funktion zu, verkehrt dieser doch eine prinzipiell erlaubte in eine grundsätzlich verbotene Datenverarbeitung. Im DSG für den privaten Bereich wird mittels Widerspruches der gesetzliche Ausgangspunkt, wie er in genereller Weise vorgesehen wird, aufgrund des Willens des Datensubjektes für den Einzelfall modifiziert. Anders wird mit einer rechtfertigenden Einwilligung ein vom Gesetzgeber als Persönlichkeitsverletzung taxiertes Verhalten gebilligt, wobei dieses – wie gezeigt – gemäss DSG in einem qualifizierten Umgang mit Personendaten liegt. Es ist (wiederum) das Subjekt, das mit der rechtfertigenden Einwilligung eine vom Gesetzgeber als persönlichkeitsverletzend und damit prinzipiell widerrechtlich zu qualifizierende Datenverarbeitung die Widerrechtlichkeit entfallen lässt.[1224] Zugleich verzichtet es gleichsam auf das unmittel-

1222 Vertiefend dritter Teil, VIII. Kapitel, B.4.2.
1223 So auch Vasella, Jusletter vom 16. November 2015, N 2; vgl. Rosenthal, HK-DSG, Art. 12 N 25; Hussein, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.114.
1224 Vgl. Art. 28 Abs. 2 ZGB und Art. 13 DSG resp. Art. 31 nDSG.

bar an die ansonsten widerrechtliche Persönlichkeitsverletzung anknüpfende Durchsetzungsinstrumentarium.

944 Vor diesem Hintergrund ist es folgerichtig, an den *Widerspruch niedrigere* Anforderungen an dessen Gültigkeit zu formulieren als für die rechtfertigende Einwilligung in ihrer Funktion in einem Regime qualifizierter Personendatenverarbeitung (insb. gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG, der gleichzeitig als Basisregime sowie Integritätsschutz beschrieben wurde). Immerhin scheint Art. 4 Abs. 5 DSG hinsichtlich der Widerspruchslösung – neben Treu und Glauben sowie den auf die Figur zurückgeführten Transparenz- und Informationsvorgaben – insofern einen Einfluss gezeitigt zu haben, als eine Pflicht zur Informierung über ein Widerspruchsrecht vertreten wird.[1225]

4.4.2. Gültigkeitsvoraussetzungen

945 Die rechtfertigende Einwilligung und hierbei ihre *Freiwilligkeit* sowie *Ausdrücklichkeit* hat der EDÖB namentlich in seinem Schlussbericht i. S. Postfinance thematisiert.[1226] Der EDÖB ging von einer Verletzung der allgemeinen Verarbeitungsgrundsätze der Proportionalität, Zweckbindung sowie Datenrichtigkeit aus. Zu prüfen war, ob ein Rechtfertigungsgrund i. S. v. Art. 13 DSG für die nach Art. 12 Abs. 2 lit. a DSG persönlichkeitsverletzenden Verarbeitungen angeführt werden konnte. Mangels gesetzlicher Grundlage oder überwiegenden Interesses war die Einwilligung als Rechtfertigungsgrund zu prüfen.

946 Damit die rechtfertigende Einwilligung *gültig* ist, haben mehrere Untervoraussetzungen erfüllt zu sein: Die *Urteilsfähigkeit*, die *Informiertheit* und *Freiwilligkeit* sowie *das Fehlen von Willensmängeln*. *Ausdrücklich* muss die Einwilligung einzig bei der Weitergabe von besonders schutzwürdigen Angaben oder Persönlichkeitsprofilen an Dritte sein, wohingegen, *e contrario*, andernorts die konkludente Einwilligung genügt. Dazu gehört die stillschweigende Einwilligungserklärung, wobei sich Abgrenzungsschwierigkeiten ergeben zu dem bloss passiven Verhalten, dem Nichtstun oder Schweigen, was gemeinhin nicht als Einwilligung qualifiziert werden kann.[1227] Die Gültigkeitsvoraussetzungen gemäss DSG werden schlaglichtartig beleuchtet. Die Darstellung bezieht sich auf die Version vor

1225 Kritisch Rosenthal, HK-DSG, Art. 12 N 26.

1226 EDÖB, E-Banking bei Postfinance: Datenanalyse wird freiwillig sein, Bern 2015, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/finanzwesen/e-banking-bei-postfinance--datenanalyse-wird-freiwillig-sein.html> (zuletzt besucht am 30. April 2021); jüngst ist sodann auf den Entscheid des Bundesverwaltungsgerichts i. S. Helsana+, BVGer A-3548/2018, Urteil vom 19. März 2019 hinzuweisen, der sich ebenso mit der datenschutzrechtlichen Einwilligung befasst, wobei sich Abgrenzungsfragen betr. die Anwendbarkeit der Bestimmungen des DSG für den öffentlichen oder den privaten Bereich ergeben.

1227 Vgl. Rampini, BSK-DSG, Art. 13 N 9 ff.

Totalrevision. In Bezug auf die Neuerungen zur Einwilligung nach neuem Regime ist auf die sich erst entwickelnde Lehre zu verweisen.

947 Die *Urteilsfähigkeit* bezüglich der datenschutzrechtlichen Einwilligung wurde bislang nur am Rande thematisiert.[1228] Nicht spezifisch zur Urteilsfähigkeit, stattdessen allgemein hinsichtlich der Gültigkeitsanforderungen an die Einwilligung wird vertreten, dass die Anforderungen umso höher sind, je sensibler die Angaben sind oder je schwerer eine Persönlichkeitsverletzung wiegt.[1229] Eine solche Forderung entspricht der allgemeinen Lehre zur Urteilsfähigkeit, wonach diese *relativ* ist.[1230] Diese Relativität mit Blick auf die Urteilsfähigkeit findet folglich ihren Niederschlag im Rahmen der datenschutzrechtlichen Einwilligung. Je anspruchsvoller und weitreichender eine Datenverarbeitung, für die eine Einwilligung gefordert wird, ist, desto höher sind die Vorgaben an die Urteilsfähigkeit anzusetzen. Ob eine Person urteilsfähig ist, bestimmt sich stets anhand des konkreten Rechtsaktes und der konkreten Umstände der Situation. In Anbetracht der Komplexität von Personendatenverarbeitungsprozessen und den hierbei eingesetzten Technologien stellt sich selbstredend die Frage, wie viel Urteilsvermögen realistischerweise von einer Person verlangt werden kann, um gültige Einwilligungen in persönlichkeitsverletzende Datenverarbeitungen abgeben zu können. Einwilligungstatbestände und -erklärungen dürfen weder zu detailliert noch zu oberflächlich umschrieben werden.[1231]

948 Im Rahmen der Urteilsfähigkeit als Voraussetzung der datenschutzrechtlichen Einwilligung kommt dem Thema des *Minderjährigendatenschutzes* besondere Bedeutung zu.[1232] Unter dem Begriff werden diverse Herausforderungen und Phänomene diskutiert, namentlich die Nutzung sozialer Netzwerke durch Minderjährige selbst, aber auch das Phänomen der sog. Helikopter-Eltern, die mittels Geotracking ihre Kinder stets im Auge haben, sowie die Publikation von Kinderfotos durch die Eltern.[1233] Ein paar Hinweise mögen in diesem Zusammenhang

1228 Jüngst allerdings vertiefend Fasnacht, N 305 ff., insb. N 308 sowie N 251 ff.; entsprechend ist auch Bezug auf die zivilgesetzlichen Vorgaben zur Urteilsfähigkeit zu nehmen, Art. 16 ZGB.

1229 M. w. H. Rampini, BSK-DSG, Art. 13 N 3.

1230 Für Deutschland immerhin Rogosch, 48 ff.; für die Schweiz Fasnacht, N 306 ff.; Aebi-Müller, N 223; Meier, N 836; m. w. H. zur Relativität der Urteilsfähigkeit im Zusammenhang mit der persönlichkeitsrechtlichen Einwilligung sodann Haas, N 265 ff.

1231 Vgl. Passadelis/Roth, Jusletter vom 4. April 2016, N 19 ff.

1232 Fankhauser/Fischer, in: Fankhauser/Reusser/Schwander (Hrsg.), 193 ff.; EDÖB, 19. Tätigkeitsbericht zum Jugendschutz im Internet und 16. Tätigkeitsbericht; vgl. mit Hinweis auf die Empfehlungen des Europarates CM/Rec (2018) 7 zum Thema der Kinderrechte in der digitalen Welt Husi-Stämpfli, digma 2019, 84 ff.; zum Minderjährigendatenschutz und zur Einwilligungsfähigkeit von Minderjährigen nach DSGVO und insb. Art. 8 DSGVO Krüger/Vogelgesang/Weller, Jusletter IT vom 23. Februar 2017; vgl. sodann auch Fountoulakis, in: Arnet/Eitel/Jungo/Künzle (Hrsg.), 145 ff.

1233 Vgl. insofern immerhin Fasnacht, N 609 ff.; rechtlich interessant wäre in diesem Zusammenhang auch eine Analyse zum Bezug digitaler Güter durch Jugendliche im Internet; vgl. EU-IPO, Intellectual Property and Youth, Scoreboard 2016.

genügen. Im Jahr 2019 erhielt ein Lehrmittel des Datenschutzbeauftragten des Kantons Zürichs, dessen Inhalte Kinder zwischen vier und neun Jahren für Themen der Privatsphäre sensibilisieren sollte, einen internationalen Preis.[1234] Auch der EDÖB leistet wichtige Sensibilisierungsarbeit in Bezug auf den Umgang von Kindern und Jugendlichen mit den neuen Technologien, wobei er sich auch zur Einwilligung von Minderjährigen resp. der gesetzlichen Vertreter geäussert hat, ohne allerdings Konkretisierungen bezüglich der Urteilsfähigkeit zu machen.[1235]

949 Spezifisch mit Blick auf die Urteilsfähigkeit im Zusammenhang mit der datenschutzrechtlichen Einwilligung sei auf einen Entscheid des Oberlandesgerichts Hamm hingewiesen, der Minderjährigen selbst ab fünfzehn Jahren die erforderliche Reife absprach, um die Tragweite einer Einwilligungserklärung zur Datenspeicherung und -verwendung einzuschätzen.[1236] Die DSGVO befasst sich spezifisch mit der Einwilligung zur Nutzung von Diensten der Informationsgesellschaft durch Minderjährige, Art. 8 i. V. m. Art. 4 Nr. 25 DSGVO. Zudem ist der Umgang mit Personendaten von Kindern als Kriterium der Datenschutz-Folgenabschätzung, vgl. Art. 35 DSGVO, relevant.[1237] Art. 8 Abs. 1 DSGVO setzt das Mindestalter für die selbstständige Einwilligung auf sechzehn Jahre, wobei die nationalen Rechte gemäss Abs. 2 – eine der vielen Öffnungsklauseln der DSGVO – ein geringeres Alter vorsehen können.[1238] Indem sich die Norm auf die Nutzung von Diensten der Informationsgesellschaft beschränkt und eine Öffnungsklausel vorsieht, ist ihr Wirkungsbereich beschränkt.

950 In der Schweiz ist *de lege lata* auf die allgemeinen Vorgaben zur Handlungsfähigkeit zurückzugreifen. Die Totalrevision schafft keine spezifische Regelung. Das Persönlichkeitsrecht gilt als relativ höchstpersönliches Recht; urteilsfähige Minderjährige üben es selbst aus, vgl. Art. 19c Abs. 1 ZGB.[1239] Weil das Datenschutzgesetz für den privaten Sektor an das zivilrechtliche Persönlichkeitsrecht anknüpft, können Kinder und Jugendliche für den Fall, dass sie hinsichtlich einer

1234 Kanton Zürich, Datenschutz, Zürich 2019, <https://dsb.zh.ch/internet/datenschutzbeauftragter/de/aktuell/medienmitteilungen/2019/internationale-datenschutz-auszeichnung-fuer-den-kanton-zuerich.html> (zuletzt besucht am 30. April 2021).

1235 Vgl. insofern <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/jugend-und-internet.html> (zuletzt besucht am 3. Juni 2021); EDÖB, 19. Tätigkeitsbericht, 21; Ders., 16. Tätigkeitsbericht, 33 ff.

1236 Oberlandesgericht Hamm, I-4U 85/12, vom 20. September 2012. Dem Entscheid lag folgender Sachverhalt zugrunde: Eine Krankenkasse hatte Gewinnspielkarten auf einer Messe für Schüler und Jugendliche verteilt. Auf deren Rückseite waren Felder angebracht, in welche Adresse, Name, E-Mail eingetragen werden konnten. Die Angaben sollten für Werbezwecke genutzt werden, wobei sich unter diesen Zeilen die entsprechenden Datenschutzhinweise sowie die Einwilligungszeile befand. Unter dieser befand sich der Hinweis, dass bei Kindern unter 15 Jahren die elterliche Zustimmung nötig sei.

1237 Vgl. WP 29/248 rev. 01, Data Protection Impact Assessment, 10 ff.

1238 Vgl. m. w. H. Krüger/Vogelgesang/Weller, Jusletter IT vom 23. Februar 2017, insb. N 3.

1239 Vgl. Breitschmid, HK-ZGB, Art. 19c N 1 und N 5; dagegen mit Verweis auf eine allfällige Mitwirkung der gesetzlichen Vertreter bei der Geltendmachung der Rechte Rampini, BSK-DSG, Art. 12 N 1.

konkreten Datenverarbeitung urteilsfähig sind, gültig in eine Persönlichkeitsverletzung – auch durch Datenverarbeitungen – rechtfertigend einwilligen. Vertreten wird die Ankoppelung der Urteilsfähigkeit an das Alter von 13 Jahren.[1240] Bezüglich der datenschutzrechtlichen Einwilligung Minderjähriger stellt sich, ähnlich wie bei Volljährigen, die schwierige Frage, ob die Urteilsfähigkeit für eine sinnhafte Einwilligung hinsichtlich einer Bearbeitungshandlung tatsächlich gegeben ist. Eine zusätzliche Herausforderung im Internet liegt in der Verifizierung von Alter und Urteilsfähigkeit eines Kindes. Insofern wurden in den vergangenen Jahren verschiedene Technologien entwickelt, die der Verifizierung der Identität des Nutzers, seines Alters usf. dienen, beispielsweise die Video- oder Stimmauthentifizierung.[1241]

951 Von der datenschutzrechtlichen Einwilligung, die im System des Persönlichkeitsschutzes als Ausübung eines relativ höchstpersönlichen Rechts zu taxieren ist und von urteilsfähigen Minderjährigen selbstständig erteilt werden kann, sind Fragen der Geschäfts- resp. Vertragsfähigkeit abzugrenzen.[1242] Es ist hier nicht der Ort, um beispielsweise das Geschäfts- und Vertragsmodell von Facebook im Lichte des Handlungsfähigkeitsrechts und der Nutzung durch Jugendliche zu analysieren. Für die Geschäftsfähigkeit wird grundsätzlich die volle Handlungsfähigkeit, Volljährigkeit und Urteilsfähigkeit verlangt. Ausnahmsweise genügt die beschränkte Handlungsunfähigkeit, will heissen, dass von Gesetzes wegen die Handlungsunfähigkeit punktuell durchbrochen wird, soweit Minderjährige urteilsfähig sind. Ein Beispiel ist das zulässige rechtsgeschäftliche Handeln im Rahmen des freien Kindervermögens, Art. 321 Abs. 2 ZGB, resp. des Ausbildungslohnes, Art. 323 Abs. 1 ZGB, für den Fall, dass das Kind mit Blick auf die konkrete rechtsgeschäftliche Handlung urteilsfähig ist.

