3 Beschäftigtendatenschutz

535 Die Realisierung von Produktions- und Assistenzsystemen der Industrie 4.0 wird nicht nur die Arbeit selbst einem tiefgreifenden Wandel unterwerfen. Die damit einhergehende umfangreiche Datenverarbeitung birgt auch ein bisher nicht gekanntes Kontrollpotenzial.[756] Eine wesentliche Herausforderung bei der Entwicklung hin zur Industrie 4.0 besteht folglich darin, die technischen Innovationen so zu gestalten, dass die informationelle Selbstbestimmung der Beschäftigten gewahrt bleibt.

536 Die Fragen des Datenschutzes am Arbeitsplatz werden oft in Zusammenhang mit Überwachungsmaßnahmen diskutiert, mit denen der Arbeitgeber tatsächliche oder vermeintliche Pflichtverstöße der Beschäftigten gegen ihn aufzudecken versucht. In neuster Zeit betraf dies z.B. den besonders eingriffsintensiven Einsatz eines Keyloggers[757] oder das geradezu „traditionelle Thema"[758] der Videoüberwachung[759]. Dieser Problemkreis wird durch die Industrie 4.0 nicht kleiner werden, ist aber auch nichts, was diese Entwicklung auszeichnen würde. Im Gegenteil, die Diskussion zur Zukunft der Arbeit ist vielfach von großer Wertschätzung für die Beschäftigten geprägt, die stets unterstützt und nicht in erster Linie überwacht werden sollen.

537 Der Beschäftigtendatenschutz im Kontext der Industrie 4.0 äußert sich folglich spezifisch in der Frage, in welchem Maße die Unterstützung der Beschäftigten und die hierdurch erwarteten Effizienzgewinne – auch angesichts des enormen Kontrollpotenzials – eine umfangreichere Verarbeitung von Beschäftigtendaten rechtfertigen können. Obwohl ein erster derart gelagerter Fall bereits das Bundesarbeitsgericht erreicht hat,[760] steht die Diskussion hier noch am Anfang.

---

756 Hierzu eingehend *Krause* 2016b, S. 8 ff.; *Langheinrich* 2007, S. 236 f. sowie die speziellen Situationen unter Gliederungspunkt 3.6.2, S. 525.

757 BAG v. 27.7.2017 – 2 AZR 681/16, E 159, S. 380–394 (=NZA 2017, S. 1327).

758 *Krause* 2016a, S. 8.

759 BAG v. 22.9.2016 – 2 AZR 848/15, E 156, S. 370–383 (=NZA 2017, S. 112); BAG v. 20.10.2016 – 2 AZR 395/15, E 157, S. 69–83 (=NZA 2017, S. 443).

760 Zu einem Assistenzsystem für Busfahrer BAG v. 17.11.2016 – 2 AZR 730/15, NZA 2017, S. 394–398.

Im Folgenden soll ein systematischer Ansatz beschrieben werden, mit dem diese Grenze präziser als bisher ermittelt werden kann. Dabei werden die Vorarbeiten des arbeitsrechtlichen Kapitels eine doppelte Rolle spielen: Zum einen wirken sie sich maßgeblich auf die datenschutzrechtliche Prüfung aus, insbesondere auf deren Kontrolldichte (siehe 2.4.4, S. 193). Zum anderen können datenschutzrechtliche Anforderungen und Grenzen aber auch in die Gestaltung der Arbeit zurückwirken. So bergen besonders stark formalisierte Arbeitsaufgaben mit wenig Handlungsspielraum für die Beschäftigten nicht selten auch ein besonders hohes Kontrollpotenzial.[761] Datenschutzrechtliche Anforderungen könnten also u.U. auch durch eine menschengerechtere Gestaltung der Arbeit erfüllt werden. 538

3.1 Das Verhältnis von europäischen und deutschen Datenschutzrecht

Das Datenschutzrecht ist in weiten Teilen durch die Datenschutz-Grundverordnung (EU) 2016/679[762], die als Verordnung gemäß Art. 288 Abs. 2 AEUV in allen ihren Teilen verbindlich ist und in jedem Mitgliedstaat unmittelbar gilt, abschließend geregelt. Daran ändert auch der Umstand nichts, dass diese Regelungen teilweise sehr generalklauselartig gefasst sind.[763] Dennoch hat der deutsche Gesetzgeber als Reaktion auf die europäische Datenschutzreform ein neues Bundesdatenschutzgesetz[764] erlassen. 539

Das Verhältnis dieser beiden Regelungen ist im Grundsatz vergleichsweise simpel. Das Unionsrecht beanspruch in seinem Anwendungsbereich gegenüber dem mitgliedstaatlichen Recht einen Anwendungsvorrang (dazu noch näher 3.2.2.1.1, S. 262).[765] Das nationale Recht behält zwar seine Geltung, kann aber im Fall eines Konflikts mit dem europäischen Recht nicht angewendet werden.[766] Diesem Effekt trägt auch § 1 Abs. 5 BDSG 2018 540

761 *Kuhlmann/Schumann* 2015, S. 130.

762 Verordnung (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 (DS-GVO), Amtsblatt der Europäischen Union L 119/1.

763 *Hornung/Hofmann,* ZD-Beil. 4/2017, S. 1, 13 f. m.w.N.; kritisch vor allem *Roßnagel,* Ausschuss-Drs. 18(24)94, S. 2. Bereits die Datenschutzrichtlinie 95/46/EG wirkte vollharmonisierend EuGH, ECLI:EU:C:2011:777, Rn. 36 – *ASNEF*.

764 BGBl. I 2017, S. 2097.

765 EuGH, ECLI:EU:C:1970:114, Rn. 3 – *Internationale Handelsgesellschaft mbH*; EuGH, ECLI:EU:C:2013:107, Rn. 59 – *Melloni*.

766 Statt Vieler *Ruffert,* in: Calliess/Ruffert 2016, Art. 1 AEUV, Rn. 18.

Rechnung, demzufolge die Vorschriften dieses Gesetzes keine Anwendung finden, soweit das Recht der Europäischen Union, im Besonderen die Datenschutz-Grundverordnung unmittelbar gilt.

541 Diese einfache Regel wird jedoch durch Öffnungsklauseln verkompliziert. Die Datenschutz-Grundverordnung enthält an – je nach Zählweise – zwischen 50 und 60 Stellen[767] Öffnungsklauseln, in denen den Mitgliedstaaten die Möglichkeit eröffnet wird oder in denen sie dazu verpflichtet werden, Ausnahmen und Abweichungen zu definieren oder spezifische Vorschriften zu erlassen. Die Datenschutz-Grundverordnung wird darum treffend als „Handlungsformhybrid"[768] bezeichnet. Im Bereich des Beschäftigtendatenschutzes sind dies Art. 88 DS-GVO sowie für die Verarbeitung besonderer Kategorien personenbezogener Daten Art. 9 Abs. 2 lit. b DS-GVO.

3.1.1 Die Öffnungsklauseln zum Beschäftigtendatenschutz

542 Die Norm des Art. 88 DS-GVO gliedert sich in zwei Teile. In Absatz 1 wird den Mitgliedstaaten die Möglichkeit eröffnet, spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorzusehen, entweder selbst durch Rechtsvorschrift oder delegiert an die Sozialpartner durch Kollektivvereinbarung. Hinsichtlich der für die Datenverarbeitung zugelassenen Zwecke werden ähnlich wie schon in § 32 Abs. 1 BDSG 2003 drei Phasen des Arbeitsvertrags unterschieden: die Einstellung, die Erfüllung und die Beendigung. Diese Aufzählung ist anders als in § 32 Abs. 1 S. 1 BDSG 2003 nicht abschließend, was bedeutet, dass insbesondere auch Regelungen zur Einwilligung im Beschäftigungskontext erlassen werden dürfen.[769]

543 Die Erfüllung des Arbeitsvertrags wird sodann noch weiter aufgeschlüsselt. Mit einbezogen werden die Erfüllung der Pflichten aus Kollektivvereinbarung und Rechtsvorschriften und die Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen sowie Zwecke des Managements, der Planung und der Or-

767 *Veil* 2016.
768 *Kühling/Martini*, EuZW 2016, S. 448, 449.
769 *Jerchel/Schubert*, DuD 2016, S. 782, 784; BeckOK DSR/*Riesenhuber*, Art. 88 DS-GVO, Rn. 76; *Wybitul*, ZD 2016, S. 203, 205; a.A. *Spelge*, DuD 2016, S. 775, 781.

ganisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie des Schutzes des Eigentums der Arbeitgeber oder der Kunden.

544 In Art. 88 Abs. 2 DS-GVO stellt die Verordnung Anforderungen an die nach Absatz 1 möglichen Maßnahmen. Danach umfassen sie – d.h. müssen sie soweit erforderlich enthalten[770] – geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.

545 Gemäß Art. 9 Abs. 2 lit. b DS-GVO können die Mitgliedstaaten schließlich die Verarbeitung besonderer Kategorien personenbezogener Daten erlauben, wenn dies erforderlich ist, um arbeits- und sozialrechtliche Rechte auszuüben oder diesbezüglichen Pflichten nachzukommen. Dies kann wiederum durch mitgliedstaatliches Recht selbst oder durch Kollektivvereinbarungen nach dem Recht der Mitgliedstaaten erfolgen. Die Regeln müssen geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen.

3.1.2 Der Sockel europarechtlicher Vorgaben

546 Der europäische Verordnungsgeber hat sich mit der Öffnungsklausel des Art. 88 DS-GVO nicht von vornherein aus dem Beschäftigtendatenschutz zurückgezogen. Soweit die Mitgliedstaaten die Öffnungsklausel nicht nutzen, kommen die allgemeinen Regelungen der Datenschutz-Grundverordnung auch im Beschäftigungsverhältnis zur Anwendung. Als Erlaubnistatbestand käme dann insbesondere die Datenverarbeitung zur Erfüllung eines Vertrags – des Arbeitsvertrags – nach Art. 6 Abs. 1 UAbs. 1 lit. b bzw. Art. 9 Abs. 2 lit. b DS-GVO in Betracht.

547 Bei aller Unklarheit über die genaue Reichweite der Öffnungsklausel steht darüber hinaus fest, dass die Mitgliedstaaten den Beschäftigtendatenschutz nicht völlig autonom regeln dürfen und darum jedenfalls an die in Art. 5

770 BeckOK DSR/*Riesenhuber*, Art. 88 DS-GVO, Rn. 79; a.A. *Körner* 2017, S. 86, der zufolge diese Maßnahmen stets vorzusehen sind.

DS-GVO geregelten Grundsätze des Datenschutzrechts gebunden sind.[771] Dass ein gewisser Mindeststandard zum Schutz der Beschäftigten nicht unterboten werden darf, zeigt sich außerdem an den Anforderungen des Art. 88 Abs. 2 DS-GVO, die ausschließlich den Schutz der betroffenen Person bezwecken und keine Abwägung mit der unternehmerischen Freiheit des Arbeitgebers vorsehen.[772]

548 Daraus folgt, dass selbst im Falle einer umfassenden mitgliedstaatlichen Regelung das Unionsrecht nicht komplett außen vor bleibt. Dem steht auch nicht entgegen, dass die Union gemäß Art. 153 i.V.m. Art. 114 Abs. 2 AEUV über keine Kompetenz für harmonisierende arbeits- und sozialrechtliche Regelungen verfügt.[773] Der Beschäftigtendatenschutz weist zwar starke Verbindungen zum Arbeitsrecht auf, kann aber als Annex auf die allgemeine Regelungskompetenz der Union zum Datenschutzrecht nach Art. 16 Abs. 2 AEUV gestützt werden.[774]

3.1.3 Der Spielraum und die Anforderungen für die mitgliedstaatliche Regelung

549 Wieviel Spielraum den Mitgliedstaaten durch Art. 88 DS-GVO im Beschäftigtendatenschutz bleibt, ist umstritten. Die Diskussion betrifft vor allem die Frage, ob die Verordnung über die Mindeststandards hinaus vollharmonisierend wirkt,[775] also eine Konkretisierung aber keine Erhöhung des

771 *Forst,* in: Auernhammer 2020, Art. 88 DS-GVO, Rn. 4; *Körner* 2017, S. 55.

772 *Körner* 2017, S. 56.; i.E. auch *Kort,* DB 2016, S. 711, 714 f.; *Taeger/Rose,* BB 2016, S. 819, 830.

773 So aber *Franzen,* RDV 2014, S. 200, 201. Auf dieses Problem weist auch *Körner,* NZA 2016, S. 1383 hin, zieht daraus aber lediglich die Schlussfolgerung, dass Art. 88 DS-GVO für die mitgliedstaatlichen Regelungen keine Höchstgrenzen im Hinblick auf das Schutzniveau enthalte. Zur Regelungskompetenz allgemein *Franzen,* in: Franzen et al. 2020, Art. 153 AEUV, Rn. 72; *Korte,* in: Calliess/Ruffert 2016, Art. 114 AEUV, Rn. 18.

774 *Maschmann,* in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 39; *Schmidt* 2016, S. 49 I.E. *Däubler,* in: Däubler et al. 2020, Art. 88 DS-GVO, Rn. 3 f., der jedoch auf die hybride Handlungsform der Datenschutz-Grundverordnung abstellt (siehe 3.1, S. 239).

775 Dafür ausführlich *Maschmann,* DB 2016, S. 2480, 2482 ff.; *Maschmann,* in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 30 ff.; i.E. auch *Franzen,* EuZA 2017, S. 313, 344 f.; *Martini/Botta,* NZA 2018, S. 625, 627 f.; *Spelge,* DuD 2016, S. 775, 776; *Zöll,* in: Taeger/Gabel 2019, Art. 88 DS-GVO, Rn. 16 ff.; dagegen ausführlich *Körner* 2017, S. 52 ff.; i.E. auch *Düwell/Brink,* NZA 2017, S. 1081, 1083; *Forst,*

Schutzstandards erlaubt. Darüber hinaus geht es auch darum, welche Anforderungen die Öffnungsklausel selbst an die sie ausfüllende mitgliedstaatliche Regelung stellt.

3.1.3.1 Mindest- oder Vollharmonisierung

Für eine bloße Mindestharmonisierung wird der insofern offene Wortlaut des Art. 88 Abs. 1 DS-GVO angeführt.[776] Besieht man sich allerdings die Entstehungsgeschichte der Norm zeigt sich, dass sich trotz entsprechender Formulierungsvorschläge aus der Kommission und dem Parlament weder eine vollharmonisierende noch eine mindestharmonisierende Version durchsetzen konnte.[777] Der Streit ist schlicht offengeblieben. Für eine vollharmonisierende Wirkung sprechen vor allem die im Vergleich mit anderen Öffnungsklauseln strengen Voraussetzungen in Art. 88 DS-GVO.[778] Das übergeordnete Ziel der Verordnung, einen europaweit einheitlichen Rechtsrahmen zu bilden, kann bei Öffnungsklauseln, die notwendigerweise ein gewisses Maß an Uneinheitlichkeit mit sich bringen, dagegen nicht entscheidend sein.[779] 550

Angesichts der hybriden Handlungsform der Datenschutz-Grundverordnung (siehe 3.1, S. 239) spricht viel dafür, hier zu differenzieren, nämlich nach Teilen, die einer Richtlinie entsprechen, und nach Teilen, die einer Verordnung entsprechen.[780] 551

in: Auernhammer 2020, Art. 88 DS-GVO, Rn. 18 f.; für eine Absenkungsmöglichkeit bei entsprechenden Schutzmechanismen BeckOK DSR/*Riesenhuber*, Art. 88 DS-GVO, Rn. 67.

776 *Körner* 2017, S. 52 ff..

777 *Maschmann,* in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 34. Die Formulierungen lauteten „in den Grenzen dieser Verordnung" (Kommission) und „Unbeschadet der übrigen Vorschriften dieser Verordnung umfassen die in Abs. 1 genannten Rechtsvorschriften der Mitgliedstaaten wenigstens die folgenden Mindeststandards." Das übersieht *Körner* 2017, S. 53 ff., die nur auf die Ablehnung der Version der Kommission abstellt.

778 *Maschmann,* in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 35; *Pötters,* in: Gola 2018, Art. 88 DS-GVO, Rn. 25.

779 So aber *Maschmann,* in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 36 f.; *Pötters,* in: Gola 2018, Art. 88 DS-GVO, Rn. 24.

780 Ähnlich *Däubler,* in: Däubler et al. 2020, Art. 88 DS-GVO, Rn. 15, der die mindest- und vollharmonisierenden Bereiche aber genau anders herum einteilt.

552 Die Datenschutzrichtlinie wirkte nach Auffassung des Europäischen Gerichtshofs vollharmonisierend.[781] Aus dieser Richtlinie übernommene, sehr abstrakte Regelungen wie die der Datenschutzgrundsätze in Art. 5 oder der Erlaubnistatbestände in Art. 6 DS-GVO müssten dann ebenfalls als vollharmonisierend betrachtet werden. Sie dürfen nur konkretisiert werden.[782] Soweit die Öffnungsklausel aber sehr detailliert geregelte Bereiche betrifft, die eher der Natur einer Verordnung entsprechen und darum kaum an die Besonderheiten des Beschäftigungsverhältnisses angepasst werden können, entfaltet sie dagegen nur mindestharmonisierende Wirkung. Das beträfe z.B. Regelungen zur Transparenz,[783] die in Art. 88 Abs. 2 DS-GVO ausdrücklich angesprochen werden. Hier darf auch nach oben abgewichen werden.

3.1.3.2 Anforderungen in Art. 88 DS-GVO

553 Die mitgliedstaatlichen Regelungen können den Anwendungsvorrang des europäischen Rechts aber nur brechen und Vorgaben der Datenschutz-Grundverordnung konkretisieren oder davon abweichen, wenn sie Anforderungen erfüllen, welche in der Öffnungsklausel in Art. 88 DS-GVO an eben diese Regelungen gestellt werden.

554 Hier genügen nicht irgendwelche Regelungen, es muss sich vielmehr gemäß Art. 88 Abs. 1 DS-GVO um spezifischere Vorschriften handeln, die überdies Maßnahmen nach Art. 88 Abs. 2 DS-GVO umfassen. Werden die mitgliedstaatlichen Regelungen diesen Anforderungen nicht gerecht, verstoßen sie gegen zwingendes Unionsrecht, mit der Folge, dass sie aufgrund des Vorrangs des Unionsrechts nicht angewendet werden können.[784]

555 Der Öffnungsklausel in Art. 88 DS-GVO lassen sich zwei Anforderungen entnehmen, die nebeneinander bestehen. Die Vorschriften für die Datenverarbeitung im Beschäftigungskontext müssen erstens gemäß Absatz 1 spezifisch durch Rechtsvorschriften oder durch Kollektivvereinbarung geregelt sein. Darüber hinaus müssen sie zweitens die Schutzmaßnahmen nach Absatz 2 umfassen. Dies bedeutet aber nicht, dass eine Vorschrift bereits spezifisch nach Absatz 1 ist, wenn sie Maßnahmen nach Absatz 2 ent-

781 EuGH, ECLI:EU:C:2011:777, Rn. 36 – *ASNEF*.
782 So i.E. auch *Düwell/Brink,* NZA 2016, S. 665, 667; *Varadinek, et al.* 2018, S. 13.
783 In die Richtung *Franzen,* EuZA 2017, S. 313, 346.
784 So auch *Gola et al.,* RDV 2016, S. 57, 59; *Taeger/Rose,* BB 2016, S. 819, 830.

hält. Die Vorschriften beziehen sich auf unterschiedliche Regelungsbereiche.[785]

Die Vorgaben in Art. 88 Abs. 1 DS-GVO betreffen die materiellen Anforderungen an die Datenverarbeitung und dabei vor allem die Maßstäbe der Interessenabwägung, mithin das Datenschutzniveau. Die Vorgaben in Art. 88 Abs. 2 DS-GVO betreffen dagegen die verfahrensmäßige Absicherung der Datenverarbeitung, die dafür sorgen soll, dass dieses Datenschutzniveau eingehalten wird. Solche absichernden Maßnahmen ergeben aber nur Sinn, wenn hinsichtlich der materiellen Anforderungen die allgemeinen Vorgaben der Datenschutz-Grundverordnung wenigstens konkretisiert wurden. Ansonsten könnte man nämlich auf die in der Verordnung selbst geregelten Schutzmaßnahmen zurückgreifen. 556

3.1.4 Die Regelung zum Beschäftigtendatenschutz in § 26 BDSG 2018 im Überblick

Der deutsche Gesetzgeber hat den Spielraum der Öffnungsklausel genutzt und die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses in § 26 BDSG 2018 geregelt. Im Kern der Norm in § 26 Abs. 1 S. 1 BDSG 2018, welche den Hauptteil der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO aufgreift, wurde dabei die Vorgängerregelung in § 32 Abs. 1 S. 1 BDSG 2003 beinahe wortgleich fortgeschrieben. 557

Im Vergleich zur Öffnungsklausel in Art. 88 Abs. 1 DS-GVO ergeben sich in den für diese Arbeit relevanten Bereichen folgende Änderungen: 558

- Statt von der Einstellung, der Erfüllung des Arbeitsvertrags und der Beendigung des Beschäftigungsverhältnisses in Art. 88 Abs. 1 DS-GVO ist in § 26 Abs. 1 S. 1 BDSG 2018 von der Entscheidung über die Begründung eines Beschäftigungsverhältnisses sowie von der Durchführung und Beendigung des Beschäftigungsverhältnisses die Rede.
- Kollektivvereinbarungen werden in § 26 Abs. 4 Satz 1 BDSG 2018 als eigenständige Erlaubnistatbestände für die Verarbeitung personenbezogener Beschäftigtendaten zu Zwecken des Beschäftigungsverhältnisses anerkannt, einschließlich besonderer Kategorien personenbezogener Daten. Die Verhandlungspartner werden durch einen schlichten Verweis in § 26 Abs. 4 S. 2 BDSG 2018 an die Maßnahmen nach Art. 88 Abs. 2 DS-GVO gebunden.

785 *Klösel/Mahnhold*, NZA 2017, S. 1428, 1430.

– Die Anforderungen an die Einwilligung nach Art. 7 DS-GVO, die zwar in der Öffnungsklausel des Art. 88 Abs. 1 DS-GVO nicht ausdrücklich, dafür aber in ErwG 155 angesprochen sind, werden auf das Beschäftigungsverhältnis hin detailliert. Für die Beurteilung der Freiwilligkeit einer Einwilligung werden in § 26 Abs. 2 BDSG 2018 weitere Kriterien eingeführt und die Schriftform wird grundsätzlich festgelegt.

559 Darüber hinaus wurden die Öffnungsklauseln noch wie folgt genutzt:

– Die in der Öffnungsklausel nicht eigens genannte Interessenvertretung der Beschäftigten wurde in § 26 Abs. 1 S. 1 BDSG 2018 berücksichtigt. Die Ausübung bzw. Erfüllung ihrer gesetzlichen oder in einer Kollektivvereinbarung verankerten Rechte und Pflichten[786] ist ein zulässiger Zweck für die Datenverarbeitung.
– Der in Art. 88 Abs. 1 DS-GVO angeführte Zweck des Schutzes des Eigentums der Arbeitgeber oder der Kunden wird in den Regeln über die Datenverarbeitung zur Aufdeckung von Straftaten nach § 26 Abs. 1 S. 2 BDSG 2018 aufgegriffen. Dieser Regelungsbereich soll in dieser Arbeit aber nicht behandelt werden.
– Die Regeln über die Verarbeitung besonderer Kategorien personenbezogener Daten in Art. 9 Abs. 2 lit. b DS-GVO werden in § 26 Abs. 3 BDSG 2018 aufgegriffen. Die dort normierte Erforderlichkeit i.e.S. wird durch eine Interessenabwägung ergänzt und Schutzmaßnahmen nach § 22 Abs. 2 BDSG 2018 werden auch auf die Verarbeitung solcher Daten im Beschäftigungsverhältnis erstreckt.
– Der Anwendungsbereich des Datenschutzrechts wurde in § 26 Abs. 7 BDSG 2018 entgegen Art. 2 Abs. 1 DS-GVO auch auf die nichtautomatisierte Verarbeitung personenbezogener Daten außerhalb von Dateisystemen erweitert.