952 Nach Art. 19 Abs. 2 ZGB können Minderjährige sodann Vorteile erlangen, die unentgeltlich sind. Ob die Bestimmung für Verträge zur Nutzung von Online-Dienstleistungen wie Facebook anwendbar ist? Das Konto kostet bekanntermassen kein Geld. Ist ein Vertrag gleichwohl als entgeltlich zu qualifizieren, weil eine Gegenleistung in Gestalt von Personendaten erfolgt? Vor dem Hintergrund solcher Fragen und der jüngsten datenschutzrechtlichen Verschärfungen erstaunt es

1240 Vgl. Rosenthal, Jusletter vom 16. November 2021, N 30.

1241 Unternehmen wie die Swisscom lassen den Abschluss eines Mobilabonnements nur in einem Ladenlokal und mittels Vorlegung einer ID zu. Allgemein stellt sich die Frage, wie weit die Sorgfaltspflicht bei der Verifizierung des Alters geht, ob ein Vertrauen in das Anklicken eines Kästchens, wonach die Nutzerin ein Mindestalter erlangt hat, oder ob beispielsweise das Nachsenden einer ID-Kopie verlangt wird; zur Stimmauthentifizierung, wie sie Bankkundenverkehr eingesetzt wird, Emmenegger/Reber, in: Emmenegger (Hrsg.), 162 ff.; zur Gesichtserkennung Keist, Jusletter vom 20. Mai 2019 N 10 ff., mit einer Analyse der rechtlichen Vorgaben und Schranken.

1242 Insofern ist auf die einschlägige zivil- und personenrechtliche resp. vertragsrechtliche (Kommentar-)Literatur zu verweisen.

nicht, dass Facebook öfter die Einwilligung der Eltern verlangt.[1243] Die Einwilligung der Eltern würde auch den Vorgaben von Art. 19 Abs. 1 ZGB Rechnung tragen.

953 Nach diesem Einschub zur datenschutzrechtlichen Einwilligung von Minderjährigen als Kernthema der Gültigkeitsvoraussetzung der Urteilsfähigkeit *zurück zu den weiteren Gültigkeitsvoraussetzungen*. Über die Urteilsfähigkeit hinaus braucht es zudem, damit eine datenschutzrechtliche Einwilligung gültig erteilt werden kann, grundsätzlich zweierlei: die *Informiertheit und Freiwilligkeit* der Einwilligung, vgl. Art. 4 Abs. 5 DSG und Art. 6 Abs. 6 nDSG. Neuerdings gewinnt die Ausdrücklichkeit der Einwilligungserklärung an Bedeutung, vgl. Art. 6 Abs. 7 nDSG.

954 Teilweise zu Recht wird Art. 4 Abs. 5 DSG nicht als Bearbeitungsgrundsatz qualifiziert.[1244] Art. 4 Abs. 5 DSG besagt, dass dort, wo eine Einwilligung zur Bearbeitung verlangt wird, die Datenbearbeitung nur zulässig ist, wenn die Einwilligung nach *angemessener Information und freiwillig* erteilt wird. Verlangt wird insofern das Wissen um und das Verstehen von Kernelementen der Datenverarbeitung – Zweck, Umfang, Konsequenzen – mit einem daraus resultierenden Entscheid aus freiem Willen, die Einwilligung in die fragliche Verarbeitungshandlung zu erklären.[1245]

955 Zur *Informiertheit*: Sie ist verbunden mit der Maxime, wonach eine (gemäss DSG rechtfertigende) Einwilligung der *angemessenen Informiertheit* vorherzugehen hat.[1246] Mit der *Informiertheit* der Einwilligung befasste sich das Bundesverwaltungsgericht in seinem Entscheid BVGer 2009/44. Im Entscheid ging es um die Beurteilung eines Zutrittskontrollsystems in ein Schwimmbad, das den Missbrauch von Jahreskarten verhindern sollte. Der EDÖB hatte eine Empfehlung zur schonenderen Gestaltung der Zutrittskontrolle erlassen, die indes – auch mit einem Kostenargument – nicht umgesetzt wurde. Daraufhin reichte der EDÖB Klage beim Bundesverwaltungsgericht ein. Das Bundesverwaltungsgericht äusserte sich zum Sinn und Zweck des Erfordernisses der angemessenen Information und konkretisierte dessen Vorgaben wie folgt:

> «Das Erfordernis einer angemessenen Information will erreichen, dass die betroffene Person ihre Einwilligung in Kenntnis der Sachlage gibt, das heisst, erst entscheiden muss, wenn sie sich ein Bild (auch) über die möglichen negativen Folgen ihrer Einwilligung machen konnte. Erforderlich, aber auch genügend ist letztlich, dass sich die betroffene Per-

1243 Computer Bild, Facebook: Datenschutz-Änderung für Jugendliche, Zürich 2018, <https://www.computerbild.de/artikel/cb-News-Internet-Facebook-Datenschutz-Eltern-Gesichtserkennung-21533117.html> (zuletzt besucht am 30. April 2021).

1244 Rosenthal, HK-DSG, Art. 12 Abs. 2 N 14 f.

1245 Vgl. Rampini, BSK-DSG, Art. 13 N 4.

1246 Hierzu Fasnacht, N 249 ff.; Heuberger, N 229 und N 281 ff.; Bühlmann/Schüepp, Jusletter vom 15. März 2021; Vasella, Jusletter vom 16. November 2015.

> son im Klaren darüber sein kann, worin sie einwilligen soll, das heisst, was die Tragweite ihrer Entscheidung ist. Je nach Situation wird eine Aufklärung erforderlich sein, die nicht nur auf die Umstände der Datenbearbeitung, sondern auch auf ihre wichtigsten möglichen Risiken bzw. Folgen für die betroffene Person hinweist, insbesondere wenn diese schwerwiegend sind. Ob und wie weit diesbezüglich informiert werden muss, hängt letztlich aber von den konkreten Umständen ab (ROSENTHAL/JÖHRI, a. a. O., Art. 4 Abs. 5 N 72 f.).»[1247]

Eine gültige Einwilligung im Sinne der *informierten* Einwilligung bedingt, dass die betroffene Person sich zumindest ein Bild machen kann über die Auswirkungen ihrer Einwilligung resp. der daraus folgenden Datenbearbeitung, in die sie einwilligt.[1248] Die datenbearbeitenden Stellen trifft eine entsprechende Informationspflicht. 956

Insofern stellt sich nicht nur die Frage nach der rechtsgenügenden Einbettung entsprechender Informationen in AGB, sondern namentlich auch diejenige nach dem Detailgrad und der Granularität der datenschutzrechtlichen Informierung als Voraussetzung einer gültigen Einwilligung.[1249] In den Worten von Radlanski: 957

> «Sollte man diese Voraussetzung wörtlich verstehen, würde dies darauf hinauslaufen, den Betroffenen für manche Einwilligungserklärungen speziell ausbilden zu müssen: Um beispielsweise genau zu erfassen, welche Implikationen die Einwilligungserklärungen bei Inbetriebnahme eines neuen Smartphones hat, müsste man bestenfalls Informatik studiert haben, oder sich zumindest extrem detailliert mit der Materie auseinandergesetzt haben. Bei den meisten Betroffenen dürfte dies nicht der Fall sein, weswegen man durchaus von einer „Illusion der umfassenden Informiertheit" sprechen kann».[1250]

Unter Umständen entsteht eine kaum zu überbrückende Leerstelle zwischen *Informierung als Pflicht der Verarbeitenden* und *Informiertheit* als Zustand und Ergebnis aufseiten des Datensubjektes. 958

Die DSGVO sowie die Totalrevision des DSG generieren ein erhöhtes Transparenzniveau, womit ebenso ein Effekt auf die Vorgaben an die Informierung und Informiertheit der Einwilligung einhergeht.[1251] Mittlerweile hat sich eine Praxis durchgesetzt, die Transparenzerfordernisse mittels *eigenständiger Privacy-Erklärungen* zu gewährleisten. Um den Vorgaben unter dem Regime der DSGVO zu genügen, sind Einwilligungserklärungen in einem separaten Block spezifisch zu erfassen. Die *Informiertheit*, welche die Kenntnis des Datensubjektes zumindest in groben Zügen über Gegenstand, Zweck, Umfang und Konsequenzen seiner Einwilligung bedingt, begründet vonseiten der Verantwortlichen die Pflicht, die- 959

1247 BVGer 2009/44, Urteil vom 4. August 2009, Regeste 4.
1248 Vgl. Rampini, BSK-DSG, Art. 13 N 4; präzisierend Rosenthal, HK-DSG, Art. 4 N 72 f.
1249 Vertiefend zur Informiertheit und datenschutzrechtlichen Einwilligung Bühlmann/Schüepp, Jusletter vom 15. März 2021; Vasella, Jusletter vom 16. November 2015.
1250 Radlanski, 16, m. w. H.
1251 Beachte insb. WP 29/259, Consent; Passadelis/Roth, Jusletter vom 4. April 2016, N 19 ff.

ses Wissen zu generieren.[1252] Die Zeiten, in denen pauschale Einwilligungserklärungen im Kleingedruckten von AGB als dem Erfordernis Rechnung tragend beurteilt wurden, gehören damit der Vergangenheit an.[1253]

960 Zur *Freiwilligkeit* der Einwilligung als weiterer Gültigkeitsvoraussetzung:[1254] In Bezug auf diese Voraussetzung sind in erster Linie negative Umschreibungen zu finden. Ungültig, weil unfreiwillig, sind Einwilligungen unbestritten zunächst, wenn diese nach Täuschung, unter Zwang oder Drohung erteilt werden.[1255] Sodann beschlagen die fehlende Informiertheit und wohl auch das Missverständnis oder die Fehlinterpretation die Freiwilligkeit einer Einwilligung.[1256] Fehlt der geforderte Grad an Verständnis über die Bearbeitung und deren Folgen, kann auch nicht freiwillig eingewilligt werden. Positiv, aber mit wenig Erkenntnisgewinn mittels Wortspalterei das Bundesverwaltungsgericht:

> «Eine Einwilligung muss freiwillig erfolgen, das heisst, Ausdruck des freien Willens der betroffenen Person sein.»[1257]

961 Aussagekräftiger dagegen die Regeste 4 von BVGer 2009/44:

> «Das Erfordernis einer angemessenen Information will erreichen, dass die betroffene Person ihre Einwilligung in Kenntnis der Sachlage gibt, das heisst, erst entscheiden muss, wenn sie sich ein Bild (auch) über die möglichen negativen Folgen ihrer Einwilligung machen konnte. Eine Einwilligung muss zudem freiwillig erfolgen. Der betroffenen Person muss „eine – mit nicht unzumutbaren Nachteilen behaftete – Handlungsalternative" zur Verfügung stehen (E. 4.2).»

962 Nach wohl herrschender Lehre, Rechtsprechung sowie den Materialien gilt eine Einwilligung dann als unfreiwillig, wenn ihre Verweigerung Nachteile mit sich bringt, die in keinem sachlichen Zusammenhang zum Bearbeitungszweck stehen oder aus anderen Gründen unverhältnismässig sind.[1258] Insb. die Konstellation, in welcher die Erteilung der Einwilligung zur Datenverarbeitung *conditio sine qua non* für den Zugang zu Dienstleistungen oder Produkten ist, hat in der Schweiz Rechtsprechung, Lehre und EDÖB beschäftigt. Hierbei setzte sich die Auffassung durch, wonach eine datenschutzrechtliche Einwilligung dann nicht als freiwillig gilt, wenn sie Voraussetzung für den Zugang zu einer Dienstleistung oder einem

1252 Rampini, BK-DSG, Art. 13 N 4.
1253 Passadelis/Roth, Jusletter vom 4. April 2016, N 22.
1254 Hierzu auch Vasella, Jusletter vom 16. November 2015, N 7 und N 14 ff.; kritisch zur datenschutzrechtlichen Freiwilligkeit der Einwilligung, auch unter Bezug auf Erfahrungen aus dem AGB-Bereich, bereits Simitis, in: Schlemmer (Hrsg.), 67 ff., 77.
1255 Rampini, BSK-DSG, Art. 13 N 4; Radlanski, 12 f.; BVGer 2009/44, Urteil vom 4. August 2009, E 4.2.
1256 Zum Konnex Vasella, Jusletter vom 16. November 2015, N 14.
1257 BVGer 2009/44, Urteil vom 4. August 2009, E 4.2.
1258 M. w. H. Vasella, Jusletter vom 16. November 2015, N 14.

Produkt ist, selbst wenn es insofern Ausweichmöglichkeiten gäbe, diese indes mit unzumutbaren Nachteilen verbunden wären.[1259]

963 Ein spezifisches Kopplungsverbot implementiert die DSGVO mit Art. 7 Abs. 4 DSGVO. Das datenschutzrechtliche Kopplungsverbot geht davon aus, dass die Erbringung einer Dienstleistung oder Erfüllung eines Vertrages nicht von einer datenschutzrechtlichen Einwilligung abhängig gemacht werden darf, die hierfür nicht erforderlich ist. Damit werden «überschiessende Einwilligungen» verhindert.[1260]

964 Kernherausforderungen der Freiwilligkeit als Gültigkeitsvoraussetzung der datenschutzrechtlichen Einwilligung bilden somit eine Machtasymmetrie sowie die Abhängigkeit von Dienstleistungen oder Produkten, die Gefährdung durch übermässige Reize oder durch sozialen Druck. Es handelt sich um Konstellationen, die allesamt in der Regel nicht die Intensität der Tatbestände des Zwanges oder der Drohung erreichen, gleichwohl die autonome Entscheidung des Subjektes beeinträchtigen können.[1261]

965 Im Rahmen der Auseinandersetzungen mit den Gültigkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung – *Urteilsfähigkeit*, *Informiertheit sowie Freiwilligkeit* – wurden Schwächen der Einwilligungsvoraussetzungen im Lichte der datenschutzrechtlichen Realität problematisiert. Gefolgert wird hieraus, dass die Einwilligungskonstruktion für verschiedene Konstellationen nicht tragfähig sei.[1262] In Kürze: Die Informiertheit lässt sich in Anbetracht der Komplexität der Verarbeitungsprozesse und Verarbeitungstechnologien faktisch kaum je erreichen.[1263] Die Freiwilligkeit wird nicht selten durch mehrere Einflüsse untergraben, allem voran infolge einer strukturellen Unterlegenheit mit der Mechanik eines «take it or leave it» oder aufgrund von übermässigen Anreizen.[1264] Folglich wird die Strategie des «notice and consent» grundlegend in Frage gestellt.[1265]

966 Gleichwohl gilt die informierte Einwilligung – wie es namentlich auch an den europäischen Rechtsentwicklungen unübersehbar ist – als ein Hauptlösungsansatz zur Bewältigung datenschutzrechtlicher Herausforderungen.[1266] Das *Selbst-*

1259 BVGer 2009/44, Urteil vom 4. August 2009, E 4.2.; m. w. H. und zugleich kritisch Vasella, Jusletter vom 16. November 2015, N 14.

1260 Vgl. Art. 7 Abs. 4 DSGVO; Ingold, Nomos-Komm DSGVO, Art. 7 N 31 f.; hierzu auch Vasella, Jusletter vom 16. November 2015, N 14; m. w. H. Heuberger, N 295.

1261 Hierzu Radlanski, 14 ff.

1262 Kritisch insb. Ders., 78 ff.; zu take it or leave it Buchner, 107 ff.; Heuberger, N 295; Barocas/Nissenbaum, 1 ff.

1263 Vgl. Rogosch, 71 ff.; Barocas/Nissenbaum, 1 ff.

1264 Grundlegend Radlanski, 78 ff.

1265 Barocas/Nissenbaum, 1 ff.; Radlanski, *passim*; kritisch unlängst auch Heuberger, *passim*; kritisch hinterfragt auch durch Passadelis, Gastkommentar NZZ vom 17. Mai 2017.

1266 Vgl. Buchner, 231 ff.; Barocas/Nissenbaum, 1 ff.; illustrativ hierfür ist der Befund, wonach sich der grosse Teil wissenschaftlicher Beiträge zum Datenschutz mit der informierten Einwilligung resp.

bestimmungsparadigma zeigt sich als logische Fortsetzung und Konsequenz eines im Persönlichkeitsschutz und damit im Subjektschutz verwurzelten Datenschutzrechts mit entsprechenden Kognitionen (Degradierung des Menschen zum Informationsobjekt qua Technologie, Emanzipationsbedarf).[1267]

967 Buchner problematisierte von wissenschaftlicher Seite den Befund, wonach Personendaten über weiteste Strecken an den Datensubjekten vorbei verarbeitet würden.[1268] Die Reaktion hierauf lässt sich durchaus als Trend beschreiben, ein subjektives Recht auf informationelle Selbstbestimmung zu stärken, auszubauen, wirksam zu machen. Es geht an dieser Stelle nicht darum, in die dogmatischen Tiefen einzugehen, zumal sich für viele Fragen erst Antworten durch Lehre und Praxis konsolidieren müssen. Allerdings riskiert eine entsprechende Betrachtungsweise, den Subjektschutz so stark in den Vordergrund zu rücken, dass die systemische Schutzdimension des Datenschutzes in den Hintergrund rückt. Wie eine Lösungsstrategie der Stärkung der Einwilligungsvorgaben als Instrumentarium zur Bewältigung datenschutzrechtlicher Herausforderungen zu evaluieren ist, wird im dritten Teil vertieft analysiert. Ebenda wird auch gezeigt, dass das *Einwilligungs- und Transparenzparadigma durch weitere Strategien paradigmatischer Natur ergänzt werden.*

968 Gleichwohl nahmen in den vergangenen Jahren Anpassungen und namentlich die Stärkung sowie Ausdifferenzierung der Vorgaben für die Gültigkeit der datenschutzrechtlichen Einwilligung (ungeachtet ihrer Positionierung im System) einen prominenten Platz in den datenschutzrechtlichen Entwicklungen ein. Sowohl die DSGVO als auch die Totalrevision des DSG heben die Anforderungen an die Gültigkeitsvoraussetzungen der Einwilligung an. Mit der Totalrevision gewinnen insb. die Informationsvorgaben, aber auch die Anforderungen an die Einwilligungserklärung und damit die Ausdrücklichkeit an Bedeutung. Die ausgebauten Vorgaben sollen die datenschutzrechtliche Einwilligung effektuieren. Damit bestätigt sich denn auch, dass in den Einwilligungskonstruktionen ein Kerninstrument zur Lösung der datenschutzrechtlichen Probleme gesehen wird.

969 Um das Bild mit Blick auf die Gültigkeitsvoraussetzungen abzurunden, ist in gebotener Kürze auf eine qualifizierende Vorgabe an die Einwilligung, die *Ausdrücklichkeit*, einzugehen (vgl. hierzu bereits oben im Rahmen der Erläuterung des Widerspruchsrechts): Qualifizierend wird nach Art. 4 Abs. 5 DSG die *Ausdrücklichkeit der Einwilligung* verlangt für die Verarbeitung von besonders schutzwürdigen Angaben und Persönlichkeitsprofilen. Art. 6 Abs. 7 nDSG ver-

Selbstbestimmung resp. dem Recht an eigenen Daten befassen; vertiefend hierzu dritter Teil, VIII. Kapitel, B.

1267 Zur gesellschaftlichen Konstruktion einer normativen Leitidee der Selbstbestimmung Krähnke, 9 ff.

1268 Vgl. Buchner, 130 ff.

langt die Ausdrücklichkeit neu für teilweise andere Konstellationen. Die nachfolgenden Ausführungen beziehen sich auf die Vorgaben vor Totalrevision.[1269]

970 Auch der Passus nach noch in Kraft stehendem Gesetz ist aus materiellrechtlicher Perspektive erklärungsbedürftig, der Gesetzeswortlaut unklar. Erneut suggeriert der Gesetzgeber ebenso für diese Konstellation, dass ein Einwilligungserfordernis, und zwar in qualifizierter Form, für die Personendatenverarbeitung von besonders schutzwürdigen Angaben und Persönlichkeitsprofilen greift. Allerdings ergibt eine systematische Auslegung, die neben Art. 4 Abs. 5 erster Satz DSG zugleich auch Art. 12 Abs. 2 lit. c DSG in die Analyse miteinbezieht, selbst für diese Konstellation kein eigenständiges Einwilligungserfordernis. Hierfür spricht an erster Stelle das dargelegte System mit dem Ausgangspunkt der prinzipiellen Verarbeitungsfreiheit. Zudem wird nach Art. 12 Abs. 2 lit. c DSG erst die Weitergabe von Personendaten und Persönlichkeitsprofilen an Dritte entgegen einem Widerspruch als Persönlichkeitsverletzung taxiert. Die dergestalt qualifizierte und damit persönlichkeitsverletzende Verarbeitungshandlung kann wiederum gerechtfertigt werden. Was folgt, ist, dass keineswegs jede Verarbeitung von Personendaten, nicht einmal diejenige von besonders schutzwürdigen Personendaten oder von Persönlichkeitsprofilen einer Einwilligung bedarf. Sodann schliesst der zweite Satz an den ersten Satz von Art. 4 Abs. 5 DSG an, wobei ersterer wie gesagt die Gültigkeitsvoraussetzungen für eine Einwilligung definiert für den Fall, dass diese (andernorts) verlangt wird. Die Auslegung, wonach eine Personendatenverarbeitung von besonders schutzwürdigen Personendaten und Persönlichkeitsprofilen der Einwilligung bedarf, hat im Gesetz keine Grundlage. Lediglich eine persönlichkeitsverletzende Verarbeitung von besonders schutzwürdigen Personendaten und Persönlichkeitsprofilen – exemplarisch diejenige, welche die allgemeinen Verarbeitungsgrundsätze nicht einhält – bedarf der Rechtfertigung, beispielsweise qua Einwilligung, die alsdann ausdrücklich zu sein hat. Immerhin mag es gerade im Rahmen der Verarbeitung von Persönlichkeitsprofilen faktisch nicht selten der Fall sein, dass diese gegen die Verarbeitungsgrundsätze verstossen. Auch Art. 4 Abs. 5 zweiter Satz DSG stellt damit erhöhte Anforderungen an die Gültigkeit der Einwilligung für den Fall, dass es sich um einen persönlichkeitsverletzenden Datenumgang mit besonders schützenswerten Angaben oder Persönlichkeitsprofilen handelt.

971 Für den Fall, dass eine persönlichkeitsverletzende Verarbeitung von besonders schutzwürdigen Personendaten oder Persönlichkeitsprofilen vorliegt und die ausdrückliche Einwilligung als Rechtfertigungsgrund figuriert, fragt sich alsdann, wann die Voraussetzung der *ausdrücklichen* Einwilligung erfüllt ist. Mit der *Ausdrücklichkeit* einer Einwilligung kann Verschiedenes gemeint sein: Zum einen

1269 Zu den Neuerungen vgl. insb. Bühlmann/Schüepp, Jusletter vom 15. März 2021; Vasella, Jusletter vom 16. November 2015.

kann es um die Art resp. Form der Kundgabe der Einwilligungserklärung gehen. Zum anderen kann sich das Adjektiv «ausdrücklich» nicht auf die Kundgabe, die Erklärung der Einwilligung, sondern auf den Inhalt der datenschutzrechtlichen Einwilligung beziehen. Problematisch in dieser Lesart sind dann Einwilligungen anhand von AGB, die sich auch, aber keineswegs nur auf die Datenverarbeitung beziehen.[1270] Epiney verschränkt die beiden Lesarten, indem sie verlangt, dass die Einwilligung nach Inhalt wie nach Form ausdrücklich zu sein hat.[1271] Nach wohl herrschender Schweizer Lehre wird «ausdrücklich» als Gegenbegriff zu stillschweigend resp. konkludent verstanden.[1272] Hält man sich vor Augen, dass zahlreiche Einwilligungen online und formulartechnisch erfolgen, wobei sich Nutzende in aller Regel passiv verhalten, sollte unter der Voraussetzung der Ausdrücklichkeit die *aktive Erklärung* verlangt werden.[1273] Ist neben dem einschlägigen Text ein leeres Kästchen angebracht und muss die Einwilligung aktiv gesetzt werden, ist von einer ausdrücklichen Einwilligung auszugehen. Nicht als ausdrücklich gelten kann indes eine Modalität, in der die Checkbox leer ist und das Leerlassen als vermutete Einwilligung gilt. Epiney ist sodann zuzustimmen, dass sich die ausdrückliche Einwilligung, sprich, die aktive Einwilligungserklärung eindeutig auf die datenschutzrechtliche Dimension und deren Inhalt beziehen muss. Sind datenschutzrechtlich mehrere Prozesse und namentlich Verarbeitungszwecke relevant, sind weiter die Erklärungen entsprechend ausdifferenziert zu gestalten und hierfür jeweils separat ausdrückliche Einwilligungen einzuholen. Mit einer so verstandenen *Ausdrücklichkeitsvorgabe* wird ein Konzept der Relativität und Ausdifferenzierung von Einwilligungsvorgaben konkretisiert. In eine solche Richtung scheint auch die Argumentation des EDÖB im Schlussbericht Postfinance zu zielen.[1274]

972 Damit die Analyse im Sinne der bisherigen Systematisierung dieser Arbeit abgerundet wird, ist zum Abschluss der Ausführungen zu den Gültigkeitsvoraussetzungen der Einwilligung (mit einer Abgrenzung zum Einwilligungserfordernis an sich) ein *struktureller Aspekt der Thematik* zu adressieren: Mit Blick auf die Anforderungen an die Gültigkeit datenschutzrechtlicher Einwilligungen wird hinsichtlich der erforderlichen Granularität von Information und Erklärungsinhalt vertreten, dass diese umso höher ist, je sensibler die Angaben resp. je

1270 In diese Richtung EDÖB, Schlussbericht vom 1. Juni 2015 i. S. PostFinance, 1 ff., 24 f.
1271 Epiney, in: Rumo-Jungo/Pichonnaz/Hürlimann-Kaup/Fountoulakis (Hrsg.), 97 ff., 103; Dies., in: Belser/Epiney/Waldmann (Hrsg.), § 9 N 19; Meier, N 899.
1272 M. w. H. Vasella, Jusletter vom 16. November 2015, N 25 ff.
1273 So auch WP 29/259, Consent, 20 f.
1274 Vgl. mit Blick auf die Ausdrücklichkeit und den Schlussbericht vertiefend Jusletter vom 16. November 2015, N 23; zur Problematik der globalen resp. «überschiessenden» Einwilligung, indes nicht spezifisch mit Blick auf die qualifizierenden Gültigkeitsvoraussetzungen der Ausdrücklichkeit der Einwilligung für den Fall von Art. 4 Abs. 5 zweiter Satz: BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, vgl. insb. E 4.8.3.

weitreichender eine Datenverarbeitung und deren Folgen sind.[1275] Eine entsprechende Relativität und Nuancierung fliesst, wie erörtert, über sämtliche Gültigkeitsvoraussetzungen ein, namentlich die Urteilsfähigkeit, die Informiertheit und Ausdrücklichkeit (sofern qualifizierend verlangt), aber auch die Freiwilligkeit. Gerade in der Anknüpfung der «Granularitätsvorgaben» resp. «Nuancierungsvorgaben», der Relativität und Staffelung bezüglich der Einwilligung lässt sich erneut ein Konzept einer abstrakten Bestimmung der Natur von Personendaten erkennen. Auch hier bilden sich Relikte der Sphärentheorie ab. Das DSG bleibt selbst an dieser Stelle, wo es um einen Mechanismus zur Integration der Entscheidungsfreiheit des Subjektes geht, einer Konstruktion verhaftet, welche das Schutzniveau gewissermassen anhand der *Natur* gewisser Angaben als «mehr oder minder sensibel» vornimmt.

973 Dass eine abstrakte Definierung der Schutzwürdigkeit dem Konzept des DSG entspricht und diese sich ebenso auf die Anforderungen im Rahmen der Einwilligung niederschlägt, wird u. a. von Vasella vertreten.[1276] Er kritisiert Ansätze, wonach die «Natur» personenbezogener Angaben nicht abstrakt zu bestimmen, stattdessen auch auf den *Verarbeitungszusammenhang abzustellen sei*, was namentlich vonseiten des EDÖB vertreten werde.[1277] Auch diese Schrift hat an mehreren Stellen einen entsprechenden Ansatz des DSG freigelegt. Etwas allgemeiner wurde wiederholt sichtbar, wie kontextuelle Bezugspunkte ebenso im DSG angelegt sind.

974 Es folgt eine Zusammenfassung der Kernerkenntnisse zum *Rechtfertigungsregime gemäss DSG*. Im Anschluss werden Einwilligungskonstruktionen aus einer erweiterten Perspektive beleuchtet. Es geht ebenda darum, die relative und kontextrelationale Bedeutung datenschutzrechtlicher Normen und die Einschlägigkeit spezifischer Differenzierungen anhand anderer Einwilligungskonstruktionen hinsichtlich des Umgangs mit Personendaten freizulegen. Hier wird sich zeigen, dass es in Bezug auf den Umgang mit Personendaten verschiedene Regelungen gibt.

5. Resümee zu den Rechtfertigungsgründen

975 Die datenschutzgesetzlichen Rechtfertigungsgründe entsprechen dem Regime, wie es im Persönlichkeitsschutz des ZGB vorgesehen wird, vgl. Art. 28 Abs. 2 ZGB und Art. 13 Abs. 1 DSG resp. Art. 31 nDSG. Die mit Blick auf die datenschutzrechtlichen Rechtfertigungsgründe lange im Zentrum der Diskussionen stehende Frage, wie die uneinheitliche Fassung des Gesetzestextes in den Art. 12

1275 Rampini, BSK-DSG, Art. 13 N 3; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 16; Botschaft DSG 2013, 2127.
1276 M. w. H. auf die weiteren Lehrmeinungen Vasella, Jusletter vom 16. November 2015, N 7.
1277 Ders., a. a. O., N 5.

Abs. 2 lit. a–c DSG zu interpretieren sei, gilt als geklärt. Für sämtliche Tatbestände ist die Möglichkeit der Rechtfertigung grundsätzlich zuzulassen; allerdings hat dies namentlich bei einem Verstoss gegen den «Integritätsschutz» gemäss Art. 12 Abs. 2 lit. a DSG mit Zurückhaltung zu erfolgen. Nach Totalrevision werden die Tatbestände der Persönlichkeitsverletzung konsequent in Art. 30 nDSG, die Rechtfertigungsgründe in Art. 31 nDSG niedergelegt. Die gebotene Zurückhaltung der Rechtfertigungsmöglichkeit in Bezug auf die wichtigsten Verarbeitungsgrundsätze, Art. 6 und Art. 8 nDSG, ist weiterhin angezeigt.