3.1.5 Die Nutzung des Ermessensspielraums in § 26 BDSG 2018

560 Ob der deutsche Gesetzgeber seinen Regelungsspielraum mit § 26 BDSG 2018 zulässigerweise genutzt hat, muss getrennt nach den einzelnen darin enthaltenden Vorschriften bewertet werden. Die Umsetzungsnorm des § 26 BDSG 2018 ist zweifellos eine Rechtsvorschrift und enthält wie eben dargestellt auch spezifische Vorschriften, etwa zu den Rechten und Pflichten der Interessenvertretung, der Einwilligung der Arbeitnehmer

786 Das Gesetz spricht von Ausübung *oder* Erfüllung ihrer Rechte und Pflichten. Das dürfte ein Redaktionsversehen sein.

und den Kollektivvereinbarungen.[787] Den Kern der Norm bildet aber die Generalklausel in § 26 Abs. 1 S. 1 BDSG 2018, die sich nur unwesentlich vom allgemeinen Erlaubnistatbestand in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO unterscheidet. Dies weckt erhebliche Zweifel an der europarechtlichen Zulässigkeit der Norm (dazu sogleich, siehe 3.1.5.2, S. 248).

3.1.5.1 Einwilligung und Kollektivvertrag § 26 Abs. 1 S. 2 ff. BDSG 2018

Zunächst fällt aber auf, dass in keinem Regelungsbereich in Art. 26 BDSG 2018 – auch nicht den spezifischen – Maßnahmen nach Art. 88 Abs. 2 DS-GVO ausdrücklich enthalten sind. Für die Kollektivvereinbarungen in § 26 Abs. 4 S. 1 BDSG 2018 ist dies unschädlich; die Pflichten ergeben sich unmittelbar aus Art. 88 Abs. 2 DS-GVO[788] und sind von den Parteien der Vereinbarungen selbst einzuhalten. Die Tarif- und Betriebsparteien können sich auf Art. 88 Abs. 1 und Art. 9 Abs. 2 lit. b DS-GVO i.V.m. §§ 3, 4 TVG bzw. §§ 77, 87 ff. BetrVG berufen. Einer Umsetzung speziell für das Datenschutzrecht in § 26 BDSG 2018 hätte es nicht bedurft. Die Regelung in § 26 Abs. 4 BDSG 2018 ist folglich rein deklaratorischer Natur.[789] 561

Aber selbst die Gegenauffassung, der zufolge sich die datenschutzrechtliche Regelungsmacht erst aus § 26 Abs. 4 S. 1 BDSG 2018 ergibt,[790] hätte in Bezug auf die Pflichten aus Art. 88 Abs. 2 DS-GVO keine negativen Auswirkungen. Die Anforderungen ergeben nämlich nur Sinn, wenn sich die darin adressierten Gefahren in der jeweiligen Vorschrift im Sinne des Art. 88 Abs. 1 DS-GVO auch in verstärktem Maße zeigen. Das ist angesichts der Fülle an Regelungsmöglichkeiten, die sich für Kollektivvereinbarungen aus § 26 Abs. 4 S. 1 DS-GVO ergeben, nicht absehbar. Insofern ge- 562

787 Insbesondere überschreitet die Konkretisierung des Merkmals der Freiwilligkeit nicht den Spielraum der Öffnungsklausel. So i.E. *Buchner/Kühling,* DuD 2017, S. 544, 546. Vgl. zu wesentlich weitgehenderen Entwürfen *Bäcker* 2012, S. 19 f.

788 Es genügt, dass den Kollektivvereinbarungen nach dem (sonstigen) Recht der Mitgliedstaaten „allgemein das Recht zugestanden [wird], verbindliche Regelungen zu treffen, die den Beschäftigten auch belasten können", *Maschmann,* in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 28.

789 *Düwell/Brink,* NZA 2017, S. 1081, 1085 Der Charakter der von § 26 Abs. 4 S. 1 BDSG ist umstritten, siehe 3.6.1.1.2, S. 488.

790 *Jerchel/Schubert,* DuD 2016, S. 782, 783; BeckOK DSR/*Riesenhuber*, Art. 88 DS-GVO, Rn. 49.

nügt es, dass der deutsche Gesetzgeber in § 26 Abs. 4 S. 2 BDSG 2018 lediglich einen Verweis auf Art. 88 Abs. 2 DS-GVO aufgenommen hat.[791]

563 Mit diesem Argument der spezifischen Gefahrerhöhung sind die Anforderungen an den nationalen Gesetzgeber aus Art. 88 Abs. 2 DS-GVO stark zu reduzieren. So ist es nicht ersichtlich, inwiefern die konkretisierten Anforderungen an die Einwilligung oder die Datenverarbeitung für die Interessenvertretung eine stärkere Gefährdung für die Grundrechte der betroffenen Person oder die Transparenz der Verarbeitung darstellen können oder inwiefern sie mit der Datenübermittelung in der Unternehmensgruppe oder der Überwachung am Arbeitsplatz zusammenhängen. Die Norm ist hier teleologisch zu reduzieren.[792] Die Regelungen verstoßen darum nicht gegen Art. 88 Abs. 2 DS-GVO.

3.1.5.2 Die Nutzung des Ermessensspielraums in § 26 Abs. 1 S. 1 BDSG 2018

564 Der Kern der Regelung in § 26 Abs. 1 S. 1 Fall 1 bis 3 BDSG 2018 – also ohne die Verarbeitung für die Rechte und Pflichten der Interessenvertretung – stellt dagegen jedenfalls für sich genommen keine spezifische Regelung nach Art. 88 Abs. 1 DS-GVO dar. Die Vorschrift konkretisiert den allgemeinen Erlaubnistatbestand für die Datenverarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO lediglich dahingehend, als sie auch die Begründung und die Beendigung des Vertrags als zulässige Zwecke erfasst. Diese Überlegung ist nicht nur zwingend und im Übrigen von jedem Rechtsanwender ohne Weiteres selbst zu bewältigen,[793] sie bleibt auch im Detaillierungsgrad sogar hinter der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO zurück. Schutzmaßnahmen nach Art. 88 Abs. 2 DS-GVO wurden ebenfalls nicht geregelt. Damit würde § 26 Abs. 1 S. 1 Fall 1 bis 3 BDSG 2018 von Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO verdrängt werden.

---

791 *Forst*, in: Auernhammer 2020, Art. 88 DS-GVO, Rn. 22; *Paal*, in: Paal/Pauly 2018, Art. 88 DS-GVO, Rn. 13; BeckOK DSR/*Riesenhuber*, Art. 88 DS-GVO, Rn. 79; *Wybitul*, ZD 2016, S. 203, 207.

792 *Forst*, in: Auernhammer 2020, Art. 88 DS-GVO, Rn. 22; BeckOK DSR/*Riesenhuber*, Art. 88 DS-GVO, Rn. 79; a.A. *Körner* 2017, S. 68.

793 Zur Einbeziehung des Vertragsabschlusses sowie der Vertragsänderung, -abwicklung und -beendigung, BeckOK DSR/*Albers/Veit*, Art. 6 DS-GVO, Rn. 31; *Buchner/Petri*, in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 33; *Plath*, in: Plath 2018, Art. 6 DS-GVO, Rn. 11.

Die Mehrzahl der Autoren in der Literatur[794] und wohl auch der deutsche Gesetzgeber[795] halten § 26 Abs. 1 S. 1 BDSG 2018 hingegen für spezifisch genug, um den Anforderungen in Art. 88 DS-GVO zu genügen. Entscheidend sei, dass das deutsche Beschäftigtendatenschutzrecht – auch auf Basis der Vorgängerregelung in § 32 Abs. 1 S. 1 BDSG – durch die Rechtsprechung des Bundesarbeitsgerichts konkretisiert wurde. Mit derselben Argumentation werden die Anforderungen des Art. 88 Abs. 2 DS-GVO bejaht.[796] 565

Eine andere Meinung lehnt diese Art der Umsetzung europäischer Vorgaben ab und sieht die Anforderungen des Art. 88 DS-GVO in § 26 Abs. 1 S. 1 Fall 1 bis 3 BDSG 2018 folglich nicht erfüllt.[797] Insbesondere *Maschmann*[798] hält der herrschenden Literatur entgegen, dass es zwar nicht per se ausgeschlossen sei, europäisches Recht mit Generalklauseln umzusetzen, die Umsetzung in § 26 Abs. 1 S. 1 BDSG 2018 aber die speziellen Anforderungen der Öffnungsklausel nicht beachte. 566

794 So *Gola et al.*, DuD 2017, S. 244, 245 ff.; *Seifert,* in: Simitis et al. 2019, Art. 88 DS-GVO, Rn. 52; *Wybitul et al.*, ZD 2015, S. 559, 561; *Wybitul/Pötters,* RDV 2016, S. 10, 14; *Zöll,* in: Taeger/Gabel 2019, Art. 88 DS-GVO, Rn. 10 ff.; ohne Begründung *Hense,* in: Sydow 2018, Art. 88 DS-GVO, Rn. 33; *Pötters,* in: Gola 2018, Art. 88 DS-GVO, Rn. 9 f. Für *Nolte,* in: Gierschmann et al. 2018, Art. 88 DS-GVO, Rn. 32 genügt offenbar schon, dass irgendwo in Art. 26 BDSG 2018 spezifische Regelungen gemacht werden.

795 Die Gesetzesbegründung liest sich so, als ob § 26 Abs. 1 S. 1 BDSG 2018 als Platzhalter für ein Beschäftigtendatenschutz dienen und einstweilen die in der Rechtsprechung entwickelten Grundsätze gelten sollen, BT-Drucks. 18/11325, S. 97: „Der Gesetzgeber behält sich vor, Fragen des Datenschutzes im Beschäftigungsverhältnis innerhalb dieser Vorschrift oder im Rahmen eines gesonderten Gesetzes konkretisierend bestimmte Grundsätze, die im Rahmen der Rechtsprechung zum geltenden Recht bereits angelegt sind, zu regeln."

796 *Gola et al.*, RDV 2016, S. 57, 60; *Wybitul/Pötters,* RDV 2016, S. 10, 14.

797 *Maschmann,* in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 63; in Bezug auf die beinahe wortgleiche Vorgängerregelung in § 32 BDSG 2003 *Körner* 2017, S. 68; *Maschmann,* DB 2016, S. 2480, 2484. Auch das am Gesetzgebungsverfahren beteiligte Bundesjustizministerium hat die Nichteinhaltung der Anforderungen des Art. 88 Abs. 2 DS-GVO kritisiert, *BMJV* 2016, S. 25. Zumindest zweifelnd *Däubler,* in: Däubler et al. 2020, Art. 88 DS-GVO, Rn. 22.

798 *Maschmann,* in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 63.

3.1.5.2.1 Die allgemeinen Anforderungen an Umsetzungsakte

567 Wie bei der Umsetzung einer Richtlinie haben die Mitgliedstaaten auch bei der Umsetzung von Öffnungsklauseln[799] das Recht zur Wahl der Form und Mittel. Die Umsetzung muss aber nicht nur in verbindliches innerstaatliches Recht erfolgen[800] – was bei § 26 Abs. 1 S. 1 BDSG unzweifelhaft der Fall ist –, sondern auch eine effektive Wirkung entfalten.[801] Hierzu gehört auch, dass die umsetzende Regelung so bestimmt ist, dass der Einzelne die Rechte, die ihm die europäische Regelung vermittelt, erkennen kann.[802]

568 Aus letzterem folgt, dass sich der Detaillierungsgrad, den die mitgliedstaatliche Regelung erreichen muss, anhand des Detaillierungsgrads des umzusetzenden europäischen Rechtsakts bestimmt. Will dieser bestimmte Rechte vermitteln, darf der Umsetzungsakt nicht hinter diesem Bestimmtheitsgrad zurückbleiben. Ob die notwendige vollständige Anwendung des umzusetzenden europäischen Rechtsakts gewährleistet ist, hängt darum – gewissermaßen als besondere Anforderung – von dessen inhaltlicher Genauigkeit ab.[803]

3.1.5.2.2 Die besonderen Anforderungen an die Regelungstiefe des Umsetzungsakts

569 Wie soeben gezeigt, müssen die allgemeinen Anforderungen an Umsetzungsakte was jenen Teilaspekt angeht, wie detailliert dieser Umsetzungsakt ausgestaltet zu sein hat, noch auf den jeweils umzusetzenden europäischen Rechtsakt angepasst werden. Dazu muss ermittelt werden, wie inhaltlich genau die Vorgaben in Art. 88 Abs. 1 und 2 DS-GVO ausfallen.

570 Dieser Detaillierungsgrad ist auffällig hoch. Die Öffnungsklausel in Art. 88 DS-GVO mutet trotz der eindeutigen Formulierung, „die Mitgliedstaaten können", beinahe wie ein Regelungsauftrag an. Insbesondere die Auffächerung der Durchführung des Beschäftigungsverhältnisses nach Art. 88 Abs. 1 DS-GVO in einzelne Beispiele kann als Wunsch nach detaillierten

799 Zur dieser Parallelität *Albrecht/Janson,* CR 2016, S. 500, 504.
800 EuGH, ECLI:EU:C:1982:192, Rn. 12 – *Kommission/Niederlande*.
801 EuGH, ECLI:EU:C:1984:153, Rn. 15 – *von Colson und Kamann*.
802 EuGH, ECLI:EU:C:1985:229, Rn. 23 – *Kommission/Deutschland*; EuGH, ECLI:EU:C:2001:35, Rn. 22 – *Kommission/Italien*.
803 *Schroeder,* in: Streinz 2018, Art. 288 AEUV, Rn. 78.

mitgliedstaatlichen Regelungen gedeutet werden. Gerade die Unterziele des Managements, der Planung und der Organisation der Arbeit sind in der neuen Regelung in § 26 BDSG 2018 nicht berücksichtigt und lassen sich, anders als bspw. die Gleichheit und Diversität oder die Gesundheit und Sicherheit am Arbeitsplatz, auch nicht auf bereichsspezifische Regelungen wie den Arbeitsschutz oder das Allgemeine Gleichbehandlungsgesetz stützen.

571 Vergleichsweise detaillierte Vorgaben finden sich auch zu den Schutzmaßnahmen nach Art. 88 Abs. 2 DS-GVO. Hier werden immerhin Regelungen zur Transparenz der Verarbeitung, zur Übermittlung von Daten in der Unternehmensgruppe und zu Überwachungssystemen am Arbeitsplatz gefordert. Gerade bei dem letzten Punkt hat der Verordnungsgeber in ErwG 75 zum Ausdruck gebracht, dass er die Verarbeitung persönlicher Aspekte, die die Arbeitsleistung betreffen, für besonders problematisch hält.

572 Angesichts der außergewöhnlich hohen inhaltlichen Genauigkeit der Öffnungsklauseln müssen die Anforderungen an die Bestimmtheit höher ausfallen als z.B. noch bei der Regelung des § 32 Abs. 1 S. 1 BDSG 2003, die mangels spezifischer Regelungen zum Beschäftigtendatenschutz in der Datenschutzrichtlinie nur den allgemeinen Erlaubnistatbestand in Art. 7 Abs. 1 lit. b DS-GVO umzusetzen hatte. Hinzu kommt, dass die Regelungen zum Beschäftigtendatenschutz zwar nicht unmittelbar darauf gerichtet sind, dem einzelnen Beschäftigten individuelle Rechte zu verleihen, aber immerhin eine Festlegung bezwecken, welche Datenverarbeitung in diesem speziellen Kontext zulässig ist. Davon hängen wiederum die Rechte der Betroffenen nach Art. 17 und 18 DS-GVO sowie letztlich auch die seiner Interessenvertretung im Betriebsrat ab.

3.1.5.2.3 Potenziell taugliche Umsetzungsakte

573 Den allgemeinen und besonderen Anforderungen an einen Umsetzungsakt kann prinzipiell auch durch eine Generalklausel entsprochen werden, wenn diese Klausel in der Rechtsausübung entsprechend interpretiert werden kann. Die genauen Voraussetzungen hierfür sind aber umstritten. Als Auslegungsmaßstab kommen sowohl nationale verfassungsrechtliche Grundsätze[804] als auch der umzusetzende Rechtsakt selbst in Betracht, hier also das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1

804 EuGH, ECLI:EU:C:1985:229, Rn. 23 – *Kommission/Deutschland*.

Abs. 1 GG in seiner Interpretation durch die Rechtsprechung des Bundesarbeitsgerichts bzw. die Öffnungsklausel in Art. 88 DS-GVO.

574 Nach einer strengeren Meinung genügt eine unionsrechtskonforme Auslegung allein nicht, damit eine nationale Norm den Rechtssicherheitsgrundsätzen des Europäischen Gerichtshofs gerecht wird. Anders als die verfassungskonforme Auslegung habe die unionsrechtskonforme Auslegung des nationalen Rechts nicht das Ziel, deren Geltung bzw. Anwendbarkeit zu erhalten.[805] Die umsetzende Norm müsse darum von sich heraus – d.h. ohne die konkretisierende Interpretation anhand des umzusetzenden Rechtsakts – dem Einzelnen ermöglichen, seine Rechte zu erkennen. Die Öffnungsklausel in Art. 88 DS-GVO fiele dieser Ansicht zufolge als Auslegungsmaßstab aus.

575 Für die Frage der Anwendbarkeit des europäischen oder mitgliedstaatlichen Datenschutzrechts kann dieser Streit aber letztlich offengelassen werden. Denn wenn sich die Vereinbarkeit des Umsetzungsakts allein aus der Interpretation anhand der europäischen Vorgabe ergibt, hat der mitgliedstaatliche Gesetzgeber jedenfalls keinen Spielraum genutzt, der eine eigenständige Regelung rechtfertigen würde. Wenn die Mitgliedstaaten eine Öffnungsklausel nicht nutzen, geht die konkurrierende Gesetzgebungskompetenz der Union vor, von der sie durch die Datenschutz-Grundverordnung umfassend Gebrauch gemacht hat (siehe 3.1.2, S. 241). Das ist die Konsequenz der Kompetenzverteilung im Datenschutzrecht.

576 Nach alledem kommt es für die Frage, ob der deutsche Gesetzgeber mit § 26 Abs. 1 S. 1 BDSG 2018 die Anforderungen an Umsetzungsakte für die Öffnungsklausel in Art. 88 DS-GVO erfüllt hat, allein darauf an, ob die deutsche Norm durch verfassungskonforme Auslegung entsprechend dieser Anforderungen interpretiert werden kann.

3.1.5.2.4 Die Bestimmtheit der Rechtsprechung des Bundesarbeitsgerichts

577 Für die Auslegungsfähigkeit von § 26 Abs. 1 S. 1 BDSG 2018 ist entscheidend, ob man mit der herrschenden Meinung die Rechtsprechung des Bundesarbeitsgerichts für konkret genug hält, um den Bestimmtheitsanforderungen an einen Umsetzungsakt zu genügen. Dabei kommt es nicht darauf an, ob das Bundesarbeitsgericht die Norm bereits hinreichend ge-

805 *Ruffert,* in: Calliess/Ruffert 2016, Art. 288 AEUV, Rn. 82, allerdings in Bezug auf Umsetzungsakte, die im Widerspruch zur nationalen Rechtsordnung stehen.

nau ausgelegt hat. Da die konkreten Umsetzungsakte zumeist neu sind, dürfte das in den wenigsten Konstellationen der Fall sein. Maßgeblich ist vielmehr, ob die bisherige Rechtsprechung – vor allem aber nicht zwingend nur zur Vorgängernorm – so gefestigt ist, dass sich belastbare Aussagen zur Interpretation des neuen Umsetzungsaktes treffen lassen.

578 Auf den ersten Blick mutet diese Argumentation zur Auslegbarkeit anhand gefestigter Rechtsprechung zirkulär an. Diese Rechtsprechung stützt sich nämlich ihrerseits auf die Interpretation des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG, ist also nicht einfachrechtlich, sondern maßgeblich grundrechtsgeleitet. Die Anwendbarkeit eben dieser deutschen Grundrechte wäre aber selbst erst eine Folge der zulässigen Nutzung der Öffnungsklausel (dazu noch eingehend 3.2.2, S. 260). Bevor aber ihre Anwendung nicht geklärt ist, kann schwerlich beurteilt werden, ob die deutschen Grundrechte die Umsetzungsnorm so weit spezifizieren, dass diese den Anforderungen der Öffnungsklausel in Art. 88 DS-GVO gerecht wird.

579 Dieser Widerspruch ist aber letztlich nur die Konsequenz einer möglichen kumulativen Anwendbarkeit unionaler und nationaler Regelungen (siehe 3.2.2.2.2, S. 267). Er lässt sich insofern auflösen, als dass sich die Anwendbarkeit der nationalen Grundrechte nicht allein aus diesen Grundrechten selbst, sondern aus dem Umstand ergibt, dass der Gesetzgeber immerhin eine einschlägige Generalklausel normiert hat, die entsprechend konkretisiert werden kann.

580 Die Anforderungen an die Bestimmtheit der Rechtsprechung des Bundesarbeitsgerichts im Hinblick auf Art. 26 Abs. 1 S. 1 BDSG 2018 sind nach den allgemeinen Grundsätzen nicht als übermäßig hoch einzuschätzen. So hat der Europäische Gerichtshof für Menschenrechte die Rechtsprechung zur Videoüberwachung von Arbeitnehmern als für einen Eingriff in Art. 8 EMRK hinreichend bestimmt angesehen.[806] Solche vergleichsweise schwerwiegenden Maßnahmen wären nach aktueller Rechtslage auf § 4 oder § 26 Abs. 1 S. 2 BDSG 2018 zu stützen.[807] Die Datenverarbeitung, die auf § 26 Abs. 1 S. 1 BDSG 2018 gestützt werden kann, dürfte deutlich weniger tief in Grundrechte eingreifen, zumal hier vor allem die Datenverarbeitung zur Organisation des Betriebsablaufs in Fokus stehen soll. Die

806 EGMR v. 5.10.2010 – 420/07, S. 10 f. – *Köpke/Deutschland*; BAG v. 27.3.2003 – 2 AZR 51/02, E 105, S. 356, Rn. 28 (=NZA 2003, S. 1193).

807 Zur Unionsrechtswidrigkeit von § 4 BDSG 2018 *Jandt,* ZRP 2018, S. 16, 17 f. Welche Regelung anzuwenden ist, soll eine Frage des Einzelfalls sein, *DSK*, Kurzpapier Nr. 15, S. 1.

Rechtsprechung ist diesbezüglich zwar nicht in dem Maße gefestigt, wie dies bei Überwachungsmaßnahmen der Fall ist (siehe 3.2.3.4.1, S. 293), insgesamt gibt es aber keine Anhaltspunkte dafür, dass sie die Anforderungen des Europäischen Gerichtshofs für Menschenrechte an die Bestimmtheit, denen sich auch der Europäische Gerichtshof angeschlossen hat,[808] nicht erfüllt.

581 Soweit es bei der Umsetzung der Öffnungsklausel in Art. 88 DS-GVO wie noch bei der Vorgängerregelung in § 32 Abs. 1 S. 1 BDSG 2003 allein darum gegangen wäre, die allgemeinen Erlaubnistatbestände zur Datenverarbeitung in Vertragsbeziehungen nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO bzw. Art. 7 lit. b DSRL umzusetzen, wäre § 26 Abs. 1 S. 1 BDSG 2018 darum nicht zu beanstanden.

582 Die Öffnungsklausel nach Art. 88 DS-GVO enthält in Absatz 1 und 2 aber die Anforderungen, spezifische Konstellationen des Beschäftigungskontextes zu regeln und dabei besondere Schutzmaßnahmen zu ergreifen. Diesen erhöhten Anforderungen wird die Rechtsprechung des Bundesarbeitsgerichts jedenfalls im Hinblick auf die oben angesprochenen Unterziele und Schutzmaßnahmen nicht gerecht. Gerade für die hier behandelte Datenverarbeitung zur Planung und Organisation der Arbeit und zur Analyse der Arbeitsleistung ist die Rechtsprechung mangels ausreichender Fälle anders als im Bereich der Mitarbeiterüberwachung weder gefestigt noch ausdifferenziert (siehe 3.6.2.3.3, S. 539). Hier hätte es einer gesetzgeberischen Initiative bedurft, was angesichts der bereits vor der europäischen Datenschutzreform mehrfach erfolglos in Angriff genommenen Gesetzesvorhaben aber wohl nicht zu erreichen war.[809]

583 Der deutsche Gesetzgeber war demnach zwar nicht verpflichtet, den Beschäftigtendatenschutz in Bezug auf alle in Art. 88 DS-GVO erwähnten Unterziele zu regeln. Art. 88 Abs. 1 DS-GVO bleibt eine Kann-Vorschrift. Eine Generalklausel wie in § 26 Abs. 1 S. 1 BDSG 2018 kann aber nicht als spezifische Regelung bezeichnet werden, auch nicht in ihrer Konkretisierung durch die Rechtsprechung des Bundesarbeitsgerichts. Es wäre darum nicht gerechtfertigt, den betroffenen Lebenssachverhalt maßgeblich den mitgliedstaatlichen Vorstellungen über den Beschäftigtendatenschutz zu unterstellen. Wo der nationale Gesetzgeber Spielräume nicht entsprechend den damit verbundenen Vorgaben nutzt, bleibt es bei der ausschließlichen Anwendung der Datenschutz-Grundverordnung.