976 Wenig Anlass zu Schwierigkeiten scheinen die *gesetzlichen Rechtfertigungsgründe* zu geben. Immerhin wird das letzte Kapitel dieser Studie zeigen, dass dies ein Trugschluss ist. Für sie wurde eine *Brückenfunktion* beschrieben, indem legitimierende Gesetzestatbestände ausserhalb des DSG der Funktionstüchtigkeit und dem Schutz der Integrität jeweils spezifischer Kontexte mit ebenda zu erreichenden Zielen dienen.

977 Als neuralgisch gelten in der datenschutzrechtlichen Debatte die *überwiegenden Interessen*, die als «Supergeneralklauseln» oder Blanko-Ermächtigungsnormen zur nahezu unbeschränkten Geltendmachung verführen. In Bezug auf die überwiegenden Interessen wurde vertreten, dass ein isolierter Blick auf wirtschaftliche Interessen zu kurz greift; vielmehr ist stets zu analysieren, welche Ziele und Zwecke im Rahmen der Verarbeitungskontexte, in welche die persönlichkeitsverletzenden Verarbeitungshandlungen eingebettet sind, verfolgt werden. Der Kontextbezug ist im Gesetz mit den Enumerationen gemäss Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG angelegt. Somit wurde dafür plädiert, die überwiegenden Interessen aus einer isolierten Perspektive individueller Interessen der Verantwortlichen zu lösen und einer kontextuellen Einbettung zuzuführen. *De lege ferenda* sind sie in eine Richtung zu strukturieren, welche die diversen Verarbeitungszusammenhänge mit den (direkten und indirekten) kontextuellen Zielen und Zwecken harmonisiert. Ein rein wirtschaftliches Interesse der Verantwortlichen, das nahezu für jede Personendatenverarbeitung aufführbar ist, kann isoliert *nur* ausnahmsweise als überwiegend gelten.

978 Folgerichtig zum Ausgangspunkt der grundsätzlichen Verarbeitungsfreiheit mit Schranken integriert das DSG für den privaten Bereich den *Willen des Datensubjektes* (neben dem Widerspruch) – insb. als *rechtfertigende Einwilligung* gegenüber qualifizierten und damit persönlichkeitsverletzenden Personendatenverarbeitungen. Die Ausführungen hierzu bestätigten, dass es fehlgeht, das System des DSG für den privaten Bereich als eines der informationellen Selbstbestimmung zu qualifizieren, wie es in seinem Gehalt vom Bundesverfassungsgericht in dessen Volkszählungsurteil geprägt wurde. Art. 4 Abs. 5 DSG statuiert kein eigenständiges Einwilligungserfordernis, stattdessen die Gültigkeitsvorgaben für die Einwilligung, sofern diese gefordert wird. Dasselbe gilt nach Totalrevision für Art. 6

Abs. 6 und Abs. 7 nDSG. Allgemein ist in der Stärkung der Transparenzvorgaben und der Einwilligungsvorgaben ein Lösungsansatz zu verorten, welcher die jüngsten datenschutzrechtlichen Entwicklungen mitprägt.

979 Dargestellt wurden die *einzelnen Gültigkeitsvoraussetzungen* der rechtfertigenden Einwilligung. Insofern wurde vor Augen geführt, dass die *Tauglichkeit* von Einwilligungskonstruktionen zur Lösung datenschutzrechtlicher Herausforderungen mit ihren Gültigkeitsvorgaben (Urteilsfähigkeit, Informiertheit und Freiwilligkeit, qualifizierend ggf. Ausdrücklichkeit) im Lichte der datenschutzrechtlichen Realität in jüngster Zeit ebenso *kritisch* thematisiert wird. Für die datenschutzrechtliche Einwilligung, die im DSG primär als Rechtfertigungsgrund figuriert, wurde zudem gezeigt, inwiefern auch hier das DSG in erster Linie von einer abstrakten Qualifizierung von Personendaten – quasi anhand ihrer Natur – als besonders schutzwürdig oder sensibel ausgeht, worin sich erneut die Verhaftung in der Sphärentheorie spiegelt. Das Datensubjekt, die Person und Persönlichkeit, wird bis heute als ein *einheitliches Subjekt perzipiert*, wobei ihm Personendaten quasi abstrakt qualifiziert und objekthaft zugeordnet werden anhand der um die Person gelegten konzentrischen Kreise.[1278] Der datenschutzgesetzlich geschützte Autonomieraum zeigt sich zumindest auf den ersten Blick als wenig ausdifferenziert. Erweitert man die Betrachtung über das DSG hinaus, werden die *ausdifferenzierten Autonomiebereiche resp. abgestuften Schutzpositionen in Bezug auf den Willen im Umgang mit Personendaten* sichtbar.

6. Diversifizierte Autonomien, plurale Verarbeitungskontexte

6.1. Bezugsrahmen

980 Nachgewiesen wurde, dass das DSG für den privaten Bereich kein Regime der informationellen Selbstbestimmung verankert (isoliert oder alternativ zu anderen Erlaubnistatbeständen), aus welchem ein prinzipielles Verarbeitungsverbot abgeleitet wird und die Einwilligung entsprechend einen Erlaubnistatbestand für die nicht qualifizierte Personendatenverarbeitung darstellt.[1279] Das Konzept des DSG lässt sich aufgrund des Ausgangspunktes der Freiheit der Personendatenverarbeitung mit Schranken am trefflichsten als Konzept des *Integritätsschutzes* be-

1278 Ein interessantes Erklärungsmuster könnte bei Page, 27, aufgespürt werden: Der Autor weist auf die Unterscheidung zwischen der individuellen Person, Selbstbestimmung sowie der sozialen Person hin. Wenn im Privatheitsschutz und Datenschutzrecht das Individuum mit seiner Autonomie in den Vordergrund gerückt wird sowie die gesamte Bedrohungslage für das Recht in der Technik verdichtet wird, dann rückt fast zwingend die Relevanz des Menschen, eingebunden in seine sozialen Realitäten und damit auch agierend in verschiedenen sozialen Rollen, in den Hintergrund.

1279 Zur Lehre und Rechtsprechung, die nicht unwesentlich zur Verwirrung mit Blick auf die Qualifizierung des Regimes des DSG für den privaten Bereich beigetragen haben, vertiefend dritter Teil, VII. Kapitel, A.

schreiben. In diesem wird der Wille des Subjektes als Ausdruck eines Autonomieschutzes zurückgestuft. Er figuriert lediglich als Widerspruch resp. rechtfertigende Einwilligung (gegenüber qualifizierten und damit persönlichkeitsverletzenden Personendatenverarbeitungen). Ein Recht an eigenen Daten im Sinne eines Herrschaftsrechts des Datensubjektes findet damit im Gesetz keine Verbürgung.[1280]

981 Ebendieser Befund wird nachfolgend weiter untermauert. Zwei Themen werden hierzu aufgegriffen: Erstens geht es um die Konstruktion und Gestaltung des *zivilrechtlichen Rechts am eigenen Bild*. Zweitens werden die für den Kontext des *Biomedizinrechts* spezialgesetzlich vorgesehenen Einwilligungskonstruktionen zum Umgang mit Personendaten dargestellt.

982 Mit dieser Betrachtung der erweiterten Landschaft von Einwilligungskonstruktionen im Zusammenhang mit Personendaten wird gezeigt, inwiefern das Recht den Willen des Datensubjektes zur Regulierung von Personendatenverarbeitungen differenziert einsetzt. Hinsichtlich der Ordnung des DSG lassen sich daraus weitere Erkenntnisse zu Ziel und Funktion nicht nur der Einwilligung des Datensubjektes generieren, sondern darüber hinausgehend für das *Datenschutzrecht – das mehr ist als das DSG – an sich*.

983 Gezeigt werden soll, dass es ein «einheitliches» Datensubjekt mit einer «einheitlichen Autonomie und Selbstbestimmung» nicht gibt. Vielmehr präsentiert sich das Datensubjekt vor dem Hintergrund verschiedener Verarbeitungszusammenhänge und unterschiedlicher Bereiche in *unterschiedlichen Rollen mit differenzierten Autonomieräumen*. Das Schweizer Recht ist gemäss einer integrativen Betrachtung der Rechtslandschaft, die sich mit dem Umgang mit Personendaten befasst, weit davon entfernt, dem Datensubjekt eine einheitlich strukturierte Entscheidungsbefugnis hinsichtlich des Umgangs mit «seinen» Personendaten einzuräumen.

6.2. Das Recht am eigenen Bild – gerichtlich anerkanntes Sonderregime

984 Die rechtliche Ausdifferenzierung der Autonomiegrade hinsichtlich des Umgangs mit Personendaten wird – *erstens* – sichtbar, wenn die Betrachtung der Normierung im DSG um diejenige des sog. *Rechts am eigenen Bild* ergänzt wird.[1281]

1280 Zur Diskussion auch unter dem Titel eines Eigentums an Personendaten u. a. Thouvenin, SJZ 2017, 21 ff.

1281 Vertiefend hierzu Bächli, *passim*; jüngst namentlich in Bezug auf die Publikation des Bildnisses von Kindern durch ihre Eltern Fankhauser/Fischer, in: Fankhauser/Reusser/Schwander, 193 ff.; Vogt/Wiget, in: Arter/Jörg (Hrsg.), 129 ff., insb. 142 ff.; zum Bildnis resp. Portrait vgl. auch den geschichtswissenschaftlichen Beitrag von Mayer, 11 ff.; interessant mit Blick auf den rechtlichen Bildnisschutz der Beitrag der Historikerin Dommann, in: Joly/Visman/Weitin (Hrsg.), 249 ff.; zum Recht am eigenen Bild im System des deutschen allgemeinen Persönlichkeitsrechts vgl. Helle, 45 ff., 47 mit dem Hinweis, dass das Schutzobjekt dieses besonderen Persönlichkeitsrechts ein Selbstbestimmungsrecht des Abgebildeten darstellt; zum Recht am eigenen Bild und weiteren Per-

Die Erstellung, Verbreitung und Speicherung des Abbildes eines Menschen ist unbestritten eine Bearbeitung von Personenangaben gemäss DSG, wobei sich das Bundesgericht in den letzten Jahren wiederholt mit dem rechtlichen Schutz des Bildnisses auch im Kontext der neuen Informationsverarbeitungstechnologien zu befassen hatte, beispielsweise in seinem Entscheid zu «Google Street View»;[1282] zudem war es mit dem Thema der Video-Observation in verschiedenen Kontexten beschäftigt. Es geht an dieser Stelle darum, die Grundstruktur des Rechts am eigenen Bild in seinem Kontrast zur allgemeinen Ordnung des DSG darzulegen. Basierend auf der bundesgerichtlichen Rechtsprechung gilt für das Recht am eigenen Bild eine spezifische Ordnung. Sie ist historisch mitbedingt: Das Abbild des Menschen in Gestalt des Portraits, die Fotografie und eventuelle Reproduktionen sowie die resultierenden rechtlichen Herausforderungen im Umgang mit Bild- und Videomaterial sind älter als (digitale) Personendatenverarbeitungen, wie man sie mit dem DSG adressieren wollte. 985

Das Abbild(en), das Bildnis des «Menschen», das gewissermassen die Person eins zu eins repräsentiert, kann als Ursituation der Personendatenverarbeitung bezeichnet werden. Weil die Person gewissermassen «kopiert» wird, findet das Bildnis wie keine andere «Personenangabe» eine Assoziation mit dem Menschen, der Person als «Ganzes». Kontrastreich insofern die informationelle Fragmentierung des Menschen, wie sie durch die digitalen Technologien erfolgt. Der rechtliche Bildnisschutz wird bis heute auf Art. 28 ZGB abgestützt. Insofern hat sich eine besondere Schutzwürdigkeit herausgebildet, die mit dem «Näheverhältnis» des Abbildes zu seiner Person zu erklären ist. 986

Im historischen Entscheid «Hodler auf dem Totenbett», BGE 70 II 127, wehrte sich die Witwe von Hodler gegen die Ausstellung eines Gemäldes von Schürch, einem Schüler – dem Lieblingsschüler – von Hodler. Das Bild stellt Hodler auf dem Totenbett dar. Die Witwe ging gegen den Galeristen Kaspar vor und verlangte, dass das Bild mangels Zustimmung der Familie nicht gezeigt werde. Die Witwe berief sich in ihrer Klage – mangels anerkannten postmortalen Persönlichkeitsschutzes – auf die Verletzung ihrer eigenen Pietätsgefühle sowie ihrer psychischen und emotionalen Integrität. Zudem störte sie sich daran, dass man mit dem intimen Abbild auch noch Geld verdienen wollte. Das Bundesgericht hatte in der Folge die eigentumsrechtliche Position des Galeristen am Bild sowie die Interessen der Öffentlichkeit an Kunst und Kulturgütern gegenüber den Interessen der Witwe abzuwägen. Es beurteilte diejenigen der Witwe als überwie- 987

sönlichkeitsmerkmalen, insb. mit Blick auf ihre kommerzielle Nutzung und das Right to Publicity, Bergmann, Loyola of Los Angeles ELR 1999, 479 ff., 484 ff.; zum Recht am eigenen Bild auch Ladeur, ZUM 2000, 879 ff.; Seemann, 136 ff., handelt das Recht am eigenen Bild, gemeinsam mit dem Recht am eigenen Namen, unter dem Titel der Publizitätsrechte im deutschen Recht ab; Lüthy, 74 ff.; Lévy, 27 ff., auch zur Verwertungskomponente, 291 ff.

1282 Vgl. BGE 138 II 346, insb. E 6.

gend. Es entbehrt nicht einer gewissen Ironie des Schicksals, dass just die Ehefrau des Künstlers sich mit Erfolg gegen etwas zur Wehr setzte, was ebendieser zu Lebzeiten getan hatte und ihn auch berühmt gemacht hatte: Hodler war es, der minutiös und erschütternd den Zerfall seiner Geliebten Valentine Godé-Darrel dargestellt hatte. Dieser intime, verstörende Zyklus, der mit der Darstellung von Valentine auf dem Totenbett endet, gilt als (s)ein Meisterwerk.[1283]

988 Jahrzehnte später hielt BGE 127 III 481 fest, dass niemand ohne seine Zustimmung abgebildet werden dürfe, sei es durch Zeichnung, Gemälde, Fotografie, Film oder ähnliche Verfahren. Das dergestalt anerkannte Recht am eigenen Bild galt als Konkretisierung des Persönlichkeitsrechts, Art. 28 Abs. 1 ZGB.[1284]

989 Mit dem Recht am eigenen Bild befasste sich das Bundesgericht weiter im Google-Street-View-Entscheid, BGE 138 II 364: Der EDÖB hatte gegen Google geklagt und verlangt, dass Bilder des Dienstes Google Street View nur veröffentlicht werden dürfen, wenn Gesichter und Autokennzeichen vollständig unkenntlich gemacht worden seien. Inhaltlich gelte das Recht am eigenen Bild, so das Bundesgericht in E 8.2. unter Zitierung von Bächli, als *Selbstbestimmungsrecht*. Ebendieses schütze vor der widerrechtlichen Verkörperung des eigenen Erscheinungsbildes. Einen ersten Teilgehalt bilde der Abwehranspruch gegen gezieltes, auf Identifikation und Ausforschung gerichtetes Erstellen von Fotos etc. Der zweite Teilgehalt bestünde in einem Recht auf Selbstbestimmung des Menschen hinsichtlich der Veröffentlichung des eigenen Bildes, insb. des Porträts, und seiner Verwendung in kommerzieller oder politischer Werbung.

990 Obschon es sich beim Abbild einer Person um eine Personenangabe handelt, *übersteuert das Recht am eigenen Bild die Regelung gemäss DSG*. Über die etablierte bundesgerichtliche Rechtsprechung zum Recht am eigenen Bild wird für das Bildnis der Person der entgegengesetzte Ausgangspunkt zum Regime des DSG im privaten Bereich anerkannt. Das Recht am eigenen Bild geht von einem Grundsatz des Verarbeitungsverbotes mit Erlaubnisvorbehalt aus. Jede Verarbeitungshandlung (und nicht erst qualifizierte Verarbeitungshandlungen) mit Blick auf das Bildnis – das Erstellen, Speichern, Weiterleiten oder Veröffentlichen – ist prinzipiell verboten, es sei denn, es läge ein Legitimationsgrund, namentlich die Einwilligung, vor.

991 Ungeachtet dessen, dass das Bildnis eines Menschen, sein Abbild, ein personenbezogenes Datum im Sinne des DSG ist – das hat BGE 127 III 481 festgehalten –,

1283 Ein Maler vor Liebe und Tod. Ferdinand Hodler und Valentine Godé-Darel. Ein Werkzyklus. Kunsthaus Zürich; Kunstverein St. Gallen; Villa Stuck, München; Kunstmuseum Bern, 1976/1977.

1284 Vgl. zur Einwilligung im Rahmen des Rechts am eigenen Bild BGE 136 III 401, E 5 und E 6; zum Right to Publicity und der Bedeutung der Einwilligung auch für die kommerzielle Nutzung des Abbildes Bergmann, Loyola of Los Angeles ELR 1999, 479 ff., 488; vgl. auch Seemann, 66 ff.; Lévy, 112.

gilt eine gerichtlich etablierte und vom gesetzlichen Regime abweichende *Sonderordnung resp. Spezialregelung*. Das grundsätzliche Verarbeitungsverbot mit Erlaubnisvorbehalt im Rahmen des Rechts am eigenen Bild nach schweizerischer Judikatur, das Gesetz derogierendes Recht ist somit strukturell näher an der Konzeptionierung gemäss Art. 6 DSGVO.

992 Gleichzeitig erhärtet diese (gerichtlich etablierte) Spezialregelung zum Bildnis, dass die Schweiz in ihrem allgemeinen Datenschutzrecht, wie es das DSG als Querschnittsgesetz liefert, für den privaten Bereich mit der grundsätzlichen Verarbeitungsfreiheit mit Schranken *kein* Regime der Selbstbestimmung vorsieht. Das Recht am eigenen Bild mit seiner Konkretisierung durch das Bundesgericht repräsentiert ein gegenüber der allgemeinen Ordnung des DSG für den privaten Bereich spezifisches Regelungssystem. Dass mit dem Recht am eigenen Bild ein grundsätzliches Verarbeitungsverbot mit Erlaubnistatbestand und aufgewerteter Relevanz der Einwilligung anerkannt wird, ist kognitiv nachvollziehbar: Das Bildnis ist keine fragmentierte Informationseinheit, stattdessen fängt es eine Person gesamthaft ein und schafft ein «Antlitz der analogen Welt». Das Abbild der Person, das diese wie eine Kopie repräsentiert, ist ihr so «nah», dass nicht erst qualifizierte Bearbeitungen, sondern jede Verarbeitungshandlung verboten ist, es sei denn, es läge ein Erlaubnistatbestand vor. Das Recht am eigenen Bild mit seiner bundesgerichtlichen Konkretisierung kann mit Fug und Recht als Selbstbestimmungsrecht bezeichnet werden.

993 Anzufügen bleibt, dass mit der Teilrevision des Urheberrechtsgesetzes, die am 27. September 2019 verabschiedet wurde, der Bildnisschutz neu geregelt wird. Die Revision will das Urheberrecht an das Zeitalter der Digitalisierung heranführen.[1285] Insofern ist auf einen neu weit gefassten Bildnisschutz hinzuweisen, demgemäss Fotografien, sofern selbst angefertigt, urheberrechtlich geschützt werden.[1286] Die Regelung hat Bedeutung für den Umgang mit sog. Selfies.

6.3. *Gesetzliche Spezialnormen – Einwilligung im Biomedizinrecht*

994 Bezüglich der *Diversifizierung von Autonomiepositionen in Bezug auf Personendaten und damit datenschutzrechtliche Autonomiepositionen* sind – *zweitens* – vom DSG abweichende, spezifische gesetzliche Einwilligungskonstruktionen einschlägig. Sie finden sich im Zivil- und Privatrecht, insb. im ZGB resp. OR sowie in Spezialgesetzgebungen. Solche Erlasse und Normen legiferieren *kontext-*

1285 Vgl. für eine Übersicht IGE, Die eidgenössischen Räte heissen die Teilrevision URG gut, Bern 2019, <https://www.ige.ch/de/recht-und-politik/immaterialgueterrecht-national/urheberrecht/revision-des-urheberrechts/parlamentarische-beratung.html#c66462> (zuletzt besucht am 30. April 2021); Parlament, Urheberrechtsgesetz, Änderung, Bern 2019, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170069 (zuletzt besucht am 30. April 2021).

1286 Kritisch zu einem «irrlichtenden Bildnisschutz» Schmidt-Gabain, NZZ vom 26. Januar 2018.

oder bereichsspezifisch in Ergänzung zum resp. Abweichung vom DSG, auch in Bezug auf die Bedeutung der Einwilligung des Datensubjektes. Der Umgang mit Personendaten wird in mehreren Erlassen ausserhalb des DSG adressiert. Exemplarisch zu nennen sind die familieninformationsrechtlichen Bestimmungen gemäss ZGB, insb. im Adoptionsrecht.

995 Im (weiten) Feld des (Bio-)Medizinrechts finden sich in verschiedenen Spezialgesetzen zahlreiche informations- und datenschutzrechtliche Vorgaben.[1287] Verfassungsrechtlich relevant ist in diesem Zusammenhang insb. Art. 119 Abs. 2 lit. f BV, der hinsichtlich Untersuchung, Registrierung oder Offenbarung des Erbgutes einer Person deren vorgängige Zustimmung fordert. Eine elaborierte und eigenständige Ordnung zur Verarbeitung von Personendaten («Gesundheitsdaten») verankern das Humanforschungsgesetz (HFG)[1288] und das Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG).[1289]

996 Das Humanforschungsgesetz befasst sich mit der Forschung am Menschen, vgl. Art. 2 lit. a–c HFG. In diesem Kontext regelt es ebenso den Umgang mit gesundheitsbezogenen Angaben, vgl. Art. 1 lit. e HFG. Das HFG liefert folglich insofern eine *lex specialis* bezüglich DSG. Die Ordnung des HFG ist nuanciert. Das Gesetz differenziert danach, ob es um die Forschung mit gesundheitsbezogenen Personendaten geht oder ob gesundheitsbezogene Personendaten für Forschungsprojekte *weiterverwendet* werden.[1290] An diese Kategorisierung schliesst ein differenziertes Einwilligungssystem an. Der Gesetzgeber definiert strengere Anforderungen für die zuerst genannte Konstellation, weil er diese als risikoträchtiger beurteilt. Werden dagegen bereits erhobene gesundheitsbezogene Personendaten zu *Forschungszwecken* weiterverwendet, sei das Gefahrenpotential geringer. Ebendies erlaube eine pragmatischere Lösung.[1291] Die Forschung mit gesundheitsbezogenen Personendaten gilt als Forschung am Menschen und wird im 2. Kapitel des HFG geregelt: Ebendiese Forschung bedinge die Erhebung der entsprechenden personenbezogenen Gesundheitsdaten, was einen stärkeren Eingriff in die Rechte der betroffenen Person darstelle. Entsprechend ist nach Art. 16 Abs. 1 HFG die Forschung mit gesundheitsbezogenen Personendaten (die nicht weiterverwendet, stattdessen erhoben werden) grundsätzlich nur zulässig, wenn die Person nach

1287 Vgl. zum Bioinformationsrecht Gruber, *passim*.
1288 SR 810.30; hierzu jüngst grundlegend Karavas, Körperverfassungsrecht, 211 ff.; vgl. auch Art. 119 Abs. 2 lit. f BV.
1289 SR 810.12; zur fehlenden Legaldefinition von Gesundheitsdaten und zu den einschlägigen Normen vgl. auch do Canto, sic! 2020, 177 ff., 179 f.; vgl. sodann die Beschreibung der Datenströme mit Blick auf Gesundheitsdaten im Zusammenhang mit der Gesundheitsversorgung durch Spitäler Gogniat, Jusletter vom 20. Juni 2016, N 16.
1290 Zum Ganzen vertiefend und kritisch Karavas, Körperverfassungsrecht, 154 ff.; vgl. zur Relevanz der Unterscheidung der verschiedenen Kontexte auch Simitis, in: Brem/Druey/Kramer/Schwander (Hrsg.), 469 ff., 491 f.
1291 Botschaft vom 21. Oktober 2009 zum Bundesgesetz über die Forschung am Menschen, BBI 2009 8082; kritisch hierzu Karavas, Körperverfassungsrecht, 219 ff.

hinreichender Aufklärung in das *konkrete Forschungsprojekt* eingewilligt hat. Die Anforderungen an die Informiertheit der Einwilligung resp. die reziproken Aufklärungspflichten werden in Art. 16 Abs. 2 lit. a–e HFG detailliert konkretisiert. Die Einwilligung hat prinzipiell schriftlich zu erfolgen; die Gültigkeit verlangt nach Art. 16 Abs. 3 HFG zudem die Einhaltung einer Bedenkfrist zwischen Aufklärung und Einwilligung.[1292] Anders wird die *Weiterverwendung* von gesundheitsbezogenen Personendaten im 4. Kapitel des HFG geregelt. Auch hier lässt sich ein differenziertes Regime feststellen. Nach Art. 17 HFG bedarf es der Einwilligung der betroffenen Person resp. des Hinweises auf ein Widerspruchsrecht im Zeitpunkt der Erhebung, sofern in diesem Moment feststeht, dass die Information später dem Forschungszweck zugeführt wird. Ein «Versäumnis» kann geheilt werden, sofern gemäss Art. 17 HFG die Einwilligung spätestens vor der Weiterverwendung gemäss Art. 32 bzw. Art. 33 HFG eingeholt wird.[1293]

997 Ebenda, in den Art. 32 f. HFG, finden sich nuancierte Modalitäten der Einwilligung, je nach Art der Daten und des Datenumgangs: Differenzierungskriterien sind die Kategorisierungen von genetischen Daten versus gesundheitsbezogenen Daten sowie die Bearbeitung in unverschlüsselter, verschlüsselter oder anonymisierter Form. Art. 32 HFG befasst sich mit den *genetischen Daten* (sowie dem biologischen Material): Eine Weiterverwendung der genetischen Daten in *unverschlüsselter Form* bedarf nach Art. 32 Abs. 1 HFG eine Einwilligung nach hinreichender Aufklärung der betroffenen Person resp. der gesetzlichen Vertretung oder der nächsten Angehörigen über das geplante und konkrete Forschungsprojekt. Nach Art. 32 Abs. 2 HFG genügt eine Generaleinwilligung, sofern die Weiterverwendung genetischer Angaben in *verschlüsselter Form* vorgesehen ist. Werden genetische Daten in *anonymisierter* Form weiterverwendet, genügt der Hinweis auf ein Widerspruchsrecht, vgl. Art. 32 Abs. 3 HFG; eine formularmässige Informierung, beispielsweise mittels einer Patienteninformationsbroschüre des Spitals, soll zulässig sein.[1294] Die Weiterverwendung von *nicht-genetischen Gesundheitsdaten* wird nach Art. 33 HFG unter ein minder strenges Zustimmungsregime gestellt: Eine Generaleinwilligung ist bei der Weiterverwendung solcher Daten in *unverschlüsselter Form einzuholen*, Art. 33 Abs. 1 HFG, wohingegen die Informierung über das Widerspruchsrecht bei der Weiterverwendung in *verschlüsselter Form statuiert wird*, Art. 33 Abs. 2 HFG; eine Weiterverwendung in anonymisierter Form wird voraussetzungslos zugelassen.

1292 Weitere erhöhte Voraussetzungen an die Aufklärung und Einwilligung werden spezifisch für sog. «besonders verletzbare Personen», beispielsweise Kinder, schwangere Frauen oder Personen im Freiheitsentzug, formuliert, vgl. Art. 7 Abs. 1 i. V. m. Art. 16 Abs. 1, Art. 26 und Art. 28 Abs. 1 HFG.

1293 M. w. H. Karavas, Körperverfassungsrecht, 153 f.

1294 Botschaft Humanforschungsgesetz 2009, 8045 ff., 8122; zum Ganzen Karavas, Körperverfassungsrecht, 155.

998 Das HFG sieht entsprechend ein abgestuftes und differenziertes Regelungskonzept vor im Kontext der Forschung und der Weitergabe von gesundheitsbezogenen resp. genetischen Angaben zu Forschungszwecken.[1295] Es geht an dieser Stelle nicht darum, eine Bewertung dieses Systems abzugeben. Vielmehr taugt dieser Blick auf die datenschutzrechtlichen Bestimmungen im HFG dazu, *dreierlei* (weiter) freizulegen und zu verdeutlichen:

999 *Erstens* lässt sich anhand der Einwilligungsvorgaben im Bereich der Forschung mit gesundheitsbezogenen genetischen und nicht-genetischen Daten des HFG bestätigen, dass das allgemeine System des DSG für den privaten Bereich gerade *keines der informationellen Selbstbestimmung* ist. Während das HFG die Einwilligung grundsätzlich als Voraussetzung zulässiger Verarbeitung verlangt – oft mit qualifizierten formellen wie informationellen Anforderungen –, genügt der Widerspruch nur ausnahmsweise. Damit liegt diesem auch datenschutzrechtlich einschlägigen, bereichsspezifischen Spezialgesetz ein prinzipielles Verarbeitungsverbot als Basisannahme zugrunde. Anders funktioniert dagegen, wie gezeigt, das System im DSG für den privaten Bereich.

1000 *Zweitens* wird mit dieser gegenüber der allgemeinen Ordnung des DSG hoch ausdifferenzierten Normierung des Umgangs mit Personendaten im Forschungskontext nach HFG dokumentiert, dass das Schweizer Datenschutzrecht – trotz der Querschnittsgesetzgebung mit dem DSG – einen *sektor- und bereichsspezifischen Ansatz* kennt.[1296] Dass das Datenschutzrecht der Schweiz – trotz der persönlichkeitsrechtlichen Anknüpfung des DSG – *systemspezifische Erwägungen* als datenschutzrechtlich einschlägiges Gestaltungselement anerkennt, wurde an diversen weiteren Stellen herausgeschält, z. B. im Rahmen der Darstellung des Dualismus im DSG, des Rechtmässigkeitsprinzips sowie des Zweckbindungsgrundsatzes, der Rechtfertigungsgründe qua Gesetz oder überwiegenden Interessen.