---

808 EuGH, ECLI:EU:C:2003:294, Rn. 78 – *ORF*.
809 BeckOK DSR/*Riesenhuber*, § 32 BDSG, Rn. 3 ff.

3.1.5.2.5 Zwischenergebnis

Entgegen der herrschenden Meinung genügen die Regelungen in § 26 Abs. 1 S. 1 Fall 1 bis 3 BDSG 2018 nicht den Anforderungen der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO. Sie sind darum im Anwendungsbereich der Datenschutz-Grundverordnung selbst nicht anwendbar, sondern werden entsprechend des Vorrangs des Unionsrechts von Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO verdrängt. 584

Die übrigen Regelungen in § 26 BDSG 2018 fallen dagegen nicht unter den Anwendungsvorrang des Unionsrechts. Sie entsprechen den Anforderungen in Art. 88 DS-GVO bzw. können im Fall der Kollektivvereinbarungen nach § 26 Abs. 4 DS-GVO diesen Anforderungen entsprechen. 585

3.1.6 Ausdehnung des Anwendungsbereichs

Abschließend stellt sich die Frage, wie es zu beurteilen ist, dass der deutsche Gesetzgeber den Anwendungsbereich des Beschäftigtendatenschutzes mit § 26 Abs. 7 BDSG 2018 auf nicht automatisierte Datenverarbeitungen außerhalb von Dateisystemen erweitert hat. 586

Der Ausweitung des Anwendungsbereichs wird entgegengehalten, dass die Mitgliedstaaten nur spezifischere Vorschriften erlassen können, also auch nicht über den Anwendungsbereich der Verordnung hinaus gehen durften.[810] In diesem Fall würde die Regelung wegen Verstoß gegen EU-Recht unanwendbar. Die gegen die Ausweitung des Anwendungsbereichs gerichtete Meinung überspannt aber ohnehin die Wirkung einer Vollharmonisierung im Bereich des Art. 88 DS-GVO (dazu 3.1.3.1, S. 243). Eine Harmonisierungswirkung kann nicht über den Regelungsbereich der gesamten Verordnung hinausgehen. 587

Der Verordnungsgeber hat die nichtautomatisierte Datenverarbeitung nicht in den Anwendungsbereich nach Art. 2 Abs. 1 DS-GVO aufgenommen und auch nicht erkennen lassen, dass er sie nicht geregelt wissen will. Damit hat er seine Kompetenz in diesem Bereich nicht abschließend ausgeübt – wodurch die Mitgliedstaaten am Zug sind.[811] Die Ausweitung des 588

---

810 *Spelge*, DuD 2016, S. 775, 778 f.

811 So auch *Düwell/Brink*, NZA 2017, S. 1081, 1083; *Maschmann*, in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 66; BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 37.

Anwendungsbereichs in § 26 Abs. 7 BDSG 2018 ist darum nicht vom Anwendungsvorrang des Unionsrechts erfasst.

3.2 Primärrechtliche Vorgaben

589 Das Datenschutzrecht ist nicht erst seit der europäischen Datenschutzreform und dem Wirksamwerden der Datenschutz-Grundverordnung stark europarechtlich geprägt. Auch ihre Vorgängernorm, die Datenschutzrichtlinie 95/46/EG hatte bereits erheblichen Einfluss auf die Art der Prüfung und führte dazu, dass der Europäische Gerichtshof verschiedentlich nationale Verarbeitungstatbestände für mit der Richtlinie unvereinbar erklärte.[812]

590 In wesentlichen Punkten und gerade dann, wenn eine im Gesetz nicht weiter detaillierte Interessenabwägung über die Zulässigkeit der Datenverarbeitung entschied, waren darum auch der europäische Datenschutzstandard und die hierin wirkenden primärrechtlichen Vorgaben zu beachten. Unter der Geltung der Datenschutz-Grundverordnung, die das Datenschutzrecht zwar nicht vollends, aber doch wesentlich stärker als bisher harmonisiert, tritt dieser Effekt noch stärker zu Tage. Folglich stellt sich die Frage, in welchen Verhältnissen diese primärrechtlichen Vorgaben wirken und worin sie im Einzelnen bestehen.

3.2.1 Grundsätze des Grundrechtsschutzes in der EU

591 Der Grundrechtsschutz in der Europäischen Union speist sich nicht aus einem zentralen Dokument. Es bestehen vielmehr drei Rechtsquellen, denen die Grundrechte als unmittelbar geltende Rechtssätze entnommen werden können. Diese Rechtsquellen stehen aber nicht nebeneinander, sondern überlappen und ergänzen sich größtenteils, sodass letztlich ein umfassender und einheitlicher Grundrechtsschutz gewährleistet ist.

592 Auf die ersten beiden Rechtsquellen wird in Art. 6 Abs. 1 und 3 AEUV verwiesen: die Charta der Grundrechte der Europäischen Union nach Absatz 1 und die allgemeinen Grundsätze des Unionsrechts nach Absatz 3. Die dritte Rechtsquelle sind die Unionsverträge selbst, die einige Grund-

812 EuGH, ECLI:EU:C:2011:777, Rn. 49 – *ASNEF*; EuGH, ECLI:EU:C:2016:779, Rn. 64 – *Breyer*.

rechte nicht nur als Verweis in Art. 6 EUV, sondern – wie z.B. Art. 16 Abs. 1 AEUV – direkt enthalten.[813] Diese Rechtsquellen stehen sämtlich im Rang des Primärrechts.[814]

3.2.1.1 Adressaten der Grundrechte

Die Adressaten der EU-Grundrechte sind in erster Linie die Union selbst, also ihre Organe, Einrichtungen und sonstigen Stellen. Dies ergibt sich bereits aus dem Umstand, dass die Grundrechte sowohl der Charta nach Art. 6 Abs. 1 EUV als auch die Grundsätze nach Art. 6 Abs. 3 EUV unmittelbar geltendes Unionsrecht sind, das keiner Konkretisierung bedarf.[815] Für die Charta-Grundrechte ist dies darüber hinaus in Art. 51 Abs. 1 S. 1 GRC geregelt. 593

Für die Mitgliedstaaten gilt die Grundrechtecharta dagegen gemäß Art. 51 Abs. 1 S. 1 GRC ausschließlich bei der Durchführung des Rechts der Union. Dies vorausgesetzt, werden die Mitgliedstaaten umfassend an die Grundrechte gebunden, d.h. in all ihren regionalen und lokalen Untergliederungen und ebenfalls mit sämtlichen Organen, Einrichtungen und sonstigen Stellen.[816] Nach demselben Prinzip sind die Mitgliedstaaten an die Grundsatz-Grundrechte nach Art. 6 Abs. 3 EUV gebunden.[817] Fallen nationale Regelungen in den Geltungsbereich des Gemeinschaftsrechts, müssen sie mit den Grundsätzen des Unionsrechts vereinbar sein.[818] 594

813 Zum Ganzen *Jarass* 2016, Einleitung, Rn. 1 f.

814 Für die Charta EuGH, ECLI:EU:C:2010:21, Rn. 22 – *Kücükdeveci*; EuGH, ECLI:EU:C:2012:372, Rn. 17 – *ANGED*; *Jarass* 2016, Einleitung, Rn. 12; für die Grundsätze *Jarass* 2016, Einleitung, Rn. 31. In Bezug auf die direkt in den Verträgen geregelten Grundrechte ergibt sich dies bereits aus der Natur der Verträge.

815 *Jarass* 2016, Einleitung, Rn. 11, m.w.N.

816 Für die Bindung der Mitgliedstaaten *Jarass* 2016, Art. 51 GRC, Rn. 16; *Schwerdtfeger*, in: Meyer/Hölscheidt 2019, Art. 51 GRC, Rn. 56.

817 Zu dem Gleichlauf der Anwendungsbereiche EuGH, ECLI:EU:C:2013:105, Rn. 20 – *Åkerberg Fransson*; *Thym,* NVwZ 2013, S. 889, 890.

818 EuGH, ECLI:EU:C:2002:752, Rn. 30 – *Rodríguez Caballero*; EuGH, ECLI:EU:C:2005:709, Rn. 75 – *Mangold*.

3.2.1.2 Drittwirkung

595 Beide Adressatenkreise – die Union und die Mitgliedstaaten – sind umfassend in allen Tätigkeitsbereichen an die Grundrechte gebunden, d.h. sowohl im Rahmen ihrer legislativen als auch der exekutiven und judikativen Tätigkeit.[819] Insbesondere müssen die Gerichte das einfache Recht grundrechtskonform auslegen. Bei der unmittelbaren Anwendung von Sekundärrecht wie der Datenschutz-Grundverordnung ergibt sich dies direkt aus dem Rangverhältnis der Normen,[820] also der in Art. 6 Abs. 1 EUV vorgenommenen Einstufung der EU-Grundrechtecharta als Primärrecht. Für mitgliedstaatliche Regelungen wie das Bundesdatenschutzgesetz folgt dies mittelbar aus dem Grundsatz der europarechtskonformen Auslegung,[821] im konkreten Fall nach der entsprechend grundrechtskonform ausgelegten Datenschutz-Grundverordnung.

596 Die grundrechtskonforme Auslegung des einfachen Rechts ist auch bei privatrechtlichen Vorschriften geboten, sowohl beim Sekundärrecht der Union[822] als auch bei einfachrechtlichen Vorschriften der Mitgliedstaaten, die der Durchführung von Unionsrecht dienen[823]. Insofern wirken die Grundrechte auch für Private, die selbst keine Grundrechtsadressaten, sondern vielmehr Grundrechtsberechtigte sind.[824] Dieser Wirkmechanismus entspricht dem der mittelbaren Drittwirkung,[825] wie er auch für die Grundrechte des Grundgesetzes weithin anerkannt ist. Insofern kann auf die Ausführungen unter Gliederungspunkt 2.2.1, S. 77 verwiesen werden.

---

819 Für die Union *Jarass* 2016, Art. 51 GRC, Rn. 14; für die Mitgliedstaaten *Jarass* 2016, Art. 51 GRC, Rn. 21 ff.

820 EuGH, ECLI:EU:C:2014:317, Rn. 68 – *Google Spain*; EuGH, ECLI:EU:C:2014:2041, Rn. 69 – *Kamino*; EuGH, ECLI:EU:C:2014:2195, Rn. 51 – *A/B u.a.*; *Jarass* 2016, Einleitung, Rn. 53.

821 EuGH, ECLI:EU:C:2008:54, S. 70 – *Promusicae*; EuGH, ECLI:EU:C:2015:485, Rn. 34 – *Coty*; *Jarass* 2016, Einleitung, Rn. 57 f.

822 EuGH, ECLI:EU:C:2008:54, Rn. 68 – *Promusicae*; EuGH, ECLI:EU:C:2012:85, Rn. 52 – *SABAM*; EuGH, ECLI:EU:C:2013:521, Rn. 30 – *Alemo-Herron*; EuGH, ECLI:EU:C:2014:317, Rn. 68 – *Google Spain*.

823 EuGH, ECLI:EU:C:2015:485, Rn. 41 f. – *Coty*.

824 Für die Datenschutzrichtlinie EuGH, ECLI:EU:C:2014:317, Rn. 69 – *Google Spain*; allgemein *Streinz/Michl,* EuZW 2011, S. 384, Rn. 386 f.

825 Dafür GA Trstenjak, ECLI:EU:C:2011:559, Rn. 83; *Herresthal,* ZEuP 2014, S. 238, 254 f.; *Jarass* 2016, Art. 51 GRC, Rn. 37; *Kahl/Schwind,* EuR 2014, S. 170, 191 f.; *Schwerdtfeger,* in: Meyer/Hölscheidt 2019, Art. 51 GRC, Rn. 57 ff.; für eine in Ausnamefällen (konkret Art. 27 GRC) unmittelbare Drittwirkung GA Cruz Villalón, ECLI:EU:C:2013:491, Rn. 41.

3.2.1.3 Die Bedeutung von Rechtserkenntnisquellen

Neben den Rechtsquellen bestehen auch Rechtserkenntnisquellen. Ihnen können keine eigenen Rechtssätze entnommen werden; sie liefern lediglich die Grundlagen, mit deren Hilfe Rechtssätze aus den Rechtsquellen entnommen werden können.[826] Zu den Rechtserkenntnisquellen zählen für die Grundrechtecharta deren offizielle Erläuterungen[827] sowie in Bezug auf die allgemeinen Grundsätze des Unionsrechts die in Art. 6 Abs. 3 EUV erwähnten gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten sowie völkerrechtliche Verträge zum Schutze der Menschenrechte, denen die Mitgliedstaaten beigetreten sind, wie z.B. der Internationale Pakt über bürgerliche und politische Rechte.[828] 597

Die Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention – EMRK) nimmt in diesem System perspektivisch eine Doppelrolle ein. Solange die Europäische Union ihr nicht beigetreten ist, stellt die Konvention keine Rechtsquelle der Union dar.[829] Die Union ist zwar gemäß Art. 6 Abs. 2 EUV zum Beitritt zur Konvention verpflichtet, hat ihn nach Bedenken des Europäischen Gerichtshofs[830] aber noch nicht vollzogen. Bis dahin bildet die Konvention lediglich eine Rechtserkenntnisquelle, wobei sie unter diesen Erkenntnisquellen eine herausgehobene Stellung einnimmt.[831] Für die Grundsatz-Grundrechte ergibt sich dies unmittelbar aus Art. 6 Abs. 3 EUV, der die Konvention ausdrücklich als Rechtserkenntnisquelle nennt. Für die Charta-Grundrechte folgt die besondere Bedeutung[832] der Konvention aus Art. 52 Abs. 3 S. 1 GRC, demzufolge sich die Bedeutung und Tragweite der in Konvention und Charta parallel geregelten Grundrechte nach der Konvention richten. Wie sich aus Art. 52 Abs. 3 S. 2 GRC ergibt, bilden die 598

826 *Jarass* 2016, Einleitung, Rn. 1.
827 *Jarass* 2016, Einleitung, Rn. 3.
828 Zum Ganzen *Jarass* 2016, Einleitung, Rn. 32; speziell zum IPbpR EuGH, ECLI:EU:C:2006:429, Rn. 36 f. – *P/R*; *Bernsdorff,* in: Meyer/Hölscheidt 2019, Art. 8 GRC, Rn. 4.
829 EuGH, ECLI:EU:C:2015:535, Rn. 45 – *Inuit*.
830 EuGH, ECLI:EU:C:2014:2454.
831 *Jarass* 2016, Einleitung, Rn. 40; *Kingreen,* in: Calliess/Ruffert 2016, Art. 6 EUV, Rn. 6.
832 EuGH, ECLI:EU:C:2004:181, Rn. 48 – *Karner*; EuGH, ECLI:EU:C:2008:461, Rn. 283 – *Kadi*; EuGH, ECLI:EU:C:2009:219, Rn. 28 – *Gambazzi*; *Jarass* 2016, Art. 52 GRC, Rn. 56.

Grundrechte der Konvention dabei eine Untergrenze für die Auslegung der Charta-Grundrechte.[833]

599 Mit dem Beitritt der Union zur Europäischen Menschenrechtskonvention würde diese ein Bestandteil des Unionsrechts, wie jede andere angenommene völkerrechtliche Übereinkunft auch. In der Normenhierarchie stünde sie dann über dem Sekundärrecht, aber unter dem Primärrecht, also insbesondere unter der Charta und den allgemeinen Grundsätzen des Unionsrechts. Dies hätte zur Folge, dass die Konvention zwar gemäß Art. 53 GRC neben der Charta zur Anwendung käme, dabei aber grundsätzlich dem Vorrang des Primärrechts unterläge.[834] Da die Konvention aber gemäß Art. 52 Abs. 3 GRC weiterhin die Untergrenze der Auslegung der Charta-Grundrechte bildete, käme dieser Vorrang des Primärrechts diesbezüglich nicht zum Tragen.[835] Abgesehen von der Möglichkeit der Individualbeschwerde gegen Akte der Union, die nach dem Beitritt zur Konvention gemäß Art. 34 EMRK möglich wäre,[836] hätte ein Beitritt der Union darum keine praktischen Konsequenzen.

3.2.2 Anwendbarkeit und das Verhältnis zu mitgliedstaatlichen Grundrechten

600 Da der weit überwiegende Teil der Hoheitsakte in der Union durch die Mitgliedstaaten erlassen wird, ist die Anwendbarkeit der EU-Grundrechte nach Art. 51 Abs. 1 S. 1 GRC in diesem Bereich von großer Bedeutung. Als durchzuführendes Unionsrecht kommt vor allem das Sekundärrecht in Betracht,[837] weshalb die EU-Grundrechte u.a. Anwendung finden, soweit die betreffende Fallgestaltung durch eine Richtlinie oder eine Verordnung geregelt ist. Die notwendige Anknüpfung an das Unionsrecht ist zumindest dann gegeben, wenn die betreffende Aktivität des Mitgliedstaats konkret zur Anwendung des Unionsrechts führt und in einem unmittelbaren Zu-

833 GA Trstenjak, ECLI:EU:C:2012:389, Rn. 87; *Jarass* 2016, Art. 52 GRC, Rn. 62.
834 *Jarass* 2016, Einleitung, Rn. 44; *Schorkopf*, in: Grabitz et al. 2020, Lfg. 52, Art. 6 EUV, Rn. 57.
835 *Jarass* 2016, Einleitung, Rn. 45; *Schorkopf*, in: Grabitz et al. 2020, Lfg. 52, Art. 6 EUV, Rn. 57.
836 *Jarass* 2016, Einleitung, Rn. 44.
837 *Jarass* 2016, Art. 51 GRC, Rn. 17; *Schwerdtfeger*, in: Meyer/Hölscheidt 2019, Art. 51 GRC, Rn. 55.

sammenhang[838] hiermit steht.[839] Die Tatsache allein, dass die Union in dem betreffenden Feld regelungskompetent ist, spielt keine Rolle. Die Kompetenz muss auch tatsächlich genutzt worden sein.[840]

3.2.2.1 Das Verhältnis der EU-Grundrechte zu nationalen Grundrechten

Die Diskussion über die Anwendbarkeit der EU-Grundrechte ist eng verknüpft mit der Frage ihres Verhältnisses zu den nationalen Grundrechten. So äußert sich das Bundesverfassungsgericht nur dann zur Anwendbarkeit der EU-Grundrechte, wenn es in Abgrenzung hierzu die Anwendbarkeit der Grundrechte des Grundgesetzes prüft.[841] 601

Diese Abgrenzungsfrage stellt sich wiederum nur für die Hoheitsakte der Mitgliedstaaten, die das Recht der Union durchführen. Die Stellen der Union sind – jedenfalls praktisch (siehe 3.2.2.1.1.2, S. 263) – nicht an die nationalen Grundrechte gebunden; mitgliedstaatliches Handeln außerhalb der Geltung des Unionsrechts ist nicht an die EU-Grundrechte gebunden.[842] 602

838 Für den Zusammenhang der Regelung über die Antiterrordatei zum damaligen europäischen Datenschutz wurde die Unmittelbarkeit verneint, BVerfG v. 24.4.2013 – 1 BvR 1215/07, E 133, S. 277, 314 – *Antiterrordateigesetz*. Die Datenschutzrichtlinie 95/46/EG finde gemäß Art. 3 Abs. 2 DSRL ausdrücklich keine Anwendung auf die Datenverarbeitung betreffend die öffentliche Sicherheit. Auch bestehe ein Bezug zum Informationsaustausch nach Art. 2 Art. 2 des Beschlusses 2005/671/JI. Entscheidend war aber wohl, dass es keine unionsrechtliche Bestimmung gab, „die die Bundesrepublik Deutschland zur Einrichtung einer solchen Datei verpflichtet, sie daran hindert oder ihr diesbezüglich inhaltliche Vorgaben macht." Dies hat sich auch mit der europäischen Datenschutzreform und insbesondere der JI-Richtlinie (EU) 2016/680 nicht geändert.

839 EuGH, ECLI:EU:C:2014:126, Rn. 21 ff. – *Siragusa*; *Jarass* 2016, Art. 51 GRC, Rn. 19 f.

840 EuGH, ECLI:EU:C:2008:517, Rn. 18 – *Bartsch*; BVerfG v. 24.4.2013 – 1 BvR 1215/07, E 133, S. 277, 313 f. – *Antiterrordateigesetz*; *Jarass* 2016, Art. 51 GRC, Rn. 19.

841 So z.B. in BVerfG v. 24.4.2013 – 1 BvR 1215/07, E 133, S. 277, 313 f. – *Antiterrordateigesetz*.

842 *Jarass* 2016, Art. 51 GRC, S. 23 f.; *Schwerdtfeger*, in: Meyer/Hölscheidt 2019, Art. 51 GRC, Rn. 36 f.

3.2.2.1.1 Der Anwendungsvorrang des Unionsrechts

603 Der Problemkomplex erklärt sich vor dem Hintergrund des Anwendungsvorrangs des Unionsrechts gegenüber sämtlichem mitgliedstaatlichem Recht, also auch gegenüber Grundrechten und anderen Regelungen von Verfassungsrang.[843] Das nationale Recht behält zwar seine Geltung, kann aber im Fall eines Konflikts mit dem europäischen Recht nicht angewendet werden.[844] Dieser Effekt ist anerkannt, wird aber unterschiedlich begründet.

3.2.2.1.1.1 Der autonom europarechtliche Ansatz

604 Der Europäische Gerichtshof begründet den Anwendungsvorrang autonom europarechtlich aus den Verträgen und insbesondere mit der Notwendigkeit, die Verwirklichung der Vertragsziele nicht zu gefährden.[845] Bei der Anwendung des Unionsrechts sind die EU-Grundrechte zu beachten,[846] der Anwendungsvorrang des Unionsrechts steht aber ausdrücklich nicht unter der Bedingung, dass die EU-Grundrechte das Schutzniveau der nationalen Grundrechte erreichen.[847]

605 Aus der europarechtlichen Sicht ist dies nur konsequent. Der Anwendungsvorrang wird nicht auf die mitgliedstaatlichen Verfassungen gestützt; die Einhaltung der dort verankerten Grundrechte kann darum auch keine Bedingung hierfür sein. Die mitgliedstaatlichen Grundrechte dienen lediglich als Rechtserkenntnisquelle der EU-Grundrechte, weshalb der Grundrechtsschutz auf der Ebene des Unionsrechts quasi von allein ein adäquates Niveau erreicht.

---

843 EuGH, ECLI:EU:C:1970:114, Rn. 3 – *Internationale Handelsgesellschaft mbH*; EuGH, ECLI:EU:C:2013:107, Rn. 59 – *Melloni*.

844 Statt Vieler *Ruffert,* in: Calliess/Ruffert 2016, Art. 1 AEUV, Rn. 18.

845 Grundlegend EuGH, ECLI:EU:C:1964:66, S. 1269 f. – *Costa/ENEL*.

846 Zu den Grundsatz-Grundrechten EuGH, ECLI:EU:C:1970:114, Rn. 4 – *Internationale Handelsgesellschaft mbH*.; zu den Charta-Grundrechten.