1001 Dass die Differenzierung je nach einbettenden *Verarbeitungszusammenhängen* datenschutzrechtlich als einschlägig anerkannt wird, erhärtet sich mittels der Gegenüberstellung des DSG mit dem HFG sowie der Regelung innerhalb des HFG selbst. Spezifisch für den *Forschungskontext* wird ein gegenüber dem DSG eigenständiges Regelungsregime im Umgang mit gesundheitsbezogenen und genetischen Personendaten verankert. Innerhalb des HFG wird zudem erneut differenziert: Werden gesundheitsbezogene Daten *zwecks* Forschung erhoben, gilt

1295 Botschaft Humanforschungsgesetz 2009, 8045 ff., 8083.

1296 Eindrücklich sichtbar wurden diese Korrelationen jüngst in BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2019, wobei sich die Erwägungen nicht nur mit den allgemeinen Verarbeitungsgrundsätzen, sondern auch den Einwilligungsvorgaben befassen. Ein Kernelement der Entscheidung ist indes in den bereichsspezifischen Erwägungen des Gerichts zu verorten, wobei nicht nur die Analyse, ob das öffentliche oder private DSG anwendbar ist, sondern auch die Relevanz der versicherungsrechtlichen Spezialgesetzgebung in ihrer Korrelation zum Datenschutzrecht deutlich wird.

dies als Forschung am Menschen. Hieran knüpfen spezifisch Verarbeitungsvorgaben an.[1297] Handelt es sich hingegen um die Weiterverwendung von gesundheitsbezogenen Daten, greift ein anderes Regime. Exemplarisch soll insofern die folgende Konstellation vorgestellt werden: Im Rahmen einer ärztlichen Untersuchung, beispielsweise einer Brustkrebs-Vorsorgeuntersuchung bei einer Frau mit familiärer Prädisposition, werden auch Personendaten erhoben. Diese Personenangaben werden entsprechend ursprünglich im Gesundheitsbereich und medizinischen Sektor erhoben; mit ihnen wird ursprünglich ein gesundheitsbezogenes Ziel verfolgt. Sollen nun die im Rahmen einer Untersuchung erlangten Gesundheitsdaten oder genetischen Angaben zur Forschung weiterverwendet werden, werden sie in einen anderen Kontext transferiert.[1298] Über das Beispiel, das auch das Regelungsregime veranschaulicht, wird in der gesetzgeberischen Konzeptionierung abermals die *dynamische Dimension des Datenschutzrechts* deutlich: Es geht um die Regelung des *Transfers* von Personendaten aus einem Kontext, dem Gesundheitskontext, in einen anderen Kontext, den Forschungskontext. In der ersten Konstellation dagegen zirkulieren die Personendaten innerhalb eines einzigen Kontextes. Im HFG wird folglich datenschutzrechtlich ein Ansatz gewählt, der sich der *rechtlichen Gestaltung von Datenflüssen innerhalb eines Kontextes, aber auch zwischen zwei Kontexten («weiterverwenden») widmet*. Dieser jüngere Rechtserlass, welcher der Bewältigung technologischer resp. bio- und informationstechnologischer Herausforderungen dient, lassen sich Anhaltspunkte für die Weiterentwicklung des Datenschutzrechts finden. Die Betrachtung des HFG zeigt, inwiefern die Verwurzelung in einer Subjekt-Objekt-Basierung, wie sie genuin im DSG verwurzelt ist, gelockert wird. Das DSG mit seiner persönlichkeitsrechtlichen Anknüpfung und den quasi objekthaften Kategorien von abstrakt charakterisierten «gewöhnlichen» resp. «besonders schutzwürdigen» Personendaten wird ergänzt. Das HFG präsentiert trotz seiner rechtlichen Anknüpfung an das Individuum und dessen Selbstbestimmung die Einschlägigkeit von Kontexten sowie die Bedingungen von Personendatentransfers, mithin von Datenflüssen im Umgang mit Personendaten und damit im Datenschutzrecht. Allerdings: Die im HFG gewählte Bewertung dürfte kritisch diskutiert werden. Es geht um die Schlussfolgerung, wonach die Bearbeitung von Personendaten *innerhalb* des Forschungskontextes die problematischere Konstellation sei als diejenige, in der Personendaten beispielsweise im Gesundheitskontext erhoben und dann in den Forschungskontext übergeleitet werden.[1299] Der Transfer von Personendaten von einem Kontext in einen anderen Kontext ist *prima vista* die eigentliche datenschutzrechtliche Herausforderung.

1297 Vertiefend hierzu Karavas, Körperverfassungsrecht, 152 ff., 210 ff.
1298 Hierzu Ders., a. a. O., 153 ff.
1299 Ders., a. a. O., 195 ff.

1002 Damit sind weitere Belege gefunden, welche die in dieser Schrift vertretene These bestätigen: Eine Kernaufgabe des Datenschutzrechts stellt die Gestaltung des *Deltas* der Datenflüsse oder der *Knotenpunkte* dar.[1300] Kritisch zeigt sich die Situation, in welcher ein Datenstrom *aus einem Kontext in einen anderen Kontext* übergeleitet wird. Diese Betrachtungsweise konterkariert diejenige, die das Datensubjekt und Personendaten als Quasi-Objekte fokussiert. Im Laufe dieser Studie wird noch robuster erhärtet werden, dass der datenschutzrechtliche Regelungsauftrag auch darin zu verorten ist, sich der *Gestaltung der Grenzverläufe und der Flussläufe zwischen verschiedenen Bereichen* anzunehmen. Mehrere im Laufe dieser Arbeit analysierte Normen und Regelungskonstruktionen innerhalb des DSG, aber auch eine einbettende Betrachtung seines Regimes in der Gesamtlandschaft von datenschutzrechtlichen Normen und Erlassen haben entsprechende bereits im geltenden Recht angelegte Elemente freigelegt. Die Fixierung auf die «persönlichkeitsrechtliche, subjektivrechtliche Anknüpfung», wie sie im DSG als sog. Querschnittsgesetz implementiert wird, lässt eine solche datenschutzrechtliche Regelungsaufgabe aus dem Blick fallen.[1301]

1003 Die Relevanz lässt sich anhand eines zweiten Erlasses veranschaulichen, seinerseits angesiedelt im *Bereich von Recht und neuen Technologien.*[1302] Das GUMG, das einer Revision unterzogen wurde, deren Ergebnisse Ende 2020 vorlagen, unterstellt den Umgang mit genetischen Informationen einer spezifischen Normierung. Auch in und über das GUMG wird eine konzeptionelle und systemische Herangehensweise angelegt. Genetische Untersuchungen haben faktisch stark an Bedeutung gewonnen. Heute werden sie nicht nur im Rahmen von Abstammungsabklärungen, sondern auch für pränatale Tests sowie zur Bestimmung von Krankheitsveranlagungen (z. B. die Mutation im BRCA1/2-Gen) eingesetzt. Auf den Erkenntnissen basierend erfolgt eine individualisierte medizinische Behandlung.[1303] Genetische Testungen, die Erkrankungsrisiken einer Person dokumentieren, sind nicht nur für das Individuum und den medizinischen Bereich, den Gesundheitssektor, aufschlussreich. Das GUMG adressiert die facettenreichen Inter-

1300 Ladeur, Vortrag, Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021).

1301 Insofern lässt sich eine Parallele zu den familienrechtlichen Entwicklungen und Herausforderungen nachzeichnen: Solange das Familienrecht sich dem Schutz der ehelichen Einheitsfamilie verschreibt, stellt sich die Frage, was die Regelungsaufgabe des Familienrechts ist, nicht resp. scheint sie beantwortet zu sein. Allerdings wurde diese Frage jüngst aufgeworfen, wobei verschiedene Ansätze und Konzepte insofern präsentiert werden: Hierzu richtungsweisend insb. die zahlreichen Beiträge von Schwenzer.

1302 Zum sich wandelnden Recht in Einbettung zu sozialen und technologischen Entwicklungen vgl. die Beiträge in Becker/Hilty/Stöckli/Würtenberger (Hrsg.), Festschrift für Manfred Rehbinder, München 2002.

1303 Vgl. zur Bedeutung von genetischen Informationen im Zusammenhang mit psychiatrischen Erkrankungen mit den hieraus resultierenden datenschutzrechtlichen Bedenken Nagenborg/El-Faddagh, IRIE 2006, 40 ff.; zu Daten als Medizin resp. im Gesundheitsbereich Baeriswyl, digma 2014, 52 ff.

essen, indem es die genetischen Untersuchungen gemäss Art. 1 Abs. 1 GUMG für den medizinischen Bereich (lit. a), den arbeitsrechtlichen Bereich (lit. b), den Versicherungsbereich (lit. c) und den Haftpflichtbereich (lit. d) unterscheidet. Es sieht ein differenziertes Einwilligungsregime vor.[1304]

Die genetische Untersuchung im *Versicherungsbereich* beispielsweise wird im fünften Abschnitt des GUMG geregelt: Art. 26 GUMG verbietet Versicherungsgebern, für den Abschluss eines Vertrages die Vornahme genetischer Untersuchungen zu verlangen. Für spezifische Versicherungsleistungen greift nach Art. 27 GUMG ein Nachforschungsverbot. Mit anderen Worten: Für die Grundversicherung dürfen Ergebnisse vorhandener genetischer Untersuchungen nicht verlangt werden. Im Übrigen dürfen die mit der Durchführung eines Gentests beauftragten Ärztinnen und Ärzte gemäss Art. 28 Abs. 1 lit. a und lit. b GUMG unter zwei Voraussetzungen vorhandene Ergebnisse der Versicherung mitteilen. Insofern ist zunächst für den Privatversicherungsbereich das VVG einschlägig, wobei Art. 6 VVG eine Anzeigepflicht des Versicherungsnehmers vorsieht. Liegen Ergebnisse vorhandener genetischer Untersuchungen vor, die für die versicherte Person ein erhöhtes Krankheitsrisiko und damit für die Versicherung ein akzentuiertes wirtschaftliches Risiko indizieren, und kommt der Versicherungsnehmer seiner Anzeigepflicht nach, ist die Versicherung grundsätzlich berechtigt, sich von ihren Vertragsverpflichtungen zu befreien. Während im Bereich der sozialen Grundversicherung allgemeine *Einwilligungsverbote* zur Transmission entsprechender Ergebnisse anerkannt sind, gilt dies nicht für den Bereich der privaten Versicherung.[1305] Insofern wird – getreu der persönlichkeitsrechtlichen Verwurzelung – jüngst die «Freiwilligkeit» einer Einwilligung des Datensubjektes hinterfragt. Die dahinterliegende Grundsatzfrage, ob eine entsprechende Wertung in Anbetracht der *systemischen Dimension* des Datenschutzes mit seiner Aufgabe, die Integrität jeweils verschiedener gesellschaftlicher Bereiche zu gewährleisten, angemessen ist, wird dagegen nicht gestellt. Auch anhand des GUMG wurde sichtbar, dass dieses – selbst wenn es ebenso nicht unwesentlich an den Willen des Datensubjektes anknüpft – datenschutzrechtlich die Einschlägigkeit kontextbezogener Kriterien anerkennt. Hieran anknüpfend schafft es ein informationsrechtlich nuanciertes Normgefüge. 1004

Lassen sich über diesen Befund hinaus, namentlich aus der Erkenntnis, wonach der Wille des Subjektes unter Anerkennung bereichsspezifischer Differenzierungen in facettenreicher, nuancierter und abgestufter Weise in das Datenschutzrecht der Schweiz – das weit mehr ist als das DSG – integriert wird, allgemeinere Schlussfolgerungen hinsichtlich der Funktion der datenschutzrechtlichen Einwilligung gewinnen? Karavas arbeitet in seiner Habilitationsschrift für den 1005

1304 Fasnacht, N 573.
1305 Vgl. hierzu Ders., N 551 ff. und zum GUMG N 570 ff.

biomedizinrechtlichen Bereich heraus, dass sich die *Funktion der informierten Einwilligung* keineswegs auf die Gewährleistung eines verfassungsrechtlich verbürgten Selbstbestimmungsrechts, das der Sicherung der freien Willensbildung und freien Willensbetätigung diene, beschränke.[1306] Indem das Rechtsinstitut auf der anderen Seite Pflichten, beispielsweise der Forscherinnen und Forscher, definiere, strukturiere es ebenso Beziehungen der involvierten Personen. Damit wird dem Rechtsinstitut der informierten Einwilligung im Bereich des Biomedizinrechts konstitutionelle Wirkung zugemessen.[1307] Zudem gilt die informierte Einwilligung als *Governance*-Instrument sowie als weit verbreitetes und etabliertes *organizational recipe* im Bereich der biomedizinischen Forschung.[1308] Folglich qualifiziert Karavas die informierte Einwilligung im weiten Feld des Biomedizinrechts aus einer funktionellen sowie kontextuellen Perspektive heraus als *Kompatibilisierungsinstrument*: Der Einwilligung wird in diesem Sinne die Funktion zugemessen, verschiedene Bereiche – z. B. den Gesundheitssektor und den Forschungsbereich – mit ihren unterschiedlichen Handlungslogiken und Erwartungen sowie ihre Schnittstellen zu harmonisieren. Allerdings hinterfragt der Autor sogleich die Tauglichkeit der informierten Einwilligung zur Lösung von Kollisionen zwischen Gesellschaftsbereichen resp. Kontexten. Seiner Ansicht nach lassen sich Spannungsfelder und Kollisionen gerade wegen ihrer kollektiven Dimension durch die informierte Einwilligung des Einzelnen nicht sinnvoll adressieren.[1309]

1006 Dass die Figur der Selbstbestimmung nicht das einzig relevante Erwägungselement ist, findet sich für das Datenschutzrecht in der Argumentation des Bundesverfassungsgerichts in seinem Volkszählungsurteil. Das Bundesverfassungsgericht richtete den Fokus auch auf die *kontextuelle Dimension* und namentlich auf die *notwendige Trennung resp. Abgrenzung der Statistik vom Vollzug mit dessen facettenreichen Teilbereichen*. Um einen Transfer oder Informationsfluss von Personendaten, die zum Zweck der Volkszählung erhoben wurden, in andere Bereiche des Verwaltungsvollzuges zu verhindern, beschränkte sich das Bundesverfassungsgericht nicht darauf, die Bedeutung des Grundrechts auf informationelle Selbstbestimmung, das prinzipielle Verarbeitungsverbot mit Schranken, die Relevanz des Zweckbindungsgrundsatzes und das Statistikgeheimnis zu thematisieren. Vielmehr wurden *flankierende personelle und organisatorische Massnahmen* verlangt. Beispielhaft zu nennen ist die Forderung, wonach die Zähler nicht in ihrem unmittelbaren räumlichen Einsatzgebiet tätig werden sollen. Es sei zu verhindern, dass sie aufgrund ihres ursprünglichen fachlichen Wirkungsfeldes nur ungenügende Neutralität aufweisen.[1310] Das Bundesverfassungsgericht

1306 Karavas, Körperverfassungsrecht, 195 ff., insb. 222 ff.
1307 Ders., a. a. O., 197.
1308 Hierzu m. w. H. Ders., 197 f.
1309 Ders., 228 f.
1310 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 220.

formuliert einen hoch *ausdifferenzierten und facettenreichen Katalog an materiellen, namentlich aber auch organisatorischen sowie formellen Vorgaben*, um damit die Trennung von Statistik und Verwaltungsvollzug zu gewährleisten. Ein Kernargument liegt darin, dass nur das *Vertrauen in diese Trennung* und damit die Gewährleistung, wonach Personendaten, die im Kontext der Statistik erhoben wurden, nicht anderen Bereichen und Behörden (z. B. Steuerbehörden oder Migrationsbehörden) zwecks konkreten Verwaltungsvollzugs zugeführt werden, sicherstelle, dass die Bürgerinnen und Bürger die Erhebungsfragen korrekt und vollständig beantworten würden. Auf ebendiese korrekten und vollständigen Angaben sei eine repräsentative statische Erhebung, welche die damit verfolgten staatlichen Ziele effizient erreichen soll, angewiesen. Zwangsmassnahmen dagegen könnten die Kooperation der Bürgerinnen und Bürger insofern gerade nicht gewährleisten. Die vom Bundesverfassungsgericht formulierten Datenschutzvorgaben zielen damit in grundlegender Weise auf den Schutz der Funktionstüchtigkeit und Integrität der Volkszählung ab.