847 EuGH, ECLI:EU:C:2013:107, Rn. 59 – *Melloni*; EuGH, ECLI:EU:C:2014:126, Rn. 32 – *Siragusa*.

3.2.2.1.1.2 Der verfassungsrechtliche Ansatz

606 Das Bundesverfassungsgericht begründet den Anwendungsvorrang dagegen mit der verfassungsrechtlichen Ermächtigung in Art. 23 GG, die den Rechtsanwendungsbefehl enthalte, von dem sich die Gemeinschaftsgewalt ableite.[848] Der Anwendungsvorrang des Unionsrechts wirke nur innerhalb dieser Ermächtigung, was das Bundesverfassungsgericht zum Anlass nimmt, Hoheitsakte der Union dahingehend zu überprüfen, ob sie den unantastbaren Kerngehalt der Verfassungsidentität des Grundgesetzes wahren[849] oder eine ersichtliche und erheblich ins Gewicht fallende Kompetenzüberschreitung seitens der Union darstellen („ausbrechender Rechtsakt").[850]

607 Aus dieser Sicht ist die Nichtanwendbarkeit der Grundrechte des Grundgesetzes ohne die Anwendbarkeit der EU-Grundrechte nicht denkbar. Damit die Grenze der Integrationsermächtigung des Art. 23 GG nicht überschritten wird, muss in der Union ein verbindlicher Grundrechtsstandard gewährleistet sein, welcher demjenigen des Grundgesetzes entspricht.[851] Da dies insbesondere durch die Rechtsprechung des Europäischen Gerichtshofs sichergestellt ist, verzichtet das Bundesverfassungsgericht darauf, das Unionsrecht anhand der Grundrechte des Grundgesetzes zu prüfen.[852]

3.2.2.1.2 Die Rolle der EU-Grundrechte beim Anwendungsvorrang

608 Der Vorrang des Unionsrechts hat nach beiden Auffassungen zur Folge, dass es keinen nationalen verfassungsrechtlichen Vorgaben unterworfen werden darf, welche die Verwirklichung der Vertragsziele gefährden. Die Anwendung nationaler Grundrechte muss darum ausscheiden, wenn da-

---

848 BVerfG v. 12.10.1993 – BvR 2134/92, E 89, S. 155, 190 – *Maastricht*; BVerfG v. 30.6.2009 – 2 BvE 2/08, E 123, S. 267, 397 – *Lissabon*; BVerfG v. 6.7.2010 – 2 BvR 2661/06, E 126, S. 286, 302 – *Ultra-vires-Kontrolle Honeywell*.

849 BVerfG v. 30.6.2009 – 2 BvE 2/08, E 123, S. 267, 354 – *Lissabon*; BVerfG v. 15.12.2015 – 2 BvR 2735/14, E 140, S. 317, 341 ff. – *Identitätskontrolle I*.

850 BVerfG v. 12.10.1993 – BvR 2134/92, E 89, S. 155, 188 – *Maastricht*; BVerfG v. 30.6.2009 – 2 BvE 2/08, E 123, S. 267, 353 f. – *Lissabon*; BVerfG v. 6.7.2010 – 2 BvR 2661/06, E 126, S. 286, 302–304 – *Ultra-vires-Kontrolle Honeywell*.

851 BVerfG v. 29.5.1974 – BvL 52/71, E 37, S. 271, 280 f. – *Solange I;* BVerfG v. 22.10.1986 – 2 BvR 197/83, E 73, S. 339, 377 – *Solange II*.

852 BVerfG v. 22.10.1986 – 2 BvR 197/83, E 73, S. 339, 378 ff. – *Solange II;* BVerfG v. 7.6.2000 – 2 BvL 1/97, E 102, S. 147, 164 – *Bananenmarktordnung*.

durch „der Vorrang, die Einheit und die Wirksamkeit des Unionsrechts beeinträchtigt werden."[853] Im Fall eindeutiger EU-Vorgaben, die den Mitgliedstaaten keinen Ermessensspielraum belassen, wird dies auch vom Bundesverfassungsgericht anerkannt.[854]

609 Dieses Ergebnis steht in einem nur mittelbaren Zusammenhang mit dem Anwendungsbereich der EU-Grundrechte für mitgliedstaatliche Stellen, wie er für die Charta-Grundrechte ausdrücklich in Art. 51 Abs. 1 S. 1 GRC normiert ist. Er ist eröffnet, wenn die Mitgliedstaaten das Recht der Union durchführen, worunter zwar u.a. das gesamte Primärrecht sowie das Sekundär- und Tertiärrecht fällt, nicht aber die EU-Grundrechte selbst. Letzteres würde nicht nur einen Zirkelschluss bedeuten,[855] sondern auch entgegen Art. 51 Abs. 1 GRC neue Zuständigkeiten[856] für den Europäischen Gerichtshof begründen. Die nationalen Grundrechte werden darum nicht speziell durch die EU-Grundrechte verdrängt, sondern durch das durchzuführende Unionsrecht nach Art. 51 Abs. 1 S. 1 GRC. Hier wirkt der allgemeine Anwendungsvorrang des Unionsrechts. Dass der Europäische Gerichtshof eigens betont, die Anwendung nationaler Grundrechte dürfe „das Schutzniveau der Charta" nicht beeinträchtigen,[857] ist lediglich dem Umstand geschuldet, dass die Charta ein wesentlicher Bestandteil des Unionsrechts ist.

610 Aus diesem allgemeinen Vorrang folgt, dass sich ein Mitgliedstaat nicht auf Art. 53 GRC berufen kann, wenn er der Anwendung des Unionsrechts grundrechtliche Schutzstandards entgegenhalten will, welche diejenigen der Charta übersteigen.[858] Die Norm regelt nämlich das Verhältnis der Charta-Grundrechte zu den nationalen Grundrechten, nicht das zum je-

853 EuGH, ECLI:EU:C:2013:105, Rn. 29 – *Åkerberg Fransson*; EuGH, ECLI:EU:C:2013:107, Rn. 59 f. – *Melloni*; EuGH, ECLI:EU:C:2014:126, Rn. 32 – *Siragusa*; EuGH, ECLI:EU:C:2014:2195, Rn. 44 – *A/B u.a.*

854 Für Verordnungen BVerfG v. 14.10.2008 – 1 BvF 4/05, E 122, S. 1, Rn. 80 – *Agrarmarktbeihilfe*; für Richtlinien BVerfG v. 13.3.2007 – 1 BvF 1/05, E 118, S. 79, 95 f. – *Treibhausgas-Emissionsberechtigungen*; BVerfG v. 11.3.2008 – 1 BvR 256/0, E 121, S. 1, 15 – *Vorratsdatenspeicherung I;* BVerfG v. 2.3.2010 – 1 BvR 256/08, E 125, S. 260, 306 f. – *Vorratsdatenspeicherung II;* BVerfG v. 19.7.2011 – 1 BvR 1916/09, E 129, S. 78, 103 – *Anwendungserweiterung*; BVerfG v. 24.4.2013 – 1 BvR 1215/07, E 133, S. 277, 313 f. – *Antiterrordateigesetz*.

855 *Jarass* 2016, Art. 51 GRC, Rn. 17.

856 EuGH, ECLI:EU:C:2013:105, Rn. 22 – *Åkerberg Fransson*.

857 EuGH, ECLI:EU:C:2013:105, Rn. 29 – *Åkerberg Fransson*; EuGH, ECLI:EU:C:2013:107, Rn. 60 – *Melloni*; EuGH, ECLI:EU:C:2014:2195, Rn. 44 – *A/B u.a.*

858 So ähnlich die Vorlagefrage bei EuGH, ECLI:EU:C:2013:107, Rn. 55 – *Melloni*.

weils einschlägigen – Anwendungsvorrang beanspruchenden – übrigen Unionsrecht. Die EU-Grundrechte kommen mittelbar zur Geltung, weil das Unionsrecht zwar Anwendungsvorrang vor den nationalen Grundrechten beansprucht, seinerseits aber mit den EU-Grundrechten vereinbar sein muss.[859] Für das hier in Rede stehende Sekundärrecht hat dies zur Folge, dass es EU-grundrechtskonform ausgelegt werden muss oder – wo diese Auslegung nicht möglich ist – nicht angewendet werden darf.[860]

611 Die nationalen und die unionalen Grundrechte geraten nach dem Gesagten nicht automatisch in Konflikt; diesen Fall regelt Art. 53 GRC. Soweit das nationale Grundrecht einen höheren Schutzstandard festschreibt als das jeweilige Charta-Grundrecht, gilt dieser höhere Standard. Verdrängt werden die nationalen Grundrechte lediglich durch EU-grundrechtskonform ausgelegtes Unionsrecht. Der Schutzstandard des nationalen Rechts wird folglich nur dann auf das Niveau der EU-Grundrechte abgesenkt, wenn er sonst im Widerspruch zu diesem durchzuführenden Unionsrecht steht.[861] Ohne diesen Kristallisationspunkt für die EU-Grundrechte im Sekundärrecht bleibt es bei der Regelung des Art. 53 GRC.

3.2.2.2 Die Durchführung des Unionsrechts in Öffnungsklauseln

612 Im Grundsatz gilt nach dem gesagten eine einfache Arbeitsteilung: Für das vereinheitlichte Unionsrecht gilt der EU-Grundrechtsschutz, für das einzelstaatliche Recht gelten die Grundrechte der jeweiligen Verfassung, hier also die des Grundgesetzes.[862] Dieser simple Grundsatz ist unmittelbar einsichtig, wenn mitgliedstaatliche Stellen einen eindeutigen, durch das Uni-

859 Vor dem Inkrafttreten der Charta hat der Europäische Gerichtshof diesen Mechanismus im Fall der Datenschutzrichtlinie auch auf die Europäische Menschenrechtskonvention ausgedehnt, EuGH, ECLI:EU:C:2003:294, Rn. 91 – *ORF*.

860 *Jarass* 2016, Art. 53 GRC, Rn. 25.

861 So sieht die spanische Verfassung als Teil des Rechts auf ein faires Verfahren vor, dass Personen nur aufgrund einer in Abwesenheit erfolgten Verurteilung auf einen Haftbefehl überstellt werden dürfen, wenn der Betroffene diese Verurteilung im Ausstellungsstaat zur Wahrung seiner Verteidigungsrechte anfechten kann (siehe EuGH, ECLI:EU:C:2013:107, Rn. 20 – *Melloni*). Dies widersprach in der konkreten Konstellation Art. 4a Abs. 1 des Rahmenbeschlusses 2002/584, der auch mit Art. 47 und 48 Abs. 2 GRC vereinbar ist. Die spanischer Verfassung war insofern nicht anzuwenden, EuGH, ECLI:EU:C:2013:107, Rn. 55 ff. – *Melloni*.

862 *Körner* 2017, S. 18.

onsrecht abschließend und zwingend definierten Rechtsbefehl umsetzen.[863]

613 Als problematisch erweisen sich aber die Fälle, in denen das Unionsrecht den Mitgliedstaaten Ermessens- oder Gestaltungsspielräume einräumt. Klassischerweise tritt diese Konstellation auf, wenn Richtlinien bei der gemäß Art. 288 Abs. 3 AEUV notwendigen mitgliedstaatlichen Umsetzung einen gewissen Spielraum gewähren. Das Problem zeigt sich aber auch, wenn gemäß Art. 288 Abs. 2 AEUV an sich unmittelbar geltende Verordnungen keine abschließende Regelung treffen,[864] weil sie z.B. Öffnungsklauseln enthalten.[865]

3.2.2.2.1 Die Problematik der Öffnungsklauseln im Beschäftigtendatenschutz

614 Für diese Arbeit stellt sich das Problem deswegen, weil der Datenschutz in der Datenschutz-Grundverordnung geregelt wird, die von den Mitgliedstaaten durchzuführen ist, für den Beschäftigtendatenschutz aber Öffnungsklauseln für die Mitgliedstaaten bestehen (siehe 3.1.1, S. 240). Hinsichtlich des besonders bedeutsamen Kerns der Norm in § 26 Abs. 1 S. 1 BDSG 2018 hat der Gesetzgeber zwar nach der hier vertretenen Meinung die Anforderungen in Art. 88 DS-GVO nicht erfüllt, weshalb sich das Problem in weiten Teilen nicht stellt. Das nimmt der Abgrenzung der Grundrechte aber nicht die Relevanz.

615 Dies hat drei Gründe: Erstens lassen sich die Argumente der herrschenden Meinung zur Anwendbarkeit von § 26 Abs. 1 S. 1 BDSG 2018 (siehe 3.1.5.2, S. 248) nicht völlig von der Hand weisen. Man könnte sich also auch mit guten Argumenten für die Anwendbarkeit von § 26 Abs. 1 S. 1 BDSG 2018 entscheiden. Zweitens gibt es seit Jahren umfassende Reformbestrebungen im Beschäftigtendatenschutz,[866] die der Gesetzgeber später noch für eine spezifische Regelung im Sinne von Art. 88 DS-GVO aufgreifen könnte. Und drittens – dieser Grund ist im Gegensatz zu den zwei vorherigen zwingend – können zumindest Kollektivvereinbarungen nach § 26

863 *Masing,* JZ 2015, S. 477, 481.
864 *Schroeder,* in: Streinz 2018, Art. 288 AEUV, Rn. 46.
865 *Albrecht/Janson,* CR 2016, S. 500, 504; zur verfassungsgerichtlichen Prüfung des durch eine Verordnung eingeräumten Spielraums BVerfG v. 14.10.2008 – 1 BvF 4/05, E 122, S. 1, Rn. 81 – *Agrarmarktbeihilfe*.
866 *Körner,* AuR 2015, S. 392; *Seifert,* in: Simitis 2014, § 32 BDSG, Rn. 2 f.

Abs. 4 BDSG 2018 die Anforderungen in Art. 88 DS-GVO (noch) erfüllen. Für sie stellt sich die Abgrenzungsproblematik in jedem Fall.

3.2.2.2.2 Die unterschiedlichen Ansätze der obersten Gerichte

Der Europäische Gerichtshof und das Bundesverfassungsgericht vertreten zum – von beiden im Ergebnis anerkannten – Anwendungsvorrang des europäischen Rechts unterschiedliche Ansätze (siehe 3.2.2.1.1, S. 262). Dies hat auch Auswirkungen auf die Abschichtung der Grundrechtsebenen. 616

3.2.2.2.2.1 Die kumulative Anwendung nach dem Europäischen Gerichtshof

Der Europäische Gerichtshof vertritt die Auffassung, dass ein Mitgliedstaat auch dann das Unionsrecht ausführt, wenn er das Ermessen nutzt, dass ihm das Unionsrecht gewährt.[867] Allgemein ist es für die Anwendbarkeit der EU-Grundrechte nicht erforderlich, dass der jeweilige Regelungsbereich vollständig durch das Unionsrecht bestimmt wird;[868] eine nur teilweise Determinierung genügt. 617

Im hier relevanten Fall einer Öffnungsklausel in einer Verordnung spreche hierfür, dass die Mitgliedstaaten weiterhin an die übrigen Bestimmungen der Verordnung gebunden und für die Ausübung des Ermessens in der Verordnung bestimmte Rechtsfolgen geregelt seien.[869] Nach dieser Begründung bezieht sich die Durchführung des Unionsrechts genau genom- 618

867 EuGH, ECLI:EU:C:2006:429, Rn. 104 f. – *Parlament/Rat*; EuGH, ECLI:EU:C:2011:865, Rn. 66 ff. – *N.S.*; so auch GA Trstenjak, ECLI:EU:C:2011:611, Rn. 82.

868 EuGH, ECLI:EU:C:2013:105, Rn. 29 – *Åkerberg Fransson*; *Jarass* 2016, Art. 51 GRC, Rn. 20a.

869 EuGH, ECLI:EU:C:2011:865, Rn. 66 f. – *N.S.* Die Mitgliedstaaten waren gemäß Art. 3 Abs. 2 der Dublin II Verordnung (EG) Nr. 343/2003 Asylanträge in Abweichung zu Art. 3 Abs. 1 der Verordnung selbst zu prüfen. Gemäß Art. 3 Abs. 2 S. 2 würden sie dadurch kraft der Verordnung für das Asylverfahren zuständig und mussten ggf. den zuvor zuständigen Mitgliedstaat darüber unterrichten.

men lediglich auf die Grenzen des Ermessens.[870] Dies zeigt aber auch, dass sich daran kaum beherrschbare Abgrenzungsschwierigkeiten anschließen.[871] So ist nicht nur die Öffnungsklausel selbst (EU-)grundrechtskonform auszulegen; eine wesentliche Grenze des Ermessens der Mitgliedstaaten bildet der Grundsatz der Verhältnismäßigkeit, der im Unionsrecht und damit in den EU-Grundrechten zu verorten wäre.[872]

619 Aus der Anwendbarkeit des Unionsrechts zieht der Europäische Gerichtshof jedoch nicht den Schluss, dass die nationalen Grundrechte in jedem Fall unanwendbar würden. „Wenn das Unionsrecht den Mitgliedstaaten bei der Durchführung eines Unionsrechtsakts einen Ermessensspielraum einräumt, [steht es] den nationalen Behörden und Gerichten weiterhin frei, die Einhaltung der durch die nationale Verfassung gewährleisteten Grundrechte sicherzustellen, sofern durch die Anwendung nationaler Schutzstandards für die Grundrechte weder das Schutzniveau der Charta, wie sie vom Gerichtshof ausgelegt wird, noch der Vorrang, die Einheit und die Wirksamkeit des Unionsrechts beeinträchtigt werden."[873]

620 Nach dieser Auffassung kommen die EU-Grundrechte und die nationalen Grundrechte kumulativ zur Anwendung.[874] Verdrängt werden die nationalen Grundrechte nur, wenn sie in Konflikt mit einer – EU-grundrechtskonform ausgelegten – Norm des Unionsrechts geraten. Das ist bei Unionsrecht, das den Mitgliedstaaten einen Ermessenspielraum einräumt, insbesondere dann der Fall, wenn für diesen Spielraum bestimmte Grenzen vorgegeben oder Anforderungen an die Ermessensausübung gestellt werden.[875] Im Übrigen entspricht es aber dem Wesen des Ermessensspielraums, dass es gerade erlaubt ist, vom Unionsrecht abzuweichen und ins-

870 *Albrecht/Janson,* CR 2016, S. 500, 505; *Cremer,* EuGRZ 2011, S. 545, 552; *Jarass* 2016, Art. 51 GRC, Rn. 20a; i.E. auch *Bäcker,* EuR 2015, S. 389, 393 f.; *Kirchhof,* NJW 2011, S. 3681, 3684; *Körner* 2017, S. 18.

871 *Bäcker,* EuR 2015, S. 389, 404; *Thym,* NVwZ 2013, S. 889, 892.

872 *Bäcker,* EuR 2015, S. 389, 396 f.; *Jarass,* NVwZ 2012, S. 457, 460.

873 EuGH, ECLI:EU:C:2014:126, Rn. 44 – *Siragusa*; ähnlich auch EuGH, ECLI:EU:C:2013:105, Rn. 29 – *Åkerberg Fransson*; EuGH, ECLI:EU:C:2017:936, Rn. 47 – *Taricco II*, wenngleich die Anwendbarkeit des Unionsrechts hier weitaus umstrittener war (siehe Fn. 881) und EuGH, ECLI:EU:C:2013:107, Rn. 60 – *Melloni*, bei dem aber ausdrücklich kein Ermessensspielraum bestand.

874 *Borowsky,* in: Meyer 2014, Art. 53 GRC, Rn. 14a; *Hoppe,* in: Meyer/Hölscheidt 2019, Art. 53 GRC, Rn. 29 ff.; *Jarass* 2016, Art. 53 GRC, Rn. 28; *Thym,* NVwZ 2013, S. 889, 892.

875 So für Art. 88 Abs. 2 *Körner* 2017, S. 18 (dort. Fn. 45).

besondere höhere Schutzstandards zu setzen.[876] Hierdurch wird „das Schutzniveau der Charta, wie sie vom Gerichtshof ausgelegt wird"[877] nicht beeinträchtigt, weil die Charta gemäß Art. 53 GRC nur einen Mindestschutz vorgibt.[878] Es gilt folglich das Meistbegünstigungsprinzip.[879]

621 Diese Auslegung stellt eine konsequente Fortsetzung der autonom europarechtlichen Begründung des Anwendungsvorrangs des Unionsrechts dar (siehe 3.2.2.1.1, S. 262). Es mag zwar nicht zwingend sein, über die dogmatisch gebotene Kontrolle der Grenzen der nationalen Spielräume derart weit in die Ausübung dieser Spielräume vorzustoßen. Wenn man diesen Weg aber beschreitet, ist es nur folgerichtig, dass die nationalen Grundrechte, die für die Begründung des Anwendungsvorrangs des Unionsrechts keine Rolle spielen, auch der Anwendung der EU-Grundrechte nicht entgegenstehen.

3.2.2.2.2.2 Die eingeschränkte Trennungsthese des Bundesverfassungsgerichts

622 Das Bundesverfassungsgericht hatte sich lange nicht umfassend zur kumulativen Anwendung unionaler und nationaler Grundrechte geäußert. In einem Fall, in dem der Europäische Gerichtshof die Anwendbarkeit der Charta-Grundrechte sehr weit ausdehnte, ist er ihr aber ausdrücklich entgegengetreten.[880] Im Feld des im Fall einschlägigen Steuerstrafrechts enthielt das Unionsrecht nur sehr abstrakte Vorgaben. Die unionsrechtliche Handlungspflicht der Mitgliedstaaten ergab sich erst aus der allgemeinen

876 Zum Spielraum, den eine Verordnung den Gerichten lässt, um nationale Grundrechte anzuwenden bereits EuGH, ECLI:EU:C:1989:321, Rn. 22 f. – *Wachauf*.

877 Siehe die Rechtsprechung des Europäischen Gerichtshofs in Fn. 873.

878 *Jarass* 2016, Art. 53 GRC, Rn. 29.

879 *Borowsky,* in: Meyer 2014, Art. 53 GRC, Rn. 22; *Hoppe,* in: Meyer/Hölscheidt 2019, Art. 53 GRC, Rn. 36; *Jarass* 2016, Art. 53 GRC, Rn. 28, jeweils m.w.N. Anschauliche Beispiele hierfür bei *Kingreen,* JZ 2013, S. 807. Das Ergebnis der Prüfung anhand der nationalen Grundrechte muss nicht mit den Vorgaben der Charta übereinstimmen. A.A. wohl *Thym,* NVwZ 2013, S. 889, 895 Nach *Kirchhof,* NJW 2011, S. 3681, 3684 f. ist die Formulierung in Art. 51 Abs. 1 S. 1 GRC „unter Wahrung des Subsidiaritätsprinzips" so auszulegen, dass die Charta erst zur Geltung kommt, soweit mitgliedstaatliche Grundrechte keinen hinreichenden Schutz gewährt. Das würde bedeuten, dass bei Gleichstand im Schutzniveau nur die nationalen Grundrechte Anwendung fänden.

880 BVerfG v. 24.4.2013 – 1 BvR 1215/07, E 133, S. 277, 316 – *Antiterrordateigesetz*.

Pflicht, innerhalb ihrer nationalen Verfahrensautonomie wirksame, abschreckende und verhältnismäßige Sanktionen bei Verstößen gegen das Unionsrecht vorzusehen.[881] Hier liegt es nahe, mit dem Bundesverfassungsgericht am notwendigen unmittelbaren Zusammenhang zwischen der mitgliedstaatlichen Maßnahme und der einschlägigen EU-Norm zu zweifeln.

623 Für den hier relevanten Bereich der durch Sekundärrecht gewährten Ermessenspielräume hat sich das Gericht erst kürzlich eindeutig positioniert. Danach finden in Öffnungsklauseln die unionalen und die Grundrechte des Grundgesetzes kumulativ Anwendung.[882]

624 Allgemein vertritt das Bundesverfassungsgericht die Auffassung, dass der Umsetzungsspielraum, den das Unionsrecht den Mitgliedstaaten lässt, grundgesetzkonform auszufüllen ist.[883] Bei der Auslegung nationalen Rechts, das nicht oder nicht vollständig unionsrechtlich determiniert ist, sind folglich die Grundrechte des Grundgesetzes zur Geltung zu brin-

881 Ausführlich *Kingreen*, JZ 2013, S. 802 ff.; *Thym*, NVwZ 2013, S. 889, 891 Der Europäische Gerichtshof (EuGH, ECLI:EU:C:2013:105, Rn. 25 ff. – *Åkerberg Fransson*) ließ es im Falle eines Strafverfahrens wegen der Hinterziehung von Mehrwertsteuer – neben den allgemeinen Handlungspflichten – ausreichen, dass die Mitgliedstaaten gemäß Art. 273 der Mehrwertsteuer-Richtlinie 2006/112/EG das Recht haben, zur Vermeidung von Steuerhinterziehung weitere Pflichten für die Steuerpflichtigen vorzusehen. Obwohl die Mitgliedstaaten zu keiner bestimmten Ausgestaltung des Sanktionssystems verpflichtet waren, betrachtete der Europäische Gerichtshof die steuerlichen Sanktionen und das Strafverfahren als Durchführung des Unionsrechts nach Art. 51 Abs. 1 S. 1 GRC. Das Bundesverfassungsgericht betonte daraufhin in einer Entscheidung zur Antiterrordatei, dass die betreffende nationale Regelung keine Durchführung des Unionsrecht darstelle (siehe bereits Fn. 838) und die Entscheidung des Europäischen Gerichtshofs als Ultra-vires-Akt zu beurteilen wäre, wenn „jeder sachliche Bezug einer Regelung zum bloß abstrakten Anwendungsbereich des Unionsrechts oder rein tatsächliche Auswirkungen auf dieses ausreiche." Der Europäische Gerichtshof hat dieses weite Verständnis zunächst bestätigt (EuGH, ECLI:EU:C:2015:555, Rn. 54 ff. – *Taricco I*), nach einer ähnlichen Drohung des italienischen Verfassungsgerichtshofs aber wieder entschärft (EuGH, ECLI:EU:C:2017:936, Rn. 58 – *Taricco II*). Dazu ausführlich *Burchardt*, EuR 2018, S. 248–263.

882 BVerfG v. 6.11.2019 – 1 BvR 16/13, E 152, S. 152–215, Rn. 43 f. – *Recht auf Vergessen I*. Zur Situation vor dem Beschluss *Thym*, NVwZ 2013, S. 889, 894.

883 BVerfG v. 18.7.2005 – 2 BvR 2236/04, E 113, S. 273, 300 – *Europäischer Haftbefehl*; BVerfG v. 19.7.2011 – 1 BvR 1916/09, E 129, S. 78, 103 – *Anwendungserweiterung*.

gen.[884] Entsprechend gestaltet sich die Abgrenzung der prozessualen Mittel zum Bundesverfassungsgericht und zum Europäischen Gerichtshof.[885]

In der Reaktion auf die oben genannte weite Auslegung des Anwendungsbereichs der Charta hatte das Bundesverfassungsgericht festgehalten, dass die angegriffenen Vorschriften über die Antiterrordatei […] schon deshalb an den Grundrechten des Grundgesetzes zu messen seien, weil sie nicht durch Unionsrecht determiniert sind."[886] Dies wurde teilweise als Wertung gegen die Anwendung unionaler Grundrechte in Ermessenspielräumen verstanden, da ein Unionsrecht, das solche Spielräume vorsieht die Handlungen der Mitgliedstaaten nur teilweise und nicht vollständig determiniert.[887] Indessen war diese etwas pauschale Aussage nur auf die spezielle Situation des Urteils, also insbesondere nicht auf mitgliedstaatliche Spielräume im Unionsrecht gemünzt.[888] 625

Der wesentliche Unterschied der beiden Konstellationen erklärt sich aus der Kompetenzverteilung der Union. Im Rahmen der geteilten Kompetenzen nach Art. 4 AEUV – zu denen gemäß Art. 16 Abs. 2 i.V.m. 4 Abs. 1 AEUV auch der Datenschutz gehört – nehmen die Mitgliedstaaten ihre Zuständigkeit gemäß Art. 2 Abs. 1 S. 2 AEUV wahr, sofern und soweit die Union ihre Zuständigkeit nicht ausgeübt hat. Wird also wie im umstrittenen Urteil des Europäischen Gerichtshofs zum Steuerstrafrecht ein Bereich vom Unionsrecht nicht oder nur am Rande geregelt, können daraus keine Vorgaben für die Mitgliedstaaten abgeleitet werden. Deren Ermessenspielräume würden lediglich durch die Existenz von Unionsrecht in diesem Kompetenzbereich begrenzt. Bei Öffnungsklauseln und Umsetzungsspielräumen gibt es dagegen meist eine Norm des Unionsrechts, die den Kom- 626

884 Für Verordnungen BVerfG v. 14.10.2008 – 1 BvF 4/05, E 122, S. 1, Rn. 80 – *Agrarmarktbeihilfe*; für Richtlinien BVerfG v. 13.3.2007 – 1 BvF 1/05, E 118, S. 79, 95 f. – *Treibhausgas-Emissionsberechtigungen*; BVerfG v. 11.3.2008 – 1 BvR 256/0, E 121, S. 1, 15 – *Vorratsdatenspeicherung I;* BVerfG v. 2.3.2010 – 1 BvR 256/08, E 125, S. 260, 306 f. – *Vorratsdatenspeicherung II;* BVerfG v. 19.7.2011 – 1 BvR 1916/09, E 129, S. 78, 103 – *Anwendungserweiterung*; BVerfG v. 24.4.2013 – 1 BvR 1215/07, E 133, S. 277, 313 f. – *Antiterrordateigesetz*.

885 Für die Verfassungsbeschwerde und das Vorabentscheidungsverfahren nach Art. 267 AEUV BVerfG v. 19.7.2011 – 1 BvR 1916/09, E 129, S. 78, 103 f. – *Anwendungserweiterung*; für die abstrakte und die konkrete Normenkontrolle BVerfG v. 13.3.2007 – 1 BvF 1/05, E 118, S. 79, 95 ff. – *Treibhausgas-Emissionsberechtigungen*.

886 Siehe Fn. 838.

887 So wurde die bisherige Position des Bundesverfassungsgerichts jedenfalls aufgefasst, siehe *Masing,* JZ 2015, S. 477, 481 f.; *Thym,* NVwZ 2013, S. 889, 894 f.

888 *Thym,* NVwZ 2013, S. 889, 895.

petenzbereich umfassend regelt und für die Bereiche, in denen sie sich zugunsten der Mitgliedstaaten zurücknimmt, spezifische Vorgaben enthält. Es ist etwas anderes, ob eine mitgliedstaatliche Maßnahme nur teilweise durch Unionsrecht determiniert wird, weil der betreffende Bereich nur am Rande geregelt ist, oder ob er nur teilweise determiniert wird, weil die Regelung des Unionsrechts bewusst einen Ermessenspielraum gewährt.

627 Der kumulativen Anwendung der unionalen und nationalen Grundrechte steht schließlich auch nicht die verfassungsrechtliche Begründung für den Anwendungsvorrang des Unionsrechts (siehe 3.2.2.1.1, S. 262) entgegen. Das Bundesverfassungsgericht verzichtet hier auf die Prüfung anhand der Grundrechte des Grundgesetzes, weil über die EU-Grundrechte ein hinreichender Schutz gewährleistet ist. Aus dem Umstand, dass die Nichtanwendung der nationalen Grundrechte ohne die stattdessen erfolgende Anwendung der EU-Grundrechte nicht denkbar ist, kann nicht der Umkehrschluss gezogen werden, dass die Anwendung der nationalen Grundrechte diejenige der unionalen Grundrechte ausschließt.

628 Für die Zurückhaltung des Bundesverfassungsgerichts ist entscheidend, dass sich Deutschland nur dann in Konflikt mit dem Unionsrecht setzt, wenn dies der Grundrechtsschutz als Identitätsmerkmal des Grundgesetzes erfordert. Dieser grundrechtliche Mindestschutz ist aber durch die gleichzeitige Anwendung der EU-Grundrechte nicht gefährdet, weil der Schutzstandard der nationalen Grundrechte gemäß dem Meistbegünstigungsprinzip nach Art. 53 GRC außerhalb des Anwendungsvorrangs zwingenden Unionsrechts nicht gesenkt wird. In den Ermessenspielräumen, die das Unionsrecht den Mitgliedstaaten gibt, ist folglich grundsätzlich kein Konflikt zu befürchten, der einer kumulativen Anwendung unionaler und nationaler Grundrechte entgegenstünde.

3.2.2.3 Probleme bei Grundrechtskollisionen

629 Nach dem Gesagten ist grundsätzlich davon auszugehen, dass in Öffnungsklauseln unionale und nationale Grundrechte nebeneinander anwendbar sind. Dies beantwortet zugleich die eingangs aufgeworfene Frage (siehe 3.2.1.2, S. 258) dahingehend, dass Mitgliedstaaten das Recht der Union auch dann nach Art. 51 Abs. 1 S. 1 GRC durchführen, wenn sie Öffnungsklauseln mit nationalen Regelungen oder Maßnahmen ausfüllen.

630 Diese Erkenntnis beruht wesentlich auf dem Meistbegünstigungsprinzip des Art. 53 GRC. Die Anwendung dieses an sich einfachen Prinzips bereitet aber dann Probleme, wenn Grundrechte – wie im Fall der Drittwir-

kung unter Privaten (siehe 3.2.1.2, S. 258) – miteinander kollidieren und unterschiedliche Schutzstandards für eines oder beide Rechte bestehen.

3.2.2.3.1 Die Nichtanwendbarkeit des Meistbegünstigungsprinzips

631 Das Meistbegünstigungsprinzip nach Art. 53 GRC funktioniert nur solange, wie sich lediglich der grundrechtsgebundene Staat und grundrechtsberechtigte Bürger gegenüberstehen. Stehen sich wie im Arbeitsverhältnis zwei grundrechtsberechtigte Subjekte gegenüber, kann unmöglich beiden Parteien gleichzeitig zu Lasten der jeweils anderen ein meistbegünstigender Grundrechtsschutz gewährt werden.[889] Würde man dem einen Grundrecht einen eventuell höheren Schutzstandard zubilligen, als ihn die Charta gewährt, würde das zwangsläufig das Schutzniveau der Charta für das andere Grundrecht beeinträchtigen. Damit wären aber die vom Europäischen Gerichtshof formulierten Voraussetzungen für die Anwendung nationaler Grundrechte nicht erfüllt.[890]

632 Wenn der Mechanismus des Art. 53 GRC nicht greift, käme zwangsläufig der Anwendungsvorrang des Unionsrechts zum Tragen.[891] Über die Balance der Grundrechte entschieden dann allein die Schutzstandards der EU-Grundrechte, was insbesondere darin zum Ausdruck kommt, dass das Verhältnismäßigkeitsprinzip so zu wahren ist, wie es sich aus dem Unionsrecht ergibt.[892] Mit Blick auf die auch in den Unionsverträgen anerkannte nationale Verfassungsidentität ist ein solcher Konflikt zwischen den nationalen Vorstellungen über die Verhältnis zwischen kollidierenden Grundrechten und jenen Vorstellungen, die das EU-Recht zu dieser Kollision hat, aber tunlichst zu vermeiden.[893] Es darf insbesondere nicht dazu führen, dass die Anwendung nationaler Grundrechte in Dreiecksituationen von

889 *Jarass* 2016, Art. 53 GRC, Rn. 31, m.w.N.; *Albrecht/Janson,* CR 2016, S. 500, 505; *Buchholtz,* DÖV 2017, S. 837, 841; *Kingreen,* JZ 2013, S. 807; *Masing,* JZ 2015, S. 477, 484.

890 *Jarass* 2016, Art. 53 GRC, Rn. 32; zu diesen Voraussetzungen EuGH, ECLI:EU:C:2013:107, Rn. 60 – *Melloni*; EuGH, ECLI:EU:C:2014:126, Rn. 44 – *Siragusa*.

891 So ähnlich *Albrecht/Janson,* CR 2016, S. 500, 506; *Bäcker,* EuR 2015, S. 389, 398 f.; *Thym,* JZ 2015, S. 53, 60.

892 EuGH, ECLI:EU:C:2008:54, Rn. 68 – *Promusicae*.

893 Zum Ganzen *Jarass* 2016, Art. 53 GRC, Rn. 32, m.w.N.

vornherein ausscheidet[894] und so der Grundsatz, dass sich die Anwendung der EU-Grundrechte nur auf die Grenzen des Ermessensspielraums, nicht aber auf dessen Ausfüllung bezieht,[895] vollends negiert wird.

3.2.2.3.2 Verfahrensrechtlicher Abgrenzungsversuch bei Grundrechtskollisionen

633 Dass die Grundrechte des Grundgesetzes in vielen Fällen auch in nur teilweise unionsrechtlich determinierten Regelungsbereichen letztlich doch durch die EU-Grundrechte verdrängt werden, wird als unbefriedigend empfunden. Dies dürfte weniger am Schutzgehalt der Grundrechte selbst liegen, sondern vielmehr an der bisher in weiten Teilen unterentwickelten Grundrechtsdogmatik des Europäischen Gerichtshofs.[896] Darum nimmt das Bundesverfassungsgericht in solchen Situationen die Interessenabwägung zunächst allein anhand der nationalen Grundrechte vor. Dem Europäischen Gerichtshof legt die Frage nur vor, wenn Anhaltspunkte dafür bestehen, dass das gefundene Ergebnis vom Schutzstandard der EU-Grundrechte abweicht.[897] Dadurch – so die Hoffnung in der Literatur, die diese Lösung vorgeschlagen hatte – könnte sich der Europäische Gerichtshof gewissermaßen von der in der Vorlagefrage dargelegten, deutlich komplexeren deutschen Grundrechtsdogmatik inspirieren lassen.[898]

634 Ein solcher eher verfahrensrechtlicher Vorschlag ist ein gangbarer Weg für einen intensiveren Dialog der Höchstgerichte. An dem Umstand, dass letztlich doch der – womöglich auf diese Art weiter verfeinerte – Schutzstandard der EU-Grundrechte zählt, ändert er aber nichts. Will man die Anwendung nationaler Grundrechte in Dreiecksituationen nicht aufgeben, bedarf es darum eines Ansatzes, wie nationalen Grundrechte und die EU-Grundrechte auf der Ebene des materiellen Rechts voneinander abzugrenzen. Genau dies war lange ungeklärt.

---

894 *Masing,* JZ 2015, S. 477, 485 f.; so aber bei *Albrecht/Janson,* CR 2016, S. 500, 505 f.; *Pötters,* in: Gola 2018, Art. 88 DS-GVO, Rn. 52.

895 Mit dieser Unterscheidung ebenfalls *Bäcker,* EuR 2015, S. 389, 404.

896 Zusammenfassend *Buchholtz,* DÖV 2017, S. 837, 841 ff.

897 BVerfG v. 6.11.2019 – 1 BvR 16/13, E 152, S. 152–215, Rn. 72 – *Recht auf Vergessen I*.

898 *Bäcker,* EuR 2015, S. 389, 404 ff.; *Buchholtz,* DÖV 2017, S. 837, 844 f.; *Thym,* JZ 2015, S. 53, 59 ff.; in die Richtung auch *Kingreen,* JZ 2013, S. 809 f.

3.2.2.3.3 Materiellrechtlicher Abgrenzungsversuch bei Grundrechtskollisionen

Für einen Abgrenzungsversuch muss man sich zunächst vor Augen halten, dass der Schauplatz eines Konflikts zwischen der nationalen und der europarechtlichen Grundrechtsauslegung in der Regel das Verhältnismäßigkeitsprinzip sein wird. Es ist zwar denkbar, dass in einigen Punkten der Umfang des Schutzbereichs oder die Qualifikation einer Maßnahme als Eingriff unterschiedlich ausgelegt wird. Das zentrale Element bei der Entscheidung über eine Grundrechtskollision ist aber das Verhältnismäßigkeitsprinzip, weil es eben das Verhältnis – oder anders ausgedrückt die Balance – zwischen den Rechtspositionen der beteiligten Privaten bestimmt. Dies wiederum gibt in der Regel den Ausschlag dafür, ob eine bestimmte Maßnahme des einen – im Beschäftigungsverhältnis meist es Arbeitgebers – zulässigerweise vorgenommen werden darf oder als rechtswidrig zu unterbleiben hat, weil sie die Rechte des anderen – des Arbeitnehmers – verletzt. 635

3.2.2.3.3.1 Begrenzter Vorrang des mitgliedstaatlichen Rechts

Sich bei der Abgrenzung auf ein Kriterium festzulegen, bedeutet, dass sich die unterschiedlichen Grundrechtsverständnisse nicht ausweichen können, ein Konflikt also nicht aufgelöst werden kann, sondern entschieden werden muss. Darum gilt zu bestimmen, wer von beiden zuerst auszuweichen hat. Dafür, dass dies das EU-Grundrechtsverständnis sein muss, sprechen zwei Erwägungen: 636

Erstens liegt angesichts des Subsidiaritätsprinzips des Unionsrechts nach Art. 5 Abs. 3 EUV der Schluss nahe, dass sich der EU-Gesetzgeber in den Regelungsbereichen, in denen er Öffnungsklauseln schafft, gerade deswegen zurückhält, weil sie in besonderem Maße von zwischen den Mitgliedstaaten divergierenden Vorstellungen geprägt sind. Diese Vorstellungen können die Mitgliedstaaten in von Dreiecksverhältnissen geprägten Bereichen aber nur einbringen, wenn sich auch das Verhältnis der betroffenen Grundrechte zueinander nach dem nationalen Grundrechtsverständnis bestimmt.[899] 637

899 BVerfG v. 6.11.2019 – 1 BvR 16/13, E 152, S. 152–215, Rn. 47 ff. – *Recht auf Vergessen I*.

638 Zweitens enthalten viele Öffnungsklauseln – im Fall des hier relevanten Beschäftigtendatenschutzes auch die in Art. 88 DS-GVO – Anforderungen an den mitgliedstaatlichen Gesetzgeber. Zumindest in den Fällen, in denen die Union den Mitgliedstaaten aber kein Blankett ausstellt, spricht einiges für eine gewisse Letztverbindlichkeit des Unionsrechts, die dann auch für zentrale Bereiche wie das Verhältnismäßigkeitsprinzip gilt. Das bedeutet aber auch, dass zunächst, d.h. innerhalb des Entscheidungsspielraums, welchen diese Anforderungen den Mitgliedstaaten belassen, das mitgliedstaatliche Recht Vorrang hat.

3.2.2.3.3.2 Der Wesensgehalt der EU-Grundrechte als Grenze

639 Nach diesem Lösungsansatz würde eine Grundrechtskollision im Bereich einer Öffnungsklausel zuerst nach den Maßstäben des jeweiligen nationalen Grundrechtsverständnisses gelöst. Das europäische Grundrechtsverständnis käme erst zum Tragen, wenn andernfalls der – nach Unionsrecht zu bestimmende – Schutzstandard des eingeschränkten Grundrechts verletzt würde.

640 Diese materielle Grenze ist nach der Rechtsprechung des Bundesverfassungsgerichts erreicht, wenn entweder das unionsrechtliche Fachrecht engere grundrechtliche Maßstäbe vorgibt oder der Europäische Gerichtshofs die Grundrechte der Charta so auslegt, dass sie keine Entsprechung im Grundgesetz haben.[900]

641 Insofern bietet es sich an, den Schutzstandard der EU-Grundrechte auf ihren Wesensgehalt zu reduzieren. Das deckt sich zum einen mit dem zum verfahrensrechtlichen Abgrenzungsansatz (siehe 3.2.2.3.2, S. 274) geäußerten Befund, wonach die europäische Grundrechtsdogmatik teilweise nur in Grundzügen entwickelt ist. Zum anderen können zur Konkretisierung dieser Grenze speziell für die Datenschutz-Grundverordnung die Grundsätze der Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO (dazu näher unter 3.4.1, S. 354) herangezogen werden. Sie sind das sekundärrechtliche Abbild des primärrechtlichen Wesensgehalts des Rechts auf Schutz personenbezogener Daten (zu diesem Grundrecht näher unter 3.2.3, S. 284) und bilden darum die Grenze der mitgliedstaatlichen Abwei-

900 BVerfG v. 6.11.2019 – 1 BvR 16/13, E 152, S. 152–215, Rn. 68 f. – *Recht auf Vergessen I*.

chungsbefugnis. Die Mitgliedstaaten dürfen diese Grundsätze nur konkretisieren, nicht aber von ihnen abweichen (siehe 3.1.3.1, S. 243).

Einen Wesensgehaltverstoß wird man nur ganz ausnahmsweise annehmen können. Im Bereich des hier relevanten Beschäftigtendatenschutzes wäre dies erst der Fall, wenn eine nach dem nationalen Grundrechtsverständnis ausgelegte mitgliedstaatliche Regelung die Prinzipien des europäischen Datenschutzes in Art. 5 DS-GVO konterkarieren würde. Hier kommt besonders zum Tragen, dass die Mitgliedsstaaten[901] und die Sozialpartner[902] gerade bei Maßnahmen der Arbeits- und Sozialpolitik einen weiten Ermessenspielraum genießen, der erst überschritten ist, wenn sie unvernünftig handeln. Dies gilt auch für Fragen der Verhältnismäßigkeit.[903] 642

3.2.2.3.3.3 Notwendige Nutzung der Öffnungsklausel

Der hier aufgezeichnete Abgrenzungsvorschlag räumt den nationalen Vorstellungen innerhalb der Öffnungsklauseln vergleichsweise breiten Raum ein. Das ist aber nur gerechtfertigt, wenn die Mitgliedstaaten die Öffnungsklauseln auch nutzen, um ihre Vorstellungen hinreichend bestimmt auszudrücken. 643

Eine wesentliche Frage für die Anwendbarkeit welcher Grundrechte ist folglich nicht nur, ob eine Öffnungsklausel besteht, sondern ob sie auch ordnungsgemäß ausgefüllt wurde. Ob nun das nationale oder das europäische Grundrechtsverständnis gilt, kann darum von Mitgliedstaat zu Mitgliedstaat variieren. Der deutsche Gesetzgeber hat die Öffnungsklausel jedenfalls nur teilweise genutzt (siehe 3.1.5, S. 246). 644

901 EuGH, ECLI:EU:C:2007:604, Rn. 68 ff. – *Palacios de la Villa*; EuGH, ECLI:EU:C:2010:601, Rn. 41, 51 – *Rosenbladt*.

902 EuGH, ECLI:EU:C:2010:601, Rn. 69 – *Rosenbladt*.

903 Das Bundesverfassungsgericht hebt auf diese Rechtsprechung im Hinblick auf das allgemeine Verhältnis der Grundrechtsebenen ab, BVerfG v. 6.11.2019 – 1 BvR 16/13, E 152, S. 152–215, Rn. 52 – *Recht auf Vergessen I*. Im Beschäftigtendatenschutz muss dies umso mehr gelten.

3.2.2.4 Zwischenergebnis zum anwendbaren Recht im Beschäftigtendatenschutz

645 Für die hier relevanten Bereiche der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO ergeben sich je nach Regelungsbereich unterschiedlichen Folgen.

646 Mit der Regelung zur Einwilligung in § 26 Abs. 2 BDSG 2018 hat der Gesetzgeber den Anforderungen nach Art. 88 Abs. 1 und 2 DS-GVO Genüge getan. Innerhalb ihres Anwendungsbereichs gelten damit vorrangig die deutschen Grundrechte.[904] Dies führt zu der auf den ersten Blick gewöhnungsbedürftigen, in der Konzeption von Öffnungsklauseln aber so angelegten Situation, dass die Freiwilligkeit der Einigung grundsätzlich am Maßstab der EU-Grundrechte zu prüfen ist, für einzelne Aspekte aber der Maßstab der Grundrechte des Grundgesetzes zugrunde zu legen ist. Dies sind die in § 26 Abs. 2 BDSG 2018 erwähnte Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist.

647 Mit der Regelung in § 26 Abs. 1 S. 1 Var. 1 bis 3 BDSG 2018 hat der deutsche Gesetzgeber allerdings gegen die Anforderungen in Art. 88 Abs. 1 und 2 DS-GVO verstoßen. Die Datenverarbeitung zur Erfüllung eines Vertrags ist darum allein auf Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO zu stützen und prinzipiell unter Anwendung der EU-Grundrechte zu bewerten.

648 Die Regelung zur Datenverarbeitung auf der Grundlage von Kollektivvereinbarungen in § 26 Abs. 4 BDSG 2018 ist schließlich rein deklaratorischer Natur. Die Regelungsmacht der Parteien einer Kollektivvereinbarung ergibt sich bereits unmittelbar aus Art. 88 Abs. 1 DS-GVO und den deutschen Regelungen, die Tarifverträgen und Betriebsvereinbarungen normative Wirkung verleihen. Ob eine Kollektivvereinbarung die Anforderungen in Art. 88 Abs. 1 und 2 DS-GVO einhält, und welche Grundrechte für die darauf gestützte Datenverarbeitung also gelten, ist stets für die einzelne Vereinbarung zu ermitteln.