6.4. Resümee – Nuancierte Autonomiegrade

Gezeigt wurde, dass das Schweizer Recht in Bezug auf den Umgang mit Personendaten in verschiedenen datenschutzrechtlich einschlägigen Erlassen variable Modalitäten für den Einsatz von Einwilligungs- resp. Widerspruchslösungen vorsieht.[1311] Eine Gesamtbetrachtung führt zu dem Schluss, dass im Umgang mit Personendaten keine einheitliche «Selbstbestimmung» verbürgt wird. Insofern wurde zum einen das durch eine stabile bundesgerichtliche Rechtsprechung etablierte Regime zum Recht am eigenen Bild dargestellt. Zum anderen fand eine Betrachtung von HFG und GUMG statt, wobei sich in diesen Erlassen nuancierte Einwilligungskonstruktionen zeigten. Diese einbettende und vergleichende Betrachtung diverser und diversifizierter Konstruktionen zur Inklusion des Willens des Datensubjektes hat bestätigt, dass das *DSG selbst kein Recht auf informationelle Selbstbestimmung* implementiert, mit einem Gehalt, wie es mit dem Volkszählungsurteil des Bundesverfassungsgerichts gemeint und assoziiert wird. 1007

Als ein Recht auf informationelle Selbstbestimmung – das eine solche Titulierung zu Recht tragen würde – lässt sich demgegenüber das *Recht am eigenen Bild* charakterisieren. Bei den Verarbeitungshandlungen im Zusammenhang mit dem Abbild einer Person handelt es sich unbestritten um Personendaten. Das Recht am eigenen Bild etabliert ein eigentliches Sonderrecht im Vergleich zum DSG. Der im Wesentlichen über Art. 28 ZGB anerkannte Inhalt des Rechts am eigenen Bild 1008

1311 Die Nuancierung von Einwilligungskonstruktionen lässt sich gesetzlich wie anhand der bundesgerichtlichen Rechtsprechung nachzeichnen; exemplarisch ist BGE 136 II 401.

lässt sich deshalb als Selbstbestimmungsrecht bezeichnen, weil Verarbeitungshandlungen im Umgang mit dem Abbild einer Person prinzipiell untersagt sind. Sie bedürfen eines Erlaubnistatbestandes, namentlich der Einwilligung des Subjektes. Ganz anders sind im DSG für den privaten Bereich Personendatenverarbeitungen grundsätzlich erlaubt. Verboten ist nur der qualifizierte Umgang mit Personendaten (insb. Verletzung der Verarbeitungsgrundsätze, Verarbeitung entgegen dem Widerspruch, Weitergabe von Persönlichkeitsprofilen und besonders schutzwürdigen Angaben an Dritte).

1009 Auch die Analyse der Einwilligungsvorgaben in *Spezialgesetzen wie dem HFG sowie dem GUMG* führte vor Augen, dass das schweizerische Datenschutzrecht *keine einheitliche Autonomie* des Datensubjektes über sämtliche Handlungsfelder hinweg implementiert. Vielmehr wird durch Normen und Erlasse mit datenschutzrechtlichen Bestimmungen ausserhalb des DSG *kontextspezifisch* nuanciert geregelt. Der Bereich des (Bio-)Medizinrechts ist als dasjenige Gebiet zu bezeichnen, in welchem der sog. Selbstbestimmung und damit dem Einwilligungserfordernis seit jeher eine prominente Rolle zugewiesen wurde.

1010 Das HFG schafft ein spezialgesetzliches Regime in Bezug auf den Umgang mit gesundheitsbezogenen Angaben im Forschungskontext. Es verankert ein hochdifferenziertes Gefüge, dessen Strukturierung kontextspezifisch geleitet ist. Das HFG unterscheidet die Einwilligungserfordernisse anhand einer Basisdifferenzierung danach, ob die Verarbeitung gesundheitsbezogener Personendaten originär zwecks Forschung erfolgt, also ob die Angaben zu Forschungszwecken erhoben werden oder ob diese weiterverwendet werden bzw. ob gesundheitsbezogene Personendaten aus einem anderen Kontext stammen, in dessen Rahmen sie primär erhoben wurden. Sichtbar wird anhand des HFG, dass datenschutzrechtlich kontextbezogen reguliert wird – in dieser Arbeit als *systemische und akzessorische Dimension des Datenschutzrechts* bezeichnet. Das Augenmerk der Regelung richtet sich auf *Datenflüsse* – in dieser Arbeit *dynamische Dimension* des Datenschutzrechts genannt. Die entsprechenden Ansätze finden sich, spezifisch für genetische Informationen, im Regelungsregime gemäss GUMG bestätigt. Sowohl HFG als auch GUMG sehen im Vergleich zum DSG eine differente und differenzierte Gestaltung der Einwilligungsvorgaben für den Umgang mit Personendaten vor. Beide Erlasse weisen der Einwilligung eine im Vergleich zum DSG stärkere Position zu.

1011 Folglich ist ein einheitliches und uniformes «informationelles Selbstbestimmungsrecht» dem schweizerischen Datenschutzrecht fremd. Dies heisst ebenso, dass es «das» Datensubjekt im Sinne eines «informationellen Einheitssubjekts» nicht gibt. Vielmehr präsentiert sich die Person und das Datensubjekt resp. Informationssubjekt facettenreich, mit pluralen informationellen Teilrollen resp. -persönlichkeiten. Seine Autonomiegrade sind je nach einschlägigem Recht und damit

relevantem gesellschaftlichem Bereich resp. Kontext unterschiedlich. Die Autonomieräume, die dem Datensubjekt durch Regelungen ausserhalb des DSG eingeräumt werden, sind facettenreich, die Positionierung der Einwilligung in den verschiedenen Feldern ist ausdifferenziert. Freigelegt wurde damit, dass die «Person», die Persönlichkeit, das Datensubjekt sich als bereichsspezifisch konkretisiertes Datensubjekt mit entsprechend variablen Autonomieräumen resp. -graden beschreiben lässt. Vordergründig zeigt sich allerdings das geltende Datenschutzrecht in Gestalt des DSG mit einer wirkungsdominanten Annahme – derjenigen eines kontext- und rollenblinden Datensubjektes, ein gewissermassen indifferentes Einheitssubjekt.

1012 Die Ausführungen zu den Tatbestandselementen der Persönlichkeitsverletzung gemäss DSG haben eine konsequente Anlehnung an die für das Persönlichkeitsrecht etablierte Figur der «qualifizierten» Verletzungshandlung für den privaten Bereich nachgewiesen. Dieser subjektiv-, abwehr- und deliktsrechtlichen Konzeption des DSG für den privaten Bereich folgt nun eine *Tour d'Horizon* über die *Umsetzungs- und Durchsetzungsinstrumente*. Damit wird dieser Abschnitt über die persönlichkeitsrechtliche Basierung des DSG für den privaten Bereich abgerundet. Gleichzeitig wird in den dritten Teil dieser Arbeit übergeleitet, der den Herausforderungen des aktuellen Datenschutzrechts nachgeht: Während der zweite Teil zeigte, dass sich die Funktionsweise des DSG anhand dreier Strukturmerkmale beschreiben lässt – Dualismus zwischen öffentlichem und privatem Bereich, generalklauselartige allgemeine Verarbeitungsvorgaben sowie persönlichkeitsrechtliche Anknüpfung und damit individual-, abwehr- sowie deliktsrechtliche Ausrichtung des DSG für den privaten Bereich –, wird im dritten Teil dieser Arbeit vorab auf die *Wirksamkeit und faktische Griffigkeit dieses Instrumentariums in der Praxis* eingegangen. Der dritte Teil wendet sich einer Kernproblematik des Datenschutzrechts und hierbei namentlich des DSG zu, dem sog. *Vollzugsdefizit*. Nach einer Auseinandersetzung mit den Fortschritten und Entwicklungen, die mit den jüngsten datenschutzrechtlichen Neuerungswellen einhergehen, wird ein Vorschlag zur Gestaltung eines wirksame(re)n Datenschutzrechts *de lege ferenda* vorgelegt.

C. Folgerung und Überleitung – Um- und Durchsetzung

1013 Die *Verwirklichung des Datenschutzrechts* hängt nicht unwesentlich auch von der Gestaltung des Umsetzungs- und Durchsetzungsinstrumentariums und der insofern gewählten Ansätze ab. Hierbei hat die *persönlichkeitsrechtliche Anknüpfung und Ausrichtung des DSG* für den privaten Bereich *de lege lata* massgeblichen Einfluss auf die Konzeptionierung der *Umsetzungs- und Durchsetzungs-*

instrumente. Die DSGVO sowie die Totalrevision des DSG sehen in diesem Feld durchgreifende Neuerungen vor. Der Massnahmen- und Sanktionenkatalog wurde markant ausgebaut sowie verschärft. Anlass zu dieser Verschärfung und zum Ausbau der möglichen behördlichen Anordnungen gab ein ernüchternder Befund, der in Bezug auf das bisherige Datenschutzrecht gemacht wurde. Für Deutschland in den Worten von Buchner:

> «In kaum einem Rechtsgebiet liegen Anspruch und Wirklichkeit so weit auseinander wie im Datenschutzrecht.»[1312]

1014 Auch für die Schweiz wird ein *Vollzugsdefizit* datenschutzrechtlicher Normierung beschrieben.[1313] Mit dem Begriff «Vollzugsdefizit» ist Verschiedenes gemeint. Zunächst geht es um die ungenügende Einhaltung der datenschutzgesetzlichen Vorgaben durch die Verarbeitenden. Es musste festgestellt werden, dass das datenschutzrechtskonforme Verhalten der Verarbeitenden eher bescheiden ist.[1314] Mehrere neue Instrumente der Totalrevision sollen hier ansetzen. Insbesondere das Verarbeitungsverzeichnis und die Datenschutz-Folgenabschätzung zielen darauf ab, eine faktische Effektuierung zu liefern. In Bezug auf die ungenügende Einhaltung des DSG vor Totalrevision ist sodann auf das Rechtsdurchsetzungsinstrumentarium einzugehen, das die persönlichkeitsrechtliche Anknüpfung rezipiert. Es geht hier zum einen um die Betroffenenrechte wie das Auskunftsrecht sowie zum anderen um die Rechtsbehelfe, die der betroffenen Person an die Hand gegeben werden, um gegen eine Persönlichkeitsverletzung durch private Verarbeitende gerichtlich vorzugehen, vgl. Art. 15 DSG und Art. 32 nDSG. Der individualrechtliche Rechtsschutz steht weder vor noch nach Totalrevision isoliert da. Er wird flankiert durch verwaltungsrechtliche sowie strafrechtliche Instrumente. Vor der Totalrevision des DSG müssen die den «zivilrechtlichen Datenschutz» ergänzenden Instrumente als schwach gestaltet beurteilt werden. Der bislang stark auf der Schulter der Datensubjekte ruhende Rechtsschutz wird mit Totalrevision ergänzt durch erweiterte Kompetenzen des EDÖB und verschärfte strafrechtliche Sanktionen, die durch die kantonalen Behörden verfügt werden, vgl. Art. 49 ff. nDSG und Art. 60 ff. nDSG.

1015 Bislang wurden die Betroffenenrechte, deren Verbürgung eng mit der individual- und persönlichkeitsrechtlichen Anknüpfung des DSG zusammenhängt, in der

1312 So der einleitende Satz von Buchner, 1; ähnlich Simitis, Symposium, 1 ff., 1; früh bereits ebenso Bull, Computer, 353; zudem Sachs, 19.

1313 Vgl. Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f., 23; indikativ hierfür Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.1; Bolliger/Féraud/Epiney/Hänni, 68; unlängst insb. auch Ebert/Widmer, 19; von einem gewissen Vollzugsdefizit sprechen Vasella/Sievers, digma 2017, 44 ff., 48 f.; in der schwachen Effektivität der Datenschutzerlasse in Europa wurde ein weiterer Grund verortet, weshalb in den USA bislang auf eine das Datenschutzrecht umfassende Datenschutzgesetzgebung verzichtet wurde, vgl. Mayer-Schönberger, Delete, 165.

1314 Vgl. Bolliger/Féraud/Epiney/Hänni, 30 ff.; Ebert/Widmer, 10 ff.

Praxis selten in Anspruch genommen. Zudem greifen die gerichtlichen Durchsetzungsinstrumentarien, die ebenso konsequent an den Persönlichkeitsschutz angelehnt sind, bloss rudimentär resp. punktuell.[1315]

1016 Solange das Datenschutzgesetz für den privaten Bereich in der Struktur des delikts- und abwehrrechtlich gedachten Persönlichkeitsschutzes angelegt ist, ist es folgerichtig, die *Verletzungshandlung* gegenüber dem Individuum, dem Datensubjekt, in das Zentrum der Aufmerksamkeit zu stellen und die «Verteidigung» des Datenschutzes dem Datensubjekt über das Arsenal der zivilrechtlichen Rechtsbehelfe zuzuweisen. Eine persönlichkeitsrechtlich fixierte Datenschutzgesetzgebung allerdings wirft die Frage auf, ob das *DSG mit seinen Strukturmerkmalen an sich geeignet ist, einen wirksamen Datenschutz zu gewährleisten*. Die insofern zu führende Diskussion ist diejenige über Schutzzweck und -objekt datenschutzrechtlicher resp. datenschutzgesetzlicher Normierung. Bis hierher wurden in dieser Arbeit mehrere Indizien herausgearbeitet, die dafürsprechen, den Datenschutz nicht isoliert dem Persönlichkeitsschutz zu verpflichten, stattdessen darüber hinausgehend systemische Schutzerwägungen als einschlägig zu inkludieren.[1316]

1017 An dieser Stelle geht es vorab allerdings um das Durchsetzungsinstrumentarium, wie es das aktuelle DSG vorsieht. *De lege lata* bilden – formell und theoretisch betrachtet – zunächst die den *Datensubjekten eingeräumten Rechte*, die sog. *Betroffenenrechte*, eine tragende Säule zur Verwirklichung des Datenschutzrechts.[1317]

1018 Hierbei ist zunächst das Auskunftsrecht gemäss Art. 8 DSG zu nennen. Das Auskunftsrecht beschränkt sich auf Personendaten, die sich in Datensammlungen befinden. Zudem formulieren Art. 9 f. DSG Gründe zur Verweigerung resp. Einschränkung der spiegelbildlichen Auskunftspflicht. Das Auskunftsrecht, so wird es gesagt, soll es der «betroffenen Person erleichtern, ihre datenschutzrechtlichen Ansprüche durchzusetzen, indem es ihr ermöglicht, Kenntnis davon zu erhalten, wer überhaupt Daten über sie bearbeitet».[1318] Theoretisch betrachtet kommt dem

1315 Vgl. Bolliger/Féraud/Epiney/Hänni, 38; Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.10 ff., insb. N 7.20 f.; interessant in diesem Zusammenhang der Befund von Ebert/Widmer, 16, wonach nur 35 Prozent der befragten Unternehmen einen Prozess zur Abwicklung von Auskunftsbegehren etabliert haben.