3.2.2.5 Die Anwendung nationaler Grundrechte im Hinblick auf die arbeitsrechtlichen Grundlagen des Beschäftigungsverhältnisses

649 Bei der Frage, ob eine konkrete Datenverarbeitung im Kontext eines Arbeitsverhältnisses zulässig ist, spielen mehr Aspekte eine Rolle als nur die

904 So i.E. auch *Däubler*, in: Däubler et al. 2020, Art. 88 DS-GVO, Rn. 13.

Erwägungen, die allein dem Beschäftigtendatenschutz zugeordnet sind. Oft sind arbeitsrechtliche Fragen über den genauen Inhalt des zu erfüllenden Arbeitsverhältnisses relevant. Der Umstand, dass § 26 Abs. 1 S. 1 Fall 1 bis 3 BDSG 2018 wegen Verstoßes gegen zwingendes Unionsrecht in Art. 88 Abs. 1 und 2 DS-GVO nicht anwendbar ist, darf jedoch nicht zu der Annahme verleiten, dass sämtliche Fragen, die im weiteren Sinne mit dem Beschäftigtendatenschutz zusammenhängen ausschließlich unter der Anwendung von EU-Grundrechten zu beurteilen sind.

Dies ergibt sich schon daraus, dass Kollektivvereinbarungen weiterhin die Öffnungsklausel in Art. 88 Abs. 1 DS-GVO nutzen können. Soweit sie dies tun, finden vorrangig die Grundrechte des Grundgesetzes Anwendung. Gleiches gilt für die Rechte und Pflichten der Interessenvertretung und für die Beurteilung der Freiwilligkeit einer Einwilligung; hier hat der deutsche Gesetzgeber die Anforderungen in Art. 88 DS-GVO erfüllt. 650

Aber auch bei der Anwendung der Generalklauseln in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO kommen nicht ausschließlich die EU-Grundrechte zum Tragen. Dies lässt sich dem Regelungskonzept der Datenschutz-Grundverordnung und der Kompetenzverteilung zwischen der Union und den Mitgliedstaaten entnehmen. 651

3.2.2.5.1 Kompetenzverteilung und Regelungskonzept im Datenschutzrecht

Die Datenschutz-Grundverordnung verfolgt gemäß Art. 2 DS-GVO einen umfassenden Ansatz, der zwar in Absatz 2 einige Bereiche ausnimmt – insbesondere den der öffentlichen Sicherheit –, im Umkehrschluss zu Absatz 2 Buchstabe b aber im Grunde den kompletten Anwendungsbereich des Unionsrechts abdeckt. Damit regelt die Verordnung eine unüberschaubare Fülle von Lebenssachverhalten,[905] was ihr nur gelingt, weil sie sich hinsichtlich der materiellen Zulässigkeit auf wenige Grundsätze beschränkt. Das Bindeglied zu den speziellen Regeln über den jeweiligen Lebenssachverhalt bildet das Prinzip der Erforderlichkeit, das in den Grundsätzen der Zweckbegrenzung, Datenminimierung und Speicherbegrenzung nach Art. 5 Abs. 1 lit. b, c und e DS-GVO zum Ausdruck kommt (siehe 3.4.1, S. 354). 652

905 *Grimm*, JZ 2013, S. 585, 591.

653 Diese Datenschutzgrundsätze werfen im Einzelnen komplexe Fragen auf. An dieser Stelle ist jedoch nur wesentlich, dass jede Erforderlichkeitsprüfung mit Blick auf einen bereits bestimmten Zweck vorgenommen werden muss. Die Legitimität dieses Zwecks – die sich unter anderem nach grundrechtlichen Maßstäben (hier vermittelt durch die Drittwirkung im Beschäftigungsverhältnis) bemisst – ist damit in einem weiteren Sinne Teil der datenschutzrechtlichen Prüfung. Das Datenschutzrecht selbst – einschließlich der neuen Datenschutz-Grundverordnung – enthält jedoch keine eigenen Maßstäbe für die Legitimitätsprüfung, sondern nimmt legitime Zwecke (z.B. aus anderen Rechtsgebieten) in Bezug. Nach diesem Regelungskonzept ist es keine Frage des Datenschutzrechts, welcher Zweck legitim oder wie er inhaltlich genau zu bestimmen ist. Dies ist nach den Vorschriften zu bestimmen, die den jeweils einschlägigen Lebensbereich regeln (dazu auch 3.4.1.4.1, S. 389).[906] Die Zulässigkeit der Datenverarbeitung kann folglich nicht autonom datenschutzrechtlich bestimmt werden.[907] Entsprechend kann auch die Grundrechtsabwägung nicht autonom dem Unionsrecht entnommen werden, wenn der jeweilige Lebensbereich nicht ebenfalls europarechtlich determiniert ist.

654 Für den Beschäftigtendatenschutz ist der maßgebliche Anknüpfungspunkt der Erforderlichkeitsprüfung gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO die arbeitsvertragliche Pflicht, zu deren Erfüllung u.U. personenbezogene Daten verarbeitet werden müssen. Ob sie legitim ist und worin sie genau besteht, ist eine Frage des Arbeitsrechts. Das ist zwar ebenfalls in wesentlichen Teilen europarechtlich determiniert, etwa im Bereich des Arbeitszeitrechts[908] oder der Gleichbehandlung[909]; gemäß Art. 153 i.V.m. Art. 114 Abs. 2 AEUV besteht jedoch keine allgemeine Kompetenz der Union im Arbeitsrecht. Der Beschäftigtendatenschutz wird lediglich als Annexkompetenz von Art. 16 Abs. 2 AEUV erfasst (siehe 3.1.2, S. 241).

906 In die Richtung kann man auch *Maschmann,* in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 39 verstehen, der betont, dass die DS-GVO in erster Linie keinen Ausgleich zwischen dem Arbeitnehmer- und dem Arbeitgeberinteresse bezwecke, sondern sich als Querschnittsregelung nur auf das Arbeitsrecht auswirkt.

907 So auch allgemein zu Erlaubnistatbeständen, die an eine vertragliche Bindung anknüpfen *Martini,* in: Paal/Pauly 2018, Art. 22 DS-GVO, Rn. 31.

908 Richtlinie 2003/88/EG über bestimmte Aspekte der Arbeitszeitgestaltung.

909 Richtlinie 2000/78/EG zur Festlegung eines allgemeinen Rahmens für die Verwirklichung der Gleichbehandlung in Beschäftigung und Beruf.

3.2.2.5.2 Folgerungen für die Anwendbarkeit der Grundrechte

Die beschriebene Kompetenzverteilung legt es nahe, dass sowohl nationale als auch unionale Grundrechte in der datenschutzrechtlichen Prüfung eine Rolle spielen werden. Indessen kann man hier nicht unbesehen dem oben für Öffnungsklauseln diskutierten Vorschlag für die Abgrenzung der Grundrechtsebenen (siehe 3.2.2.2, S. 265) folgen. Öffnungsklauseln werden vom europäischen Gesetzgeber ausnahmsweise verwendet, wenn in dem betreffenden Bereich nationale Vorstellungen und Wertungen in der ganzen Breite des Prüfungsaufbaus eingehen sollen. Dass der jeweils von der Datenschutz-Grundverordnung erfasste Lebenssachverhalt nicht oder nur punktuell europarechtliche determiniert ist, ist dagegen angesichts des weitgreifenden Regelungsansatzes der Verordnung der Normalfall. Es würde dem Grundgedanken eines europaweit einheitlichen und überdies unmittelbar anwendbaren Datenschutzrechts nicht gerecht, wenn die unionalen Grundrechte hier wie bei Öffnungsklauseln nur als rahmenmäßiger Schutz im Sinne einer Wesensgehaltsgarantie verstanden würden. 655

Für die Abschichtung der Grundrechtsebenen außerhalb der Öffnungsklauseln – und für Fälle des § 26 Abs. 1 S. 1 BDSG 2018, in denen die Öffnungsklausel nicht ordnungsgemäß ausgefüllt wurde – muss folglich ein anderer Ansatz entwickelt werden, der sich am Regelungskonzept des Datenschutzes und der Kompetenzverteilung in dem jeweiligen Bereich orientiert. Speziell für das Arbeitsrecht, im Grunde aber auch für alle anderen Bereiche, bietet sich eine horizontale Aufteilung in zwei Bereiche an: die Bestimmung des Verarbeitungszwecks auf der einen und die Prüfung, welche Datenverarbeitung für diesen Zweck erforderlich und angemessen ist, auf der anderen Seite. 656

Der erste Teil ist nach Wertungen des mitgliedstaatlichen Arbeitsrechts vorzunehmen und betrifft – zumindest im hier relevanten Bereich des Umgangs mit Assistenzsystemen – die Kernfrage im Beschäftigungsverhältnis, welche Tätigkeit der Arbeitgeber anordnen darf. Der zweite Teil ist nach den Wertungen des europäischen Datenschutzrechts vorzunehmen und betrifft die Frage, inwieweit das Persönlichkeitsrecht des Beschäftigten wirtschaftlichen Interessen weichen muss. Das Datenschutzrecht stellt zwar auch selbst Anforderungen an den Zweck (siehe 3.4.1.2, S. 355). Sie betreffen aber – als notwendiger Vorlauf des Erforderlichkeitsprinzips – nur die Konkretisierung des Zwecks im Sinne eines notwendigen Mindestmaßes an Bestimmtheit. Die Legitimität des Zwecks und nach welchen Maßstäben der Zweck zu konkretisieren ist, gehört dagegen nicht zu den 657

datenschutzrechtlichen Anforderungen. Für die hier vorzunehmende Abschichtung der Grundrechtsebenen ist allein letztere relevant.

658 Die Möglichkeit zur sauberen Trennung ergibt sich bereits aus dem Aufbau der Prüfung, in der die arbeitsrechtliche Zulässigkeit des Verarbeitungszwecks eine Art Vorfilter für die eigentliche datenschutzrechtliche Prüfung darstellt (siehe 3.6.1.2.1.2, S. 493). Zum anderen können auch die Interessen der Beschäftigten untereinander abgeschichtet werden. Soweit es um die Frage geht, welche Konsequenzen eine Datenverarbeitung für das Arbeitsverhältnis selbst hat, ob es etwa deswegen beendet oder inhaltlich wesentlich verändert werden kann, ist dies eine Frage des Arbeitsrechts. Hier stehen sich allein die Wirtschaftsgrundrechte der Beteiligten gegenüber, deren Abwägung das Datenschutzrecht nur am Rande regelt. Die Abwägung ist hier anhand des mitgliedstaatlichen Grundrechtsstandards vorzunehmen. Die Problemkreise, ob eine Datenverarbeitung einen unzulässigen Beobachtungsdruck, ein Gefühl des Ausgeliefertseins oder eine übermäßige Fremdbestimmung nach sich zieht, sind dagegen klassische Fragen des Datenschutzrechts, da sie Aspekte des dort geregelten Persönlichkeitsrechtsschutzes betreffen. Hier ist der europäische Grundrechtsstandard anzulegen.

659 Auch eine solche horizontale – weil bei verschiedenen Punkten des Prüfungsablaufs angesiedelte – Trennung der Bereiche kann bei mehrpoligen Grundrechtsverhältnissen Probleme bereiten. Die Grundrechtsebenen stehen zwar in keiner Hierarchie zueinander, infolge des Prüfungsaufbaus kommt dem Datenschutzrecht aber eine gewisse Letztentscheidungskompetenz zu. Anders ausgedrückt: Es nützt dem Arbeitgeber wenig, dass die vom ihm angestrebte Arbeitsorganisation nach nationaler Grundrechtsbetrachtung als zulässig und in der Folge von seinem Weisungsrecht nach § 106 GewO gedeckt ist, wenn der damit verbundene Eingriff in das europäische Recht des Arbeitnehmers auf Schutz personenbezogener Daten trotzdem als zu hoch eingestuft wird.

660 Diese Letztentscheidungskompetenz ist aber nur die logische Folge eines einheitlichen europäischen Datenschutzrechts. Da die entscheidende Interessenabwägung europarechtlich determiniert ist, muss hier auch die europäische Auslegung des Rechts auf Schutz personenbezogener Daten vorrangig sein. Etwaige Auswirkungen auf die Durchsetzungsfähigkeit entgegenstehender und durch nationale Grundrechte geschützter Interessen sind dem Regelungskonzept des Datenschutzrechts immanent und hinzunehmen. Die Wirkung dieses Vorrangs dürfte aber begrenzt sein. Die datenschutzrechtliche Interessenabwägung kennt nur wenige Tabuzonen, in denen die nationalen Grundrechtsvorstellungen für das Ergebnis praktisch

keine Rolle spielen würden (speziell für den Beschäftigtendatenschutz siehe 3.6.1.2.3, S. 508). Die in dem betreffenden Lebenssachverhalt vorherrschenden Wertungen hinsichtlich der Legitimität der beteiligten Interessen dürften darum in der Regel relevant sein. Insofern hat die beschriebene horizontale Abgrenzung gerade im Arbeitsverhältnis und anderen Konstellationen, in denen der Verantwortliche und der Betroffene komplexe (vertraglichen) Beziehungen zueinander pflegen, ihre Bedeutung. Hier kommt es zu einem „Dialog" der Grundrechtsebenen.

In zulässigerweise ausgefüllten Öffnungsklauseln, also z.B. bei Kollektivvereinbarungen, die den Anforderungen in Art. 82 Abs. 1 und 2 DS-GVO entsprechen, bestehen dagegen viel weniger Abgrenzungsprobleme. Dort gilt es nach dem oben skizzierten materiellen Abgrenzungsversuch (siehe 3.2.2.3.3, S. 275) nur den Wesensgehalt der unionalen Grundrechte zu wahren. Ansonsten kommen sowohl bei der – außerhalb des Datenschutzrechts stattfindenden – Zweckbestimmung als auch bei den – innerhalb des infolge der Öffnungsklausel national geregelten – übrigen Prüfungsschritten ausschließlich nationale Grundrechte zur Anwendung. 661

3.2.2.6 Zusammenfassung zur Anwendbarkeit der Grundrechte

Für die Anwendbarkeit unionaler und mitgliedstaatlicher Grundrechte im Datenschutzrecht ergibt sich nach der hier vertretenen Meinung ein differenziertes Bild: 662

Innerhalb der von einem Mitgliedstaat zulässigerweise ausgefüllten Öffnungsklauseln kommen unionale und nationale Grundrechte grundsätzlich nebeneinander zur Anwendung (siehe 3.2.2.2, S. 265). Eine Ausnahme gilt jedoch für Situationen, in denen es zu Grundrechtskollisionen kommt, in denen also – wie im Arbeitsverhältnis – die grundrechtlich geschützten Interessen mehrerer grundrechtsberechtigter Subjekte aufeinandertreffen. Dann gelten in erster Linie nur die nationalen Grundrechte; die unionalen Grundrechte bilden lediglich den Rahmen, in dem die Grundrechtskollision vorrangig nach den Maßstäben des mitgliedstaatlichen Rechts entschieden werden. Dieser EU-Grundrechtsrahmen ist aber erst dann berührt, wenn der – nach Unionsrecht zu bestimmende – Wesensgehalt der Grundrechte verletzt wird (siehe 3.2.2.3.3, S. 275) 663

Außerhalb der Öffnungsklauseln und in den Fällen, in denen die Öffnungsklauseln von den Mitgliedstaaten nicht zulässigerweise ausgefüllt wurden, genießen die EU-Grundrechte grundsätzlich Vorrang. Die mitgliedstaatlichen Grundrechte kommen nur dann zum Tragen, wenn das 664

Datenschutzrecht mit seinen Wertungen an Regelungsbereiche anknüpft, diese aber selbst nicht regelt. Das ist beim Erlaubnistatbestand für die Datenverarbeitung zur Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO der Fall. Für die Bestimmung der arbeitsvertraglichen Pflicht, die den Zweck der Datenverarbeitung bildet, ist hier auf die Regelungen des mitgliedstaatlichen – für diese Arbeit also des deutschen – Arbeitsrechts abzustellen. Die übrige Prüfung erfolgt nach den Maßstäben der unionalen Grundrechte (siehe 3.2.2.5.2, S. 281).

665 Im Beschäftigtendatenschutz kommen in den für diese Arbeit besonders relevanten Konstellationen beide Modelle für das Verhältnis der unionalen und nationalen Grundrechte zum Tragen. Dies liegt daran, dass der deutsche Gesetzgeber die Öffnungsklausel für den Beschäftigtendatenschutz zumindest mit der Regelung des § 26 Abs. 1 S. 1 BDSG 2018 nicht entsprechend der Anforderungen nach Art. 88 Abs. 1 und 2 DS-GVO ausgefüllt hat (siehe 3.1.5.2.5, S. 255). Die Datenverarbeitung seitens des Arbeitgebers, die sich auf arbeitsvertragliche Pflichten stützt, ist folglich nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO und – abhängig von den Prüfungsschritten – nach nationalen und unionalen Grundrechten zu prüfen. Bei der Datenverarbeitung aufgrund von Kollektivvereinbarungen kommen – vorausgesetzt die Vereinbarungen beachten die Vorgaben in Art. 88 Abs. 1 und 2 DS GVO – nur deutsche Grundrechte zur Anwendung.

666 Eine gänzlich eigenständige Kategorie bilden schließlich die Konstellationen, in denen der mitgliedstaatliche Gesetzgeber den Anwendungsbereich der nationalen Regelung über den der Datenschutz-Grundverordnung hinaus ausgedehnt hat. Im deutschen Beschäftigtendatenschutz ist dies mit Art. 26 Abs. 7 BDSG 2018 geschehen (siehe 3.1.6, S. 255). Da hier nach Art. 51 Abs. 1 S. 1 GRC kein Unionsrecht durchgeführt wird und die EU-Grundrechte folglich nicht anwendbar sind, gelten allein die nationalen Grundrechte, ohne dass es einer Abgrenzung bedürfte.

3.2.3 Das Recht der Beschäftigten auf Schutz personenbezogener Daten

667 Auf Seiten des Beschäftigten kommen im Bereich des Persönlichkeitsschutzes ausschließlich die EU-Grundrechte zur Anwendung. Speziell persönlichkeitsschützend wirken hier das Recht auf Achtung des Privat- und Familienlebens nach Art. 7 GRC i.V.m. Art. 8 EMRK sowie das Recht auf Schutz personenbezogener Daten nach Art. 8 GRC und Art. 16 AEUV. Sie bilden die Grundlage des sekundärrechtlichen Datenschutzrechts. Darüber hinaus enthält gerade Art. 7 GRC noch weitere Gewährleistungen, die das

Thema dieser Arbeit aber nur streifen und auf die darum nur kurz eingegangen werden soll. Auch finden sich Aspekte des Persönlichkeitsschutzes im Grundrecht der Berufsfreiheit nach Art. 15 GRC; wie im nationalen Rahmen auch sind die Grundrechte aus Art. 7 und 8 GRC hier aber spezieller.

668 Die wirtschaftlichen Interessen der Beschäftigten werden in den hier relevanten Fällen ausschließlich durch die nationalen Grundrechte geregelt. Die Ausweitung des sekundärrechtlichen Datenschutzes in den Beschäftigungskontext führt nicht dazu, dass die damit verbundenen Aspekte des Arbeitsrechts ausschließlich oder auch nur kumulativ auf der Basis der unionalen Grundrechte zu betrachten wären (siehe 3.2.2.5.2, S. 281). Hier kann folglich auf Gliederungspunkt 2.2.2 (S. 82) verwiesen werden.

3.2.3.1 Grundrechtskonstellationen ohne speziellen Bezug zu Assistenzsystemen

669 Das Grundrecht auf Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation – so die vollständige Umschreibung des Schutzbereichs in Art. 7 GRC – enthält noch weitere Gewährleistungen, die im Beschäftigungsverhältnis eine Rolle spielen können. Das gilt allen voran für den ausdrücklich erwähnten Schutz der Kommunikation. Es ließe sich aber auch darüber nachdenken, ob das sog. IT-Grundrecht, das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, welches das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht abgeleitet hat,[910] auch im Kontext der EU-Grundrechte zum Tragen kommen könnte. Diese Ausprägungen des Art. 7 GRC betreffen aber keine Besonderheiten der Industrie 4.0,[911] sondern lediglich Aspekte des Einsatzes von Informationstechnologie am Arbeitsplatz, die hier nicht im Fokus stehen sollen.

670 Der Schutz der Kommunikation betrifft im Beschäftigungskontext vor allem die Überwachung der – dienstlich oder auch privat genutzten – betrieblichen Kommunikationsinfrastruktur, sei es per Telefon, E-Mail oder Messenger. Im Zuge der Entwicklung der Industrie 4.0 kann auch die Kommunikation unter den Mitarbeitern verbessert und intensiviert wer-

910 BVerfG v. 27.2.2008 – 1 BvR 370, 595/07, E 120, S. 274–350 – *Online-Durchsuchungen*.

911 Vgl. zu Sensorik in Schutzanzügen *Roßnagel, et al.* 2012, S. 38 ff.

den. Im Fokus dieser Untersuchung sollen aber Assistenzsysteme stehen, die dem Beschäftigten Informationen anzeigen, seinen Einsatz planen oder ihn bei der körperlichen Arbeit entlasten (siehe 1.3.2, S. 71). Die hierfür notwendigen Daten stammen aus dem Produktionsprozess und ggf. auch aus dem Arbeitsverhalten des Beschäftigten, nicht aber aus seiner Kommunikation. Sollte aber dennoch auf Kommunikationsumstände oder -inhalte zurückgegriffen werden, ergeben sich aus dem Umstand, dass dies im Kontext der Industrie 4.0 erfolgt, keine Besonderheiten. Diesbezüglich kann auf die umfangreiche Literatur, die allein speziell zu dem Thema erschienen ist, verwiesen werden.[912]

671 Für das IT-Grundrecht stellt sich die Situation ähnlich dar. Das Recht schützt zwar auch geschäftlich genutzte IT-Systeme und kommt darum zumindest für solche Assistenzsysteme in Betracht, die dem Beschäftigten persönlich zugeordnet sind.[913] Bedingt durch seinen Entstehungskontext steht dieses Grundrecht aber in einem sehr engen Verhältnis zur Telekommunikationsüberwachung, soll also dagegen schützen, dass das System kompromittiert wird. Das ist bei Assistenzsystemen sicherlich möglich; der Arbeitgeber kann sie dazu einsetzen, seine Beschäftigten zu überwachen. Dies ist aber wiederum keine Besonderheit der Industrie 4.0.

3.2.3.2 Das Verhältnis der einzelnen Grundrechte im Datenschutz

672 Das Verhältnis der einschlägigen Grundrechte aus Art. 8 EMRK, Art. 7 und 8 GRC und Art. 16 AEUV ist teilweise ungeklärt. Dies ist in erster Linie auf die historische Entwicklung dieser Grundrechte im europäischen Kontext zurückzuführen, wohl aber auch darauf, dass die Abgrenzung keine ersichtliche praktische Relevanz hat.

3.2.3.2.1 Die Rolle der Europäischen Menschenrechtskonvention

673 Der Schutz personenbezogener Daten auf europäischer Ebene bestand bereits vor der Kodifizierung der Grundrechtecharta. Er wurde vom Europäischen Gerichtshof zu den allgemeinen Prinzipien des Unionsrechts ge-

912 Siehe z.B. *Baier* 2010; *Block* 2012; *Elschner* 2004; *Hoppe* 2010; *Koeppen* 2007; *Mattl* 2008; *Meyer-Michaelis* 2014; *Mölter* 2012; *Neu* 2014; *Schmitz* 2016.

913 Siehe allgemein zu IT-Arbeitsmitteln *Schmitz* 2016, S. 62 f.

zählt, wofür er sich maßgeblich an Art. 8 EMRK orientierte.[914] Daran hat sich auch mit der Kodifizierung der Charta nichts geändert, da der Europäische Gerichtshof nun darauf abhebt, dass die Konvention gemäß Art. 52 Abs. 3, 53 GRC die Auslegung der Charta im Sinne eines Mindestschutzes bestimme.[915]

674 Die Konvention enthält kein eigenständiges Recht auf Schutz personenbezogener Daten, sondern in Art. 8 EMRK lediglich ein „klassisches" Recht auf Achtung des Privat- und Familienlebens. Ähnlich wie das Bundesverfassungsgericht, welches das Recht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht entwickelte,[916] hat der Europäische Gerichtshof für Menschenrechte den Schutzbereich von Art. 8 EMRK über den inneren Bereich der Persönlichkeit bzw. des Privatlebens ausgeweitet. Er erfasst demnach jedenfalls auch Informationen, die das Berufsleben betreffen.[917] Über die Transfernorm des Art. 52 Abs. 3 GRC wirkt diese Ausweitung des Schutzbereichs auch für die Charta-Grundrechte.

675 Gemäß Art. 52 Abs. 3 GRC haben diejenigen Rechte in der Charta, die denen in der Europäischen Menschenrechtskonvention entsprechen, auch deren Bedeutung und Tragweite. Dass die beiden Rechte in Art. 7 GRC und Art. 8 Abs. 1 EMRK identisch sind, ergibt sich bereits aus dem beinahe vollständig übereinstimmenden Wortlaut der Normen. Es lässt sich aber auch der Liste in den Erläuterungen zu Art. 52 GRC entnehmen, in der alle Rechte aufgezählt sind, die nach Meinung des Präsidiums des Europäischen Konvents identisch sind. Der Schutz personenbezogener Daten ließe sich folglich nach Art. 52 Abs. 3 GRC i.V.m. Art. 8 Abs. 1 EMRK auch allein über Art. 7 GRC konstruieren.[918]

914 EuGH, ECLI:EU:C:2003:294, Rn. 68 ff. – *ORF*.
915 EuGH, ECLI:EU:C:2010:662, Rn. 51 f. – *Schecke*.
916 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 42 ff. – *Volkszählung*.
917 EGMR v. 16.12.1992 – 13710/88, Rn. 29 – *Niemietz/Deutschland*; EGMR v. 16.2.2000 – 27798/95, Rn. 65 – *Amann/Schweiz*; EGMR v. 3.4.2007 – 62617/00, MMR 2007, S. 431, Rn. 41 f. – *Copland/Vereinigtes Königreich*; EGMR v. 5.9.2017 – 61496/08, ZD 2017, S. 571, Rn. 73 f. – *Barbulescu v. Romania*; EGMR v. 22.2.2018 – 588/13, ZD 2018, S. 263, 264 – *Libert/France*; daran anknüpfend EuGH, ECLI:EU:C:2003:294, Rn. 73 – *ORF*.
918 *Schiedermair,* in: Simitis et al. 2019, Einleitung, Rn. 168.

3.2.3.2.2 Dopplungen nach aktueller Rechtslage

676 Mit Art. 8 GRC wurde ein Grundrecht eingeführt, das ausweislich seines Wortlauts spezieller ist als dasjenige in Art. 7 GRC.[919] Der Europäische Gerichtshof wendet in datenschutzrechtlichen Fragen dennoch beide Grundrechte gemeinsam an und hat auch bisher keine ernsthaften Versuche unternommen, die Schutzbereiche von Art. 7 und 8 GRC gegeneinander abzugrenzen, sondern im Gegenteil stets deren engen Zusammenhang betont.[920] In der Literatur mangelt es nicht an Ansätzen, wie die Abgrenzung der beiden Grundrechte vorzunehmen ist.[921] Ihnen ist aber auch gemein, dass sie nicht erkennen lassen, wie sich die Abgrenzung auf das – im Rahmen dieser Arbeit vornehmlich relevante – Ergebnis der Grundrechtsprüfung auswirkt.

677 Am plausibelsten scheint es, die Ausweitung des Schutzbereichs des Rechts auf Achtung des Privat- und Familienlebens in Art. 7 GRC als der engen Bindung an Art. 8 EMRK geschuldetes rechtshistorisches Relikt zu betrachten. Es würde wohl nicht gegen Art. 52 Abs. 3, 53 GRC verstoßen, die in Art. 8 EMRK enthaltenen Grundsätze zum Datenschutz allein auf das Grundrecht in Art. 8 GRC zu beziehen.[922] Der Schutzbereich des Rechts auf Achtung des Privat- und Familienlebens würde so gewissermaßen auf zwei neue Grundrechte in der Charta verteilt.

678 Es gibt folglich keinen Grund, den Anwendungsbereich des Art. 7 GRC weiterhin über seinen Wortlaut hinaus auf sämtliche personenbezogene Daten auszuweiten. Für personenbezogene Informationen aus dem Privatleben ist die Norm hingegen spezieller als Art. 8 GRC. Informationen aus dem beruflichen Kontext sind schließlich allein durch Art. 8 GRC geschützt.[923] Letztlich kommt der Debatte über die Abgrenzung der Schutzbereiche aber keine entscheidende Bedeutung zu. Der Schutzbedarf von Daten bestimmt sich nach der konkreten Verarbeitungssituation und nicht danach, welcher Sphäre sie abstrakt zuzuordnen sind.[924] Die Entscheidung

---

919 *Kingreen,* in: Calliess/Ruffert 2016, Art. 8 GRC, Rn. 1a.
920 EuGH, ECLI:EU:C:2008:54, Rn. 64 – *Promusicae*; EuGH, ECLI:EU:C:2010:662, Rn. 47 – *Schecke*; EuGH, ECLI:EU:C:2011:777, Rn. 41 f. – *ASNEF*; EuGH, ECLI:EU:C:2017:592, Rn. 122 f. – *Fluggastdatenabkommen*.
921 *Burgkardt* 2013, S. 346 ff.; *Marsch* 2018; *Michl,* DuD 2017, S. 349–353; *Wagner* 2015.
922 BeckOK DSR/*Schneider*, Völker- und unionsrechtliche Grundlagen, Rn. 19.
923 Ähnlich *Jarass* 2016, Art. 8 GRC, Rn. 4.
924 Ähnlich *Michl,* DuD 2017, S. 349, 352.

des Europäischen Gerichtshofs, Art. 7 und 8 GRC zusammen zu prüfen und gemeinsamen Schranken zu unterwerfen, mag dogmatisch zweifelhaft sein, spielt aber zumindest für die hier vorgenommene Betrachtung keine Rolle.

679 Weitaus weniger Schwierigkeiten bereitet zumindest dem Europäischen Gerichtshof die Abgrenzung der Art. 7 und 8 GRC zu Art. 16 AEUV. Letzteres ist im Hinblick auf seinen Gewährleistungsgehalt vollständig in Art. 8 GRC enthalten und unterliegt insbesondere auch den Schrankenbestimmungen des Art. 8 Abs. 2 GRC.[925] Die Anforderung der Kontrolle durch unabhängige Stellen nach Art. 16 Abs. 2 UAbs. 1 S. 2 AEUV stimmt mit der in Art. 8 Abs. 3 GRC überein. Art. 16 AEUV kommt damit lediglich als Kompetenznorm eine eigenständige Bedeutung zu. Ob sie eine Grundrechtsnorm ist, spielt letztlich keine Rolle, weil sie als solche jedenfalls vernachlässigt werden kann.[926]

3.2.3.3 Schutzgewährleistung des Grundrechts

680 Das Recht auf Schutz personenbezogener Daten nach Art. 8 Abs. 1, Art. 7 GRC ist ein relativ junges Grundrecht,[927] dass besonders auf die spezifischen Gefährdungen sowohl in als auch der Informationsgesellschaft abstellt. Da diese Gefährdungen für den Einzelnen oft schwer fassbar sind, lässt sich auch die Schutzgewährleistung dieses Rechts anders als die der „klassischen" Grundrechte wie etwa dem Recht auf Schutz der Privatsphäre oder auf Unversehrtheit nicht leicht erschließen. Im Folgenden soll

925 Nach *Kingreen,* in: Calliess/Ruffert 2016, Art. 8 GRC, Rn. 3; *Streinz/Michl,* in: Streinz 2018, Art. 52 GRC, Rn. 23 ist Art. 52 Abs. 2 GRC nicht auf den erst im Lissabonner Vertrag eingeführten Art. 16 Abs. 1 AEUV anwendbar. I.E. ebenso, aber über eine teleologische Reduktion des § 52 Abs. 2 GRC, sodass die Schrankenregelung in der Charta auch auf Art. 16 Abs. 1 AEUV Anwendung findet, *Döhmann/Eisenbarth,* JZ 2011, S. 169, 172.

926 EuGH, ECLI:EU:C:2017:592, Rn. 120 – *Fluggastdatenabkommen*; *Kingreen,* in: Calliess/Ruffert 2016, Art. 16 AEUV, Rn. 3; *Schiedermair,* in: Simitis et al. 2019, Einleitung, Rn. 177. Zum Ganzen *Schmidt* 2017, S. 154 ff.

927 Die aus zeitlicher Sicht „längste" Wurzel dieses Grundrechts ist das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" des Europarats vom 28.1.1981, *Bernsdorff,* in: Meyer/Hölscheidt 2019, Art. 8 GRC, Rn. 2. Die Europäische Menschenrechtskonvention, in der die „klassischen" Grundrechte enthalten sind und die eine Rechtserkenntnisquelle für die unionalen Grundrechte bildet (siehe 3.2.1.3, S. 259), wurde am 4.11.1950 unterzeichnet und trat am 3.9.1953 allgemein in Kraft.

darum ein Überblick über die Spezifika des Rechts auf Schutz personenbezogener Daten gegeben werden.

3.2.3.3.1 Der Anknüpfungspunkt des personenbezogenen Datums

681 Das Schutzobjekt des Grundrechts auf Datenschutz nach Art. 8 Abs. 1, Art. 7 GRC sind personenbezogene Daten. Dieser Begriff umfasst jede Information, die eine bestimmte oder bestimmbare natürliche Person betrifft,[928] unabhängig davon, ob diese Information als sensibel anzusehen ist.[929] Damit werden auch Bereiche abgedeckt, die man gemeinhin nicht mit dem Begriff „Daten" assoziiert. So ließe sich das Recht am eigenen Bild auch ohne Weiteres unter den Schutzbereich von Art. 8 GRC subsumieren. Jedenfalls zu Art. 7 GRC ist es über Art. 52 Abs. 3 GRC i.V.m. Art. 8 Abs. 1 EMRK anerkannt.[930]

682 Unter welchen Umständen eine Person bestimmbar ist, wurde bisher in der Rechtsprechung des Europäischen Gerichtshofs nicht unter der Maßgabe des Primärrechts, sondern nur im Hinblick auf die gleichlautende Definition in Art. 2 der Datenschutzrichtlinie 95/46/EG (DSRL)[931] diskutiert.[932] Da die Datenschutzrichtlinie aber in den Erläuterungen zu Art. 8 GRC ausdrücklich als Rechtserkenntnisquelle angeführt wird, kann man davon ausgehen, dass die dazu ergangene Rechtsprechung den Schutzbereich von Art. 8 Abs. 1, 7 GRC konkretisiert. Insofern sei auf die Erörterungen zum Sekundärrecht verwiesen (siehe 3.3.1, S. 315).

928 EuGH, ECLI:EU:C:2010:662, Rn. 52 – *Schecke*.

929 EuGH, ECLI:EU:C:2014:238, Rn. 33 – *Digital Rights Ireland*; EuGH, ECLI:EU:C:2015:650, Rn. 87 – *Schrems*; EuGH, ECLI:EU:C:2017:592, Rn. 124 – *Fluggastdatenabkommen*; noch zum Grundsatz-Grundrecht, abgeleitet aus Art. 8 EMRK, EuGH, ECLI:EU:C:2003:294, Rn. 75 – *ORF*.

930 EGMR v. 24.6.2004 – 59320/00, GRUR 2004, S. 1051, Rn. 50 – *Hannover/Deutschland*.

931 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, letzte konsolidierte Fassung CELEX 01995L0046–20031120.

932 EuGH, ECLI:EU:C:2016:779, Rn. 31 ff. – *Breyer*.

3.2.3.3.2 Die Art der Verarbeitung

Wie sich im Umkehrschluss aus der Schrankenbestimmung in Art. 8 Abs. 2 S. 1 GRC ergibt, wird in den Schutzbereich des Rechts auf Schutz personenbezogener Daten nach Art. 8 Abs. 1, Art. 7 GRC eingegriffen, wenn diese Daten verarbeitet werden. Auch hier ist der Begriff in Anlehnung an Art. 2 lit. b DSRL[933] denkbar weit auszulegen, als jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang im Zusammenhang mit personenbezogenen Daten.[934] Der Begriff des Vorgangs ist kleinteilig zu betrachten, was dafür sorgt, dass in einem mehraktigen Geschehen auch mehrere Eingriffe vorliegen. So ist es z.B. gesondert rechtfertigungsbedürftig, wenn einmal gespeicherte Daten anderen übermittelt oder zugänglich gemacht werden.[935] Ob der Betroffene aus dem jeweiligen Vorgang irgendwelche Nachteile erleidet, spielt keine Rolle.[936] 683

Um einen Eingriff in die informationelle Selbstbestimmung zu bejahen, ist es schließlich unbedeutend, wie genau die Daten gespeichert werden. Zwar kommt jenen Speichermethoden besondere Relevanz zu, die es dem Verarbeiter ermöglichen, die Daten schnell wieder aufzufinden, sie effizient massenhaft auszulesen und sie ggf. mit anderen Daten in Verbindung zu bringen, um neue Informationen zu generieren. Entsprechend hat sich der europäische Verordnungsgeber mit Art. 2 Abs. 1 DS-GVO auf die Regulierung von automatisierter Datenverarbeitung und nichtautomatisierter Datenverarbeitung in Datensystemen – in der Regel Akten – beschränkt. 684

Auf der Ebene des Grundrechts reicht aber auch die unsystematische Datenspeicherung, etwa auf einem losen Notizzettel eines Sachbearbeiters, um einen Eingriff in den Schutzbereich zu bejahen. Der deutsche Gesetzgeber hat den Anwendungsbereich des Beschäftigtendatenschutzes hierauf in § 26 Abs. 7 BDSG 2018 ausgeweitet. Abgesehen davon, dass hierauf die Grundrechte des Grundgesetzes Anwendung finden (siehe 3.1.5, S. 246) 685

933 EuGH, ECLI:EU:C:2013:670, Rn. 28 – *Schwarz*.

934 *Jarass* 2016, Art. 8 GRC, Rn. 8; *Kingreen*, in: Calliess/Ruffert 2016, Art. 8 GRC, Rn. 12.

935 EuGH, ECLI:EU:C:2014:238, Rn. 35 – *Digital Rights Ireland*; EuGH, ECLI:EU:C:2014:317, Rn. 35 ff. – *Google Spain*; EuGH, ECLI:EU:C:2017:592, Rn. 124 – *Fluggastdatenabkommen*.

936 EuGH, ECLI:EU:C:2014:238, Rn. 33 – *Digital Rights Ireland*; EuGH, ECLI:EU:C:2014:317, Rn. 96 – *Google Spain*; EuGH, ECLI:EU:C:2015:650, Rn. 87 – *Schrems*; noch zum Grundsatz-Grundrecht, abgeleitet aus Art. 8 EMRK, EuGH, ECLI:EU:C:2003:294, Rn. 75 – *ORF*.

und diese Ausweitung nicht recht in die Herleitung des Bundesverfassungsgerichts passt, spielt diese Form der Verarbeitung für Assistenzsysteme in der Industrie 4.0 naturgemäß eine untergeordnete Rolle.

3.2.3.3.3 Die Wirkung der Einwilligung

686 Die Einwilligung der betroffenen Person ist nach dem Wortlaut des Art. 8 Abs. 2 S. 1 GRC als Rechtfertigungsgrund für Eingriffe aufgezählt. Nach allgemeiner Grundrechtsdogmatik wirkt eine – wirksam erteilte – Einwilligung jedoch eingriffsausschließend.[937] Der Formulierung zur Eingriffsrechtfertigung in Art. 8 Abs. 2 S. 1 GRC lässt sich aber entnehmen, dass die Einwilligung im Hinblick auf festgelegte Zwecke zu erfolgen hat. Auch das ist aber keine Anforderung, die sich nicht bereits aus der allgemeinen Regelung ableiten ließe. Ein Grundrechtsverzicht kann nicht abstrakt, sondern nur im Hinblick auf durch den Grundrechtsträger absehbare konkrete Situationen erklärt werden.[938]

687 Dieser letzten Auffassung scheint auch der Europäische Gerichtshof zuzuneigen. Anders wäre seine in ihrer Allgemeinheit äußerst zweifelhafte Aussage, „die bloße Speicherung personenbezogener Daten über die an das Personal gezahlten Gehälter durch einen Arbeitgeber [begründe] als solche keinen Eingriff in die Privatsphäre“[939], nicht zu erklären.[940] Der Europäische Gerichtshof geht augenscheinlich davon aus, dass die Notwendigkeit, Gehaltsdaten zu speichern, derart auf der Hand liegt, dass man von einer konkludent erteilten Einwilligung der betroffenen Beschäftigten ausgehen könne. Zumindest in dem damaligen Fall scheint dies gerechtfertigt, da weder die Datenschutzrichtlinie noch das einschlägige nationale Recht Formerfordernisse für die Einwilligung enthielten.[941]

---

937 *Jarass* 2016, Art. 8 GRC, Rn. 9; *Kingreen,* in: Calliess/Ruffert 2016, Art. 8 GRC, Rn. 13; *Wagner* 2015, S. 70 ff.

938 Dazu allgemein *Fischinger,* JuS 2007, S. 808, 809.

939 EuGH, ECLI:EU:C:2003:294, Rn. 74 – *ORF*; dagegen bejaht der Europäische Gerichtshof in anderen Fällen den Eingriffscharakter der Speicherung EuGH, ECLI:EU:C:2013:670, Rn. 28 – *Schwarz*; EuGH, ECLI:EU:C:2014:238, Rn. 34 – *Digital Rights Ireland*.

940 Ähnlich BeckOK DSR/*Schneider*, Völker- und unionsrechtliche Grundlagen, Rn. 16.

941 Die Anforderungen an die Einwilligung ergaben sich lediglich aus Art. 2 lit. h DSRL. Auch das österreichische Datenschutzgesetz 2000 (BGBl. I 1999, 165), das die Einwilligung in § 8 Abs. 1 Nr. 2 und § 4 Nr. 1 DSG regelte, erwähnt kei-

3.2.3.4 Abwägungsfestigkeit des Rechts auf Schutz personenbezogener Daten

Angesichts des äußerst weiten Schutzbereichs- und Eingriffsverständnis ist die Kernfrage des Datenschutzrechts diejenige der Rechtfertigung. Für den privaten Arbeitgeber, der die Daten seiner Arbeitnehmer verarbeitet, spielt dies nur im Rahmen der mittelbaren Drittwirkung eine Rolle. Zumindest auf primärrechtlicher Ebene benötigt er – der kein Grundrechtsadressat ist – keine gesetzliche Grundlage, um personenbezogene Daten zu verarbeiten. Der sich aus Art. 52 Abs. 1 S. 1 GRC ergebende Gesetzesvorbehalt ist darum hier nicht relevant (dazu auch 3.2.5, S. 310). 688

An welche Voraussetzungen staatliche Datenverarbeitung gebunden ist, ist dennoch auch für den Arbeitgeber bedeutsam. Anhand der Anforderungen, welche die Grundrechtsordnung an staatliche Eingriffe stellt, lassen sich sowohl der Stellenwert des jeweiligen Grundrechts als auch die spezifischen Schutzgewährleistungen ablesen, die es enthalten soll. Dies schlägt sich auch in den staatlichen Schutzpflichten nieder, die – und sei es nur über die Auslegung des europäischen Sekundärrechts und ggf. des durchführenden mitgliedstaatlichen Rechts durch die Gerichte – letztlich dazu führen, dass auch das Handeln Privater bestimmten Mindestanforderungen unterliegt. 689

Der Schwerpunkt der Prüfung liegt bei der Frage der Verhältnismäßigkeit der Beschränkung. Daneben müssen aber auch die besonderen Eingriffsvoraussetzungen erfüllt sein. Speziell für den Datenschutz gilt es dabei zu beachten, dass er nach der Rechtsprechung des Europäischen Gerichtshofs zumindest formal in zwei Grundrechten wurzelt. 690

3.2.3.4.1 Die Schranken-Schranken nach Art. 52 Abs. 1 GRC

Die wichtigste Schranken-Schranke bildet die Anforderung nach Art. 52 Abs. 1 S. 2 GRC, den Grundsatz der Verhältnismäßigkeit zu wahren. Teil dieses Grundsatzes ist es, Grundrechte nur zu legitimen Zwecken einzuschränken. Neben den von der Union anerkannten, dem Gemeinwohl die- 691

---

ne Formvorschriften. Anders war dies hingegen im damalige deutsche Recht; das Bundesdatenschutzgesetz in der Fassung vom 18.5.2001, das der Umsetzung der Richtlinie diente, sah in § 4a Abs. 1 S. 3 BDSG 2003 – wortgleich mit der vorherigen Fassung (§ 4 Abs. 2 S. 2 BDSG 2003) – grundsätzlich die Schriftform vor.

nenden Zielsetzungen wird dabei in Art. 52 Abs. 1 S. 2 GRC auch der Schutz der Rechte und Freiheiten anderer als legitimes Ziel ausdrücklich anerkannt. Im Kontext des Beschäftigtendatenschutzes sind es in aller Regel die Grundrechte des Arbeitgebers, aus denen ein legitimer Verarbeitungszweck abgeleitet werden kann.

692 Die Prüfung der Verhältnismäßigkeit besteht im Übrigen aus dem bekannten Dreiklang aus Geeignetheit, Erforderlichkeit und Angemessenheit.[942] Die Datenverarbeitung muss dem festgelegten Verwendungsziel nach Art. 52 Abs. 1 S. 2 GRC „tatsächlich entsprechen", wobei es ausreicht, wenn dieser Zweck nicht komplett erreicht, sondern nur gefördert wird.[943] Die Datenverarbeitung darf nicht über das Erforderliche hinausgehen,[944] muss also auf das absolut Notwendige beschränkt bleiben.[945] Hierzu gehört auch, einen wirksamen Schutz vor Missbrauch sicherzustellen.[946] Abschließend ist zu überprüfen, ob die konfligierenden Rechte und Interessen ausgewogen gewichtet werden.[947]

693 Die absolute Grenze der Einschränkbarkeit eines Grundrechts ist dort erreicht, wo sein Wesensgehalt berührt wird. Die Anforderung lässt sich ebenfalls aus dem Grundsatz der Verhältnismäßigkeit ableiten, ist aber – wie diejenige zu den legitimen Zielsetzungen – in Art. 52 Abs. 1 S. 1 GRC eigens aufgeführt. Wo diese Grenze verläuft, lässt sich nicht abstrakt bestimmen, und wenn, dann nur mit generalklauselartigen Formulierungen, die keinerlei Erkenntnisgewinn vermitteln.[948] Auch im Kontext der EU-Grundrechte gilt darum das Bonmot, wonach das Wesen des Wesensgehalts unbekannt ist.[949] Eine Annäherung an dieses Problem findet sich in der Entscheidung des Europäischen Gerichtshofs zur Richtlinie 2006/24/EG über die Vorratsdatenspeicherung. Danach sei der Wesensge-

---

942 Zur Kritik am Vorgehen des Europäischen Gerichtshofs, der nur unzureichend zwischen der Erforderlichkeitsprüfung einerseits und der Abwägung im Rahmen der Angemessenheit unterscheidet, *Kühling/Klar*, JURA 2011, S. 774 f., m.w.N.

943 EuGH, ECLI:EU:C:2013:670, Rn. 43 – *Schwarz*; EuGH, ECLI:EU:C:2014:238, Rn. 50 – *Digital Rights Ireland*.

944 EuGH, ECLI:EU:C:2010:662, Rn. 75 – *Schecke*.

945 EuGH, ECLI:EU:C:2013:670, Rn. 40 – *Schwarz*.

946 EuGH, ECLI:EU:C:2014:238, Rn. 54 – *Digital Rights Ireland*; EuGH, ECLI:EU:C:2017:592, Rn. 141 – *Fluggastdatenabkommen*.

947 EuGH, ECLI:EU:C:2010:662, Rn. 77 – *Schecke*.

948 Ähnlich *Jarass* 2016, Art. 52 GRC, Rn. 29, der z.B. auf die Formulierung in EuGH, ECLI:EU:C:2016:84, Rn. 52 – *J.N.* verweist, wonach der „Gewährleistungsgehalt dieses Rechts nicht in Frage" gestellt werden darf.

949 Nach *Luhmann* 2013, S. 133, der dort allerdings zum Machtbegriff schreibt.

halt des Rechts nach Art. 8 GRC nicht angetastet, weil die Richtlinie in Art. 7 die Einhaltung der Grundsätze des Datenschutzes und Datensicherheit forderte und insbesondere vorschrieb, dass technische und organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit zu ergreifen sind.[950]

694 Den Anforderungen der Schranken-Schranken müssen sowohl die einschränkende Norm als auch die sie ggf. umsetzende Einzelmaßnahme genügen. Für die Norm selbst ergeben sich daraus Anforderungen an ihre Bestimmtheit, die dergestalt gewährleistet sein muss, dass die Betroffenen die Folgen voraussehen können.[951] Diese Anforderungen steigen, je tiefer durch die Norm oder aufgrund der Norm in Grundrechte eingegriffen wird bzw. werden kann.