1316 Ein Recht auf informationellen Systemschutz als neuer Ansatz für ein «wirksames Datenschutzrecht», das über den Subjektschutz hinausgeht, diesen gleichwohl inkludiert, wird – nach einer kritischen Auseinandersetzung mit den derzeit präsentierten Lösungsansätzen zur Adressierung aktueller datenschutzrechtlicher Herausforderungen – im dritten Teil, IX. Kapitel elaboriert; der Begriff des Systemschutzes wird im datenschutzrechtlichen Kontext von Hoffmann-Riem, AöR 1998, 513 ff., 534 ff. verwendet, wobei ebenda nicht dieselbe Schutzkonzeption gemeint wird, wie sie in dieser Arbeit präsentiert wird; bereits Mallmann, 67 ff. statuierte, dass Privatheit eine Reihe existenzieller Funktionen für die Gesellschaft und den einzelnen erfülle.

1317 Vertiefend hierzu Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 5.

1318 Vgl. BBl 1988 II 414 ff., 452.

Auskunftsrecht in einem Regime, wie es die Schweiz *de lege lata* im DSG für den privaten Bereich aufgrund des Ausgangspunktes der prinzipiellen Verarbeitungsfreiheit mit Schranken und des Fehlens einer allgemeinen aktiven Informationspflicht vorsieht, besondere Bedeutung zu. Dem Auskunftsrecht wird Präventivwie Kontrollfunktion zugewiesen.[1319] Insofern wird vertreten, dass unrechtmässige Datenverarbeitungen resp. persönlichkeitsverletzende Verarbeitungshandlungen in aller Regel erst über die Wahrnehmung des Auskunftsrechts von den Betroffenen in Erfahrung gebracht würden, weshalb diesem Recht hohe Relevanz zugemessen wird.[1320] Dies reflektierend sieht das DSG für den Fall der Verletzung des Auskunftsrechts geeignete Instrumente vor, vgl. Art. 15 Abs. 4 DSG; sodann wird gemäss Art. 34 Abs. 1 lit. a DSG auf Antrag mit Busse bestraft, wer eine falsche oder unvollständige Auskunft erteilt. Zwar werden Auskunftsrechte in der Realität ausgeübt, allerdings muss die Bedeutung des Auskunftsrechts in Anbetracht des Ausmasses von Personendatenverarbeitungen gleichwohl als marginal bezeichnet werden. Es sind ernsthafte Zweifel daran anzubringen, im Auskunftsrecht des einzelnen Datensubjektes einen wirkungsstarken Mechanismus zu verorten, um die Einhaltung der Vorgaben des DSG zu verwirklichen.

1019 Wie erwähnt bringen die jüngsten datenschutzrechtlichen Entwicklungen neue Elemente und Ausrichtungen dergestalt, dass in erster Linie die Verantwortlichen in die Pflicht genommen werden, die Einhaltung der datenschutzrechtlichen Vorgaben umzusetzen und zu dokumentieren. Das Auskunftsrecht wird zwar beibehalten, die Last der «Umsetzungs- und Prüfungs- sowie Beweispflicht» wird indes verlagert. Das Auskunftsrecht selbst ist nach Totalrevision im 4. Kapitel unter dem Titel «Rechte der betroffenen Person» in Art. 25 ff. nDSG verbürgt. Weitere Ansprüche der Datensubjekte finden sich an anderen Stellen, so in Art. 32 nDSG. Zudem sind Informationspflichten gegenüber dem Datensubjekt zu beachten, vgl. Art. 19 ff. nDSG.

1020 Die *zivilrechtlichen Ansprüche* verbürgt Art. 15 Abs. 1 DSG resp. Art. 32 nDSG. Es handelt sich hier um die Klagebehelfe, die allgemein im Rahmen des Regimes der Persönlichkeitsverletzung gemäss Art. 28 ff. ZGB anerkannt sind. Im Rahmen des *zivilgerichtlichen Rechtsschutzes* sind die Klagen auf Unterlassung und Beseitigung, vgl. auch Art. 28a Abs. 1 Ziff. 1 und Ziff. 2, aber auch die Feststellungsklage, vgl. Art. 28a Abs. 1 Ziff. 3, eröffnet; daran anknüpfend die Klagen auf Schadenersatz, Genugtuung und Gewinnherausgabe.[1321] Für vertiefende Ausführungen zu den entsprechenden Ansprüchen und Klagen sei auf die einschlägige

1319 Vgl. m. w. H. Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 5 N 5.4.
1320 Vgl. Ders., a. a. O., § 5 N 5.85.
1321 Zu diesen Grundansprüchen vgl. Pedrazzini, in: Schweizer (Hrsg.), 81 ff., 82 ff., und 88 f., wo der Autor bereits früh auf den starken Ausbau der privatrechtlichen Durchsetzungsinstrumente qua DSG hinwies, allerdings Zweifel daran äusserte, ob sich diese in der Realität bewähren würden.

Kommentarliteratur verwiesen. Datenschutzgesetzliche Spezifika liefert Art. 15 Abs. 1 und Abs. 3 DSG mit den Ansprüchen auf eine Bearbeitungssperre sowie Sperre der Bekanntgabe, auf Berichtigung der Personendaten sowie auf Vernichtung resp. Löschung von Personendaten. Art. 15 Abs. 2 DSG sieht zudem das Instrument des Bestreitungsvermerkes vor. In der Totalrevision finden sich vergleichbare Ansprüche in Art. 32 Abs. 1, Abs. 3 und Abs. 4 nDSG. Unbestritten sollte sein, dass alle Ansprüche vorab auch aussergerichtlich geltend gemacht werden können.

1021 Für datenverarbeitende Unternehmen stellen die zivilrechtlichen Ansprüche der Datensubjekte formell, nicht aber in der Realität ein Risiko dar, da sie sowohl aussergerichtlich als auch gerichtlich kaum je durchgesetzt werden. Mit einer zivilrechtlichen Klage wegen Persönlichkeitsverletzung durch Personendatenverarbeitung hat in der Schweiz kaum jemand ernsthaft zu rechnen.[1322] Zudem ist zu attestieren, dass selbst eine individualrechtlich geführte Klage wegen Persönlichkeitsverletzung durch Personendatenverarbeitungen stets eine auf den Einzelfall gerichtete Beurteilung mit sich bringt. Das abwehrrechtlich strukturierte und im Persönlichkeitsrecht verwurzelte Durchsetzungsregime des Datenschutzrechts hat entsprechend kaum (bzw. keinerlei) für die Einhaltung motivierende resp. abschreckende Wirkung. Die *individualrechtliche und selbstverteidigte Privatsphäre* weist beträchtliche Schwachstellen auf.

1022 Der Vollständigkeit halber sei daher im Rahmen des zivilrechtlichen Rechtsschutzes auf Art. 89 Abs. 1 und Abs. 2 ZPO hingewiesen. Damit wird über das allgemeine zivilprozessuale Regime eine Verbandsklage auch für den Bereich des zivilrechtlichen Datenschutzes anerkannt.[1323] Zudem besteht die Möglichkeit, gerichtlich vorsorgliche Massnahmen zu verlangen, Art. 261 ff. ZPO.[1324]

1023 In diesem persönlichkeitsrechtlichen Klagenarsenal erschöpft sich das zivilrechtliche Durchsetzungsregime nicht. Vielmehr würden gemäss Rosenthal die *vertragsrechtlichen Sanktionierungen* in der Praxis als effektiver und wichtiger beurteilt.[1325] Zudem kann eine betroffene Person einen Strafantrag gemäss Art. 34 Abs. 1 DSG einreichen oder dem EDÖB eine Meldung erstatten, womit zu den

1322 Vgl. Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.20; vertiefend zur Rechtsprechung nachfolgend dritter Teil, VII. Kapitel, A.2.; zur fehlenden Rechtsdurchsetzung nicht nur in der Schweiz vgl. Burghardt/Böhm/Buchmann/Kuhling/Sivridis, in: Sivridis/Patrikakis/Burghardt et al. (Hrsg.), die von einer Nichtreaktion auf Auskunftsbegehren in rund 30 Prozent der Fälle berichten, 3 ff.

1323 Vgl. zum Vorentwurf der Revision der ZPO mit Blick auf den Ausbau der Verbandsklage und die Einführung eines Gruppenvergleichs Ceregato, Jusletter vom 10. September 2018, N 7 ff.; dagegen wurde die Einführung einer Verbandsklage im Rahmen der Verabschiedung des DSG abgelehnt, BBl 1988 II 414 ff., 465; zur Revision der ZPO mit ihrer Stärkung des kollektiven Rechtsschutzes auch Domanig, Jusletter vom 17. Juni 2019, N 5 ff.

1324 Rampini, BSK-DSG, Art. 15 N 33.

1325 So Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.22.

verwaltungsrechtlichen sowie strafrechtlichen Sanktionen bei Datenschutzverstössen übergeleitet wird.

1024 Auf die *verwaltungsrechtlichen Massnahmen* des EDÖB für den privaten Bereich, Art. 29 DSG, wurde bereits im Kapitel über den Dualismus eingegangen. Seine Kompetenzen sind – systemkonform – für den privaten Bereich insb. vor der Totalrevision nur beschränkt.[1326] Der EDÖB kann über seine Informations-, Aufklärungs- und Beratungsfunktion – in deren Rahmen insb. auch seine Leitfäden von Interesse sind[1327] – im Anschluss an eine Sachverhaltsabklärung, die er allerdings nur bei sog. Systemfehlern durchzuführen befugt ist, vgl. Art. 29 Abs. 1 DSG, eine Empfehlung erlassen. Kommt der Adressat dieser nicht nach, kann der EDÖB die Angelegenheit dem Verwaltungsgericht vorlegen.[1328] Entscheidungen vom Bundesverwaltungsgericht sind alsdann vom Bundesgericht überprüfbar. Hierbei ist zu verzeichnen, dass der EDÖB gerade in den letzten Jahren seine Interventionen intensiviert hat. Indem er seine Empfehlungen konsequenter durchsetzt, sind auch einige namhafte Urteile vonseiten des Bundesverwaltungsgerichts und Bundesgerichts ergangen.[1329] Ebendiese Urteile werden folgend genauer beleuchtet, wobei bereits an dieser Stelle festzuhalten ist, dass es Urteile von grundlegender Bedeutung sind, nicht zuletzt, indem sie datenschutzrechtliche Herausforderungen weit über einen verengten Blick auf das Individuum hinaus beleuchten. Hier deutet sich auch für die Schweiz der Bedeutungsgewinn und Bedeutungswandel im Datenschutzrecht an. Die Kompetenzen des EDÖB werden mit der Totalrevision neu gestaltet, vgl. Art. 49 ff. nDSG.[1330]

1025 Ergänzend ist festzuhalten, dass nicht nur der EDÖB datenschutzrechtlich eine Aufsichtsfunktion wahrnimmt. Vielmehr ist auf branchen- und sektorspezifische Regulierungen und Organisationen hinzuweisen. Allem voran zu nennen sind der Finanzmarktsektor sowie der Versicherungsbereich und hierbei die FINMA, welche in ihrer aufsichtsrechtlichen Funktion ebenso die Einhaltung datenschutzrechtlicher Vorgaben im Auge hat. So wird die Datenschutzrechtskonformität im Rahmen des Rundschreibens «operationelle Risiken» thematisiert. Die Möglichkeit aufsichtsrechtlicher Massnahmen vonseiten der FINMA im Kontext des Datenschutzes werde in der Praxis ernst genommen.[1331] Mit Blick auf die Einhaltung

1326 Vgl. zweiter Teil, IV. Kapitel, B.3.3.
1327 Abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden.html> (zuletzt besucht am 3. September 2021).
1328 Jüngst geschehen in der Angelegenheit BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018; Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.61, wonach es sich um ein Verwaltungsverfahren handle, das indes im Wesentlichen den Grundsätzen des Zivilprozesses folge; das Verfahren könne als eine Art Popularklage bezeichnet werden.
1329 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018.
1330 Hierzu Rosenthal, Jusletter vom 16. November 2020, N 181 ff.
1331 So Ders., in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.22; zur bankaufsichtsrechtlichen Relevanz des Datenschutzrechts, insb. des DSG, auch Meier, in: Emmenegger (Hrsg.), 1 ff.

datenschutzrechtlicher Vorgaben sowie deren Überprüfung präsentiert sich der Bankensektor mit einer gegenüber anderen Bereichen höheren Reife, was traditionell damit zu erklären ist, dass in der Branche seit jeher und ebenso im Zuge der jüngsten Fintech-Entwicklungen stark auf die Vertrauensbeziehung zwischen Finanzinstitut und Kunde gesetzt wird, in deren Zentrum das (mittlerweile kleine) traditionelle Schweizer Bank(kunden)geheimnis steht, vgl. Art. 47 BankG. Letzteres leitet zu den strafrechtlichen Sanktionierungen von Datenschutzverstössen über.

Im DSG finden sich *nur ganz punktuell strafrechtliche Sanktionierungsmöglichkeiten*, vgl. Art. 34 f. DSG.[1332] Von hoher Relevanz sind die Strafbestimmungen des StGB, die namentlich für den Geheimnisschutz vorgesehen sind, vgl. Art. 162 StGB; zudem ist im Zusammenhang mit Sanktionierungen im Kontext von Datenverarbeitungen auf Art. 179–179^{novies} hinzuweisen. Sodann finden sich Strafbestimmungen im Fernmeldegesetz, vgl. Art. 49 ff. FMG. Zu beachten ist die Strafandrohung gemäss Art. 23 Abs. 1 UWG mit seinem in Art. 3 Abs. 1 lit. o UWG niedergelegten Spam-Verbot sowie gemäss Art. 3 Abs. 1 lit. u UWG. Der Hinweis von Rosenthal im Zuge seiner Darstellung des Sanktionierungssystems bei Datenschutzverstössen, wonach die im UWG und StGB zu findenden Bestimmungen nicht als Normen des Datenschutzes wahrgenommen werden,[1333] dokumentiert, dass eine kontextuelle Sicht des Datenschutzrechts in der Schweiz (noch) nicht etabliert ist. Die Totalrevision baut die datenschutzgesetzlichen Strafbestimmungen markant aus, vgl. Art. 60 ff. nDSG.[1334] 1026

Mit der Totalrevision wird der *bisherige Akzent des DSG auf die Persönlichkeitsverletzung und die individualrechtliche Geltendmachung von Datenschutzrechtsverstössen markant ergänzt*. Bis zu ihrer Umsetzung bleibt die retrospektive und repressive sowie subjektivrechtliche Sichtweise prägend. Sie entspricht der Anknüpfung des Datenschutzrechts in einem defensivrechtlich sowie deliktsrechtlich angelegten Persönlichkeitsrecht, vgl. Art. 1 DSG. Dass hierin eine Mitursache für die ungenügende Wirksamkeit des Datenschutzrechts und spezifisch des Datenschutzgesetzes liegt, wird im VII. Kapitel des dritten Teils vertieft werden. Im VIII. Kapitel des dritten Teils wird kursorisch gezeigt, inwiefern die jüngsten datenschutzrechtlichen Neuerungen an diesem Schwachpunkt ansetzen. 1027

1332 Hierzu vertiefend Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.36 ff.
1333 Ders., a. a. O., § 7 N 7.56.
1334 Hierzu Ders., Jusletter vom 16. November 2020, N 191 ff.