695 Bei besonders schwerwiegenden Eingriffen wie z.B. der heimlichen Telekommunikations- oder Videoüberwachung im Zusammenhang mit staatlichem Handeln hat der Europäische Gerichtshof für Menschenrechte sehr detaillierte Anforderungen an die Rechtsgrundlage formuliert.[952] Sie umfassen Vorgaben zur Art der Straftaten, der überwachten Personengruppe, der zeitlichen Grenze, dem Verfahren der Auswertung, Verwendung und Speicherung, zu Vorsichtsmaßnahmen bei der Übermittlung und zu den Umständen, unter denen die Daten zu löschen sind. Ähnlich agiert der Europäische Gerichtshof in der Entscheidung zur Richtlinie über die Vorratsdatenspeicherung, bei der er zusätzlich die mangelnde Regelungsdichte im Hinblick auf die Maßnahmen zum Schutz vor missbräuchlicher Verarbeitung moniert.[953] Um den Wesensgehalt zu achten, hatte dies noch ausgereicht. Der Verhältnismäßigkeitsprüfung einschließlich den Anforderungen zur Bestimmtheit hielten die Regelungen hingegen nicht mehr stand.

696 Diese Anforderungen lassen sich nicht ohne Weiteres auf das Handeln Privater übertragen. Das liegt zum einen daran, dass Private für den Betroffenen keine Folgen bewirken können, die denen der Strafverfolgung – für

950 EuGH, ECLI:EU:C:2014:238, Rn. 40 – *Digital Rights Ireland* Zur Anforderung, Schutzmaßnahmen gegen Missbrauch vorzusehen auch EuGH, ECLI:EU:C:2013:670, Rn. 55 – *Schwarz*.

951 Allgemein noch zu Art. 8 EMRK EuGH, ECLI:EU:C:2003:294, Rn. 77 – *ORF*.

952 Zur Telekommunikationsüberwachung im Rahmen der Strafverfolgung EGMR v. 29.6.2006 – 54934/00, NJW 2007, S. 1433, Rn. 95 – *Weber u. Saravia/Deutschland*, m.w.N. Zur Videoüberwachung einer privaten Versicherungsgesellschaft, die Leistungen aus einer staatlichen Pflichtversicherung erbringt EGMR v. 18.10.2016 – 61838/10, NJW-RR 2018, S. 294, Rn. 73 ff. – *Vukota-Bojić/Schweiz*.

953 EuGH, ECLI:EU:C:2014:238, Rn. 54 ff. – *Digital Rights Ireland*.

die diese Bestimmtheitskriterien entwickelt wurden[954] – nahekommen. Zum anderen schwächt auch die nur mittelbare Grundrechtsbindung die Bestimmtheitskriterien – dann für die staatlichen Schutzpflichten – ab. So hat der Europäische Gerichtshof für Menschenrechte an die Videoüberwachung durch eine öffentliche Unfallversicherung, die sich gegen Leistungsmissbrauch schützen wollte, ähnlich strenge Anforderungen an die Bestimmtheit der Rechtsgrundlage wie bei der staatlichen Telekommunikationsüberwachung angelegt.[955] Bei der Videoüberwachung durch einen privaten Arbeitgeber zur Aufdeckung gegen ihn gerichteter Straftaten lassen es der Europäische Gerichtshof und der Europäische Gerichtshof für Menschenrechte hingegen genügen, wenn der Zweck der Maßnahme und die betroffene Personengruppe feststehen und die übrige Konkretisierung, insbesondere die der notwendigen Vorbehalte und Schutzmaßnahmen, durch die Rechtsprechung vorgenommen wird.[956] Insofern steht die private Videoüberwachung auf einer Stufe mit weniger intensiven staatlichen Eingriffen.[957]

697 Auch im Hinblick auf weniger schwere Eingriffe gibt es aber hinsichtlich der Konkretisierung durch die Gerichte grenzen. Eine völlig unbestimmte Generalklausel, der zufolge eine Behörde alle Maßnahmen ergreifen kann, die sie zur Erfüllung ihrer Aufgaben für erforderlich hält, reicht hingegen nicht.[958] Das ergibt sich aber bereits aus dem Grundsatz, wonach von der Aufgabenzuweisung nicht einfach auf die Eingriffsbefugnis geschlossen werden darf.[959]

698 Nach diesen Grundsätzen sind zumindest die Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz selbst nicht zu beanstanden. Sie genügen erstens dem Gesetzesbegriff und sehen zweitens in Art. 5, 25 und 32 DS-GVO Grundsätze des Datenschutzes vor (siehe dazu 3.4.1,

954 EGMR v. 29.6.2006 – 54934/00, NJW 2007, S. 1433, Rn. 95 – *Weber u. Saravia/Deutschland*, m.w.N.

955 EGMR v. 18.10.2016 – 61838/10, NJW-RR 2018, S. 294, Rn. 73 ff. – *Vukota-Bojić/Schweiz*.

956 EGMR v. 5.10.2010 – 420/07, S. 10 f. – *Köpke/Deutschland*. Skeptisch in Bezug auf letzteres noch *Hornung,* MMR 2007, S. 433, 434.

957 Skeptisch zur Übermittlung von Daten über die jährlichen Bezüge von Beschäftigten EuGH, ECLI:EU:C:2003:294, Rn. 78 – *ORF*; zur GPS-Ortung EGMR v. 2.9.2010 – 35623/05, NJW 2011, S. 1333, Rn. 66 f. – *Uzun/Deutschland*; zur Videoüberwachung von Beschäftigten.

958 EGMR v. 3.4.2007 – 62617/00, MMR 2007, S. 431, Rn. 45 ff. – *Copland/Vereinigtes Königreich*.

959 *Hornung,* MMR 2007, S. 433, 434.

S. 354), einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Rechtmäßigkeit der Datenverarbeitung sowie der Datensicherheit. Die Frage verschiebt sich damit auf die Ebene der konkreten Datenverarbeitung. Solange sie die erwähnten Grundsätze einhält, wird aber auch hier die Einschränkung der Grundrechte nach Art. 7 und 8 GRC zu rechtfertigen sein.

3.2.3.4.2 Spezifische Anforderungen nach Art. 8 Abs. 2 EMRK

699 Das Recht auf Achtung des Privat- und Familienlebens nach Art. 7 GRC enthält keine zusätzlichen Eingriffsvoraussetzungen. Über die Transfernorm des Art. 52 Abs. 2 GRC (siehe 3.2.3.2, S. 286) gelten in Bezug auf Art. 7 GRC aber die spezifischen Eingriffsvoraussetzungen des Art. 8 Abs. 2 EMRK. Das gilt nicht nur hinsichtlich des Schutzbereichs, sondern auch hinsichtlich der Schrankenbestimmung. Der einfache Gesetzesvorbehalt des Art. 52 Abs. 1 GRC wird durch die speziellere Norm in Art. 52 Abs. 3 GRC i.V.m. Art. 8 Abs. 2 EMRK zwar nicht verdrängt, deren Anforderungen sind aber bei der Auslegung der Schrankenbestimmung zu beachten.[960]

700 In Art. 8 Abs. 2 EMRK wird ein Eingriff in das Recht auf Achtung des Privat- und Familienlebens zumindest dem Wortlaut nach einem qualifizierten Gesetzesvorbehalt unterworfen. Die legitimen Ziele, zu denen u.a. der Schutz der Rechte und Freiheiten anderer zählen, sind aber so weit gefasst, dass sie keine ernstzunehmende Einschränkungswirkung entfalten.[961] Der Anforderung, dass der Eingriff „in einer demokratischen Gesellschaft notwendig" sein muss, lässt sich das Verhältnismäßigkeitsprinzip entnehmen, wobei die Prüfung nicht grundlegend anders abläuft als im Rahmen des Art. 52 Abs. 1 GRC. In der Sache enthält Art. 8 Abs. 2 EMRK darum keine zusätzlichen Anforderungen, bewirkt aber, dass die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zur Verhältnismäßigkeitsprüfung berücksichtigt werden muss.

---

960 *Jarass* 2016, Art. 52 GRC, Rn. 60; *Kingreen,* in: Calliess/Ruffert 2016, Art. 52 GRC, Rn. 38; *Schwerdtfeger,* in: Meyer/Hölscheidt 2019, Art. 52 GRC, Rn. 63 m.w.N., a.A. im Sinne einer Verdrängung von Art. 52 Abs. 1 GRC noch *Borowsky,* in: Meyer 2014, Art. 52 GRC, Rn. 29.

961 BeckOK InfoMedienR/*Gersdorf*, Art. 8 GRC, Rn. 55.

3.2.3.4.3 Spezifische Anforderungen nach Art. 8 Abs. 2 GRC

701 Für das Recht auf Schutz personenbezogener Daten sind in Art. 8 Abs. 2 und 3 GRC zusätzliche spezifische Eingriffsvoraussetzungen normiert. Danach dürfen Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat zudem das Recht Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird schließlich von einer unabhängigen Stelle überwacht. Nicht alle dieser Anforderungen haben eine eigenständige Bedeutung. So ist die legitime Grundlage in Art. 8 Abs. 2 S. 1 GRC nichts anderes als der legitime Zweck nach Art. 52 Abs. 1 S. 2 GRC (dazu 3.2.3.4.1, S. 293). Andere Anforderungen betonen hingegen die Spezifika des Datenschutzes.

702 Die in Art. 8 Abs. 2 S. 1 GRC geregelten Anforderungen – sowohl die, die Zwecke festzulegen, als auch die, die Datenverarbeitung hierfür nur nach Treu und Glauben zu verarbeiten – betonen die Selbstbestimmung der betroffenen Person, die eingeschränkt wird, wenn deren personenbezogene Daten verarbeitet werden. Die Zwecke müssen festgelegt sein, damit die betroffene Person das Ausmaß dieser Einschränkung überblicken und ggf. mithilfe ihrer Betroffenenrechte nach Art. 8 Abs. 2 S. 2 GRC nachsteuern kann. Gerade wenn die Datenverarbeitung wie im Beschäftigtendatenschutz auch auf der Grundrechtsausübung der betroffenen Person beruht – nämlich dem Entschluss, ein Beschäftigungsverhältnis zu begründen – entsteht mit dem Datenverarbeiter ein Vertrauensverhältnis, das diesem gewisse Rücksichtnahmepflichten aufbürdet (näher siehe 3.4.1.6.2, S. 420). Das kommt in der Formulierung „Treu und Glauben" zum Ausdruck, die insofern die ohnehin zu berücksichtigenden Rechtmäßigkeitsanforderungen der Zweckbindung und des Verhältnismäßigkeitsprinzips bekräftigt.[962] Eine eigenständige Bedeutung hat dieses Merkmal jedenfalls nicht.

703 Ohne das Auskunfts- und Berichtigungsrecht nach Art. 8 Abs. 2 S. 2 GRC wäre es dem Betroffenen in vielen Verarbeitungssituationen nicht möglich, sich zu vergewissern, ob die Verarbeitung fehlerfrei durchgeführt wird und insgesamt zulässig ist. Dieses Recht ist darum ein integraler Be-

962 In Bezug auf die Zweckbindung werden aus dem Merkmal Treu und Glauben Unterrichtungspflichten für den Fall der zweckändernden Weiterverarbeitung abgeleitet, noch zur Datenschutzrichtlinie EuGH, ECLI:EU:C:2015:638, Rn. 34 – *Bara*; *Wagner* 2015, S. 89 f.

standteil des Rechts auf Schutz der Privatsphäre nach Art. 7 GRC des Rechts auf Schutz personenbezogener Daten nach Art. 8 GRC. Es bezieht sich sowohl auf die Vergangenheit als auch auf die Gegenwart.[963]

Zusätzlich zur Kontrolle durch den Betroffenen muss die Einhaltung der Vorschriften aus Art. 8 Abs. 1 und 2 GRC nach Absatz 3 von einer unabhängigen Stelle überwacht werden. Diese unabhängige Kontrolle wird durch die Vorschriften der Datenschutz-Grundverordnung über die Aufsichtsbehörden gewährleistet. 704

Die Eingriffskautelen in Art. 8 Abs. 2 EMRK haben für die Rechtfertigung eines Eingriffs in das Recht auf Schutz personenbezogener Daten keine Auswirkung. Die Transferklausel in Art. 52 Abs. 3 greift hier nicht, weil sich die beiden Rechte nicht entsprechen. Zwar kommen sich die Schutzbereiche angesichts der weiten Auslegung des Art. 8 EMRK durch den Europäischen Gerichtshof für Menschenrechte sehr nahe (siehe 3.2.3.2, S. 286), um einen Zirkelschluss zu vermeiden – das Entsprechen der Rechte ist gewissermaßen sowohl Tatbestandsvoraussetzung als auch Rechtsfolge der Regelung in Art. 52 Abs. 3 S. 1 GRC – wird hier aber eher eine formalisierte Betrachtung angestellt.[964] Da Art. 8 GRC in den Listen zu vollständigen oder teilweisen Identität der Rechte in Charta und Konvention nicht auftaucht, findet die Transfernorm in Art. 52 Abs. 3 GRC keine Anwendung.[965] 705

3.2.3.5 Kriterien zur Bestimmung der Eingriffstiefe

Das Recht auf Schutz personenbezogener Daten nach Art. 7, 8 GRC ist unabhängig vom Aussagegehalt und der Schutzwürdigkeit der einzelnen Information anwendbar (siehe 3.2.3.3.1, S. 290). Es gibt folglich weder per se belanglose und darum grundrechtlich nicht schutzwürdige Informationen noch gibt es Kategorien von Informationen, die auf jeden Fall einem Verarbeitungsverbot unterliegen. Entscheidend ist stets der Verarbeitungskon- 706

963 EuGH, ECLI:EU:C:2009:293, Rn. 49 ff. – *Rijkeboer* Dass der Europäische Gerichtshof in dem Urteil das Auskunfts- und Berichtigungsrecht auf das Recht auf Schutz der Privatsphäre bezieht ist dem Umstand geschuldet, dass er zwischen den Rechten auf Art. 7 und 8 GRC nicht unterscheidet, 3.2.3.2, S. 286.

964 *Borowsky*, in: Meyer 2014, Art. 52 GRC, Rn. 31, offen dagegen *Kingreen*, in: Calliess/Ruffert 2016, Art. 52 GRC, Rn. 30; *Schwerdtfeger*, in: Meyer/Hölscheidt 2019, Art. 52 GRC, Rn. 57 f.

965 BeckOK InfoMedienR/*Gersdorf*, Art. 8 GRC, Rn. 22.

text im Einzelfall.[966] So mag die Wohnadresse für viele Menschen keine übermäßig sensible Information darstellen, für eine Betroffene, die in einem Frauenhaus Schutz sucht, dürfte die Vertraulichkeit ihres Aufenthaltsorts in diesem Moment überaus wichtig sein. Umgekehrt dürften Informationen über die Religionszugehörigkeit in aller Regel als sensibel eingestuft werden, vor allem in Staaten, welche die Religionsfreiheit nicht effektiv gewährleisten. Dass der Papst katholisch ist, zählt hingegen zum Allgemeinwissen und kann nicht als sensible Information betrachtet werden.[967]

707 Der Annahme, stets den konkreten Verarbeitungskontext zu betrachten, steht es aber nicht entgegen, typische Kriterien zu definieren, die, wenn sie vorliegen, ein Indiz dafür darstellen, dass die jeweilige Datenverarbeitung tief oder gering in das Grundrecht des Betroffenen aus Art. 7 und 8 GRC eingreift. Diese Überlegung hat auch in das Sekundärrecht Eingang gefunden, für das in ErwG 75 der Datenschutz-Grundverordnung Kriterien zur Risikobewertung niedergelegt sind. Auf der Ebene des Primärrechts kann die Rechtsprechung des Europäischen Gerichtshofs und ergänzend des Europäischen Gerichtshofs für Menschenrechte herangezogen werden. Sie ist zwar bisher bei weitem nicht so umfangreich wie die der deutschen Gerichte, insbesondere der des Bundesverfassungsgerichts, erlaubt aber dennoch bereits eine gewisse Systematisierung.

3.2.3.5.1 Betroffener Lebensbereich

708 Das Recht auf Schutz personenbezogener Daten hat seine Wurzeln im Recht auf Schutz der Privatsphäre, welches auch als allgemeines Persönlichkeitsrecht verstanden werden kann. Auf europäischer Ebene hat sich zwar keine Abstufung der Rechtfertigungsanforderungen vergleichbar der „Sphärentheorie" des Bundesverfassungsgerichts[968] entwickelt. Dennoch gilt auch hier, dass der Eingriff umso schwerer wiegt, je stärker sich die Da-

966 *Wagner* 2015, S. 128 f.
967 *Roßnagel, et al.* 2001, S. 62.
968 BVerfG v. 15.1.1970 – 1 BvR 13/68, E 27, S. 344, 351 – *Ehescheidungsakten*; BVerfG v. 19.7.1972 – 2 BvL 7/71, E 33, S. 367 ff. – *Zeugnisverweigerungsrecht für Sozialarbeiter*; dazu ausführlich *Di Fabio,* in: Maunz/Dürig 2015, Lfg. 39, Art. 2 GG, Rn. 158 ff., m.w.N.

tenverarbeitung auf private oder gar intime[969] Lebensbereiche auswirkt. In der Regel rührt dies daher, dass Daten verarbeitet werden, die wie z.B. die Information über die sexuelle Orientierung per se einem solchen Lebensbereich zugeordnet werden. Zwingend ist dies allerdings nicht; entscheidend ist der gesamte Verarbeitungskontext.

Aus dem verstärkten Schutz besonderer Lebensbereiche kann zu einem gewissen Grad auch auf die Sensibilität einer Datenquelle geschlossen werden. So bedeutet die Verarbeitung von Daten aus nicht zugänglichen Quellen in der Regel einen schwereren Eingriff als die aus öffentlich zugänglichen Quellen, weil der Verantwortliche hier mit höherer Wahrscheinlichkeit Informationen über die Privatsphäre der betroffenen Person erlangt.[970] 709

3.2.3.5.2 Umfang und Art der Verarbeitung

Mit der Abstufung der Lebensbereiche steht auch der Umfang oder die Art der Datenerhebung in einem engen Verhältnis. Je umfangreicher die jeweilige Erhebungsmethode das Verhalten der betroffenen Person erfasst, desto höher ist die Wahrscheinlichkeit, auch besonders persönlichkeitsrelevante Aspekte einzufangen. 710

Das zeigt sich z.B. im Bereich der Videoüberwachung. Auch in von sozialer Interaktion geprägten Räumen wie in der Öffentlichkeit oder am Arbeitsplatz, kann der Mensch unmöglich eine z.B. ausschließlich professionelle Rolle einnehmen, die keinerlei Rückschlüsse auf seine Persönlichkeit zulässt. Da die Videoüberwachung aber das gesamte optisch wahrnehmbare Verhalten der betroffenen Person erfasst, sind dadurch zwangsläufig Aspekte betroffen, die typischerweise stärker geschützten Lebensbereichen zugeordnet werden. Die Videoüberwachung, auch die, die in der Öffentlichkeit oder am Arbeitsplatz stattfindet, stellt darum einen schwerwiegenden Eingriff in das Recht der betroffenen Person auf Achtung des Privatlebens und Schutz personenbezogener Daten nach Art. 7, 8 GRC dar.[971] 711

Dagegen wurden andere Verarbeitungsformen, die das Verhalten weniger umfangreich erfassen, sich also auf gewisse Aspekte beschränken, als ein 712

969 EGMR v. 27.9.1999 – 31417/96, Rn. 82 – *Lustig-Prean and Beckett/Vereinigtes Königreich*; EGMR v. 24.6.2004 – 59320/00, GRUR 2004, S. 1051, Rn. 60 – *Hannover/Deutschland*.

970 EuGH, ECLI:EU:C:2011:777, 45 – *ASNEF*.

971 EGMR v. 28.1.2003 – 44647/98, Rn. 59 – *Peck/Vereinigtes Königreich*.

zwar immer noch erheblicher, aber nicht besonders schwerwiegender Eingriff eingeordnet. Ein Beispiel hierfür ist die Ortung einer Person mittels GPS, die nicht den strengen Anforderungen der Telekommunikationsüberwachung (siehe 3.2.3.4.1, S. 293) unterworfen wurde.[972] Der Aufenthaltsort einer Person ist deshalb nicht unproblematisch, liefert aber dennoch kein derart detailliertes Bild über sie, wie etwa eine Videoüberwachung.

713 Dabei ist jedoch zu beachten, dass der Aussagegehalt einzelner Merkmale durch die Kombination mit anderen, ebenfalls für sich genommen wenig aussagekräftigen Merkmalen steigen kann. In der Summe ist der informationelle Eingriff dann weitaus schwerer zu bewerten und auf eine Stufe mit bereits an sich sehr eingriffsintensiven Verarbeitungsmethoden zu stellen. So hat der Europäische Gerichtshof die umfangreiche Verarbeitung von Daten über die Umstände der Kommunikation im Rahmen der Vorratsdatenspeicherung hinsichtlich der Eingriffsschwere mit der Überwachung von – selbst nicht erfassten – Telekommunikationsinhalten gleichgestellt.[973]

3.2.3.5.3 Die Qualität des Personenbezugs und das Interesse hieran

714 Ein Bezug zum Umfang der Verarbeitung besteht auch im Hinblick auf das Merkmal, über das die Informationen auf die betroffene Person bezogen werden. So bedeutet es zwar auch einen Eingriff, wenn personenbezogene Daten nur „am Rande" erhoben werden. Wenn ein solches Vorgehen aber nicht gezielt oder systematisch darauf ausgelegt ist, bestimmte Personen zu identifizieren, kann der damit verbundene Eingriff geringer ausfallen.

715 Der Europäische Gerichtshof für Menschenrechte hat mehrfach zum Ausdruck gebracht, dass er eine Videoüberwachung für eher unproblematisch hält, wenn die Aufnahmen weder aufgezeichnet werden noch systematisch erfolgen.[974] Dabei spielt sicher eine Rolle, dass mit der Speicherung schlicht ein Verarbeitungsschritt wegfällt, an dem wiederum eine Weiter-

---

972 EGMR v. 2.9.2010 – 35623/05, NJW 2011, S. 1333, Rn. 66 – *Uzun/Deutschland*.

973 EuGH, ECLI:EU:C:2014:238, Rn. 27 f., 37 – *Digital Rights Ireland*.

974 EGMR v. 28.1.2003 – 44647/98, Rn. 59 – *Peck/Vereinigtes Königreich*; EGMR v. 5.10.2010 – 420/07, S. 11 – *Köpke/Deutschland*; EGMR v. 18.10.2016 – 61838/10, NJW-RR 2018, S. 294, Rn. 55 – *Vukota-Bojić/Schweiz*; EGMR v. 9.1.2018 – 1874/13, Rn. 63 – *López Ribalda/Spanien*.

verarbeitung anknüpfen könnte. Es geht aber auch darum, dass die Verarbeitungskapazität des Beobachtenden notwendigerweise beschränkt ist, auch und gerade im Hinblick auf die Herstellung des Personenbezugs. Ein Mensch wird in der Regel nicht in der Lage sein, sich viele Gesichter zu merken oder sie in der Kürze der Zeit einer Person zuzuordnen. Ein Personenbezug mag hier zwar vorhanden sein, ist aber denkbar schwach ausgeprägt.

716 Zu dieser Logik passt es, dass die Verarbeitung wieder deutlich problematischer betrachtet wird, wenn sie systematisch erfolgt. Das ist z.B. dann der Fall, wenn nur eine begrenzte Anzahl von Personen beobachtet wird, die u.U. dem Verarbeiter sogar positiv bekannt sind.[975] Entsprechend dürfte die Videoüberwachung von Beschäftigten selbst dann als schwerer Eingriff zu bewerten sein, wenn der Verantwortliche von der Speicherung der Aufnahmen absieht.

717 Bei langlebigen, nicht veränderbaren und hochqualitativen Merkmalen zur Herstellung des Personenbezugs, wie z.B. Fingerabdrücken,[976] verschärft sich die Situation noch zusätzlich. Hier ist es für den Verarbeiter einfacher, eine Vielzahl von Informationen einer Person über einen längeren Zeitraum zuzuordnen. Dadurch steigt die Wahrscheinlichkeit einer besonders umfangreichen Datenverarbeitung. Die Verwendung dieser Merkmale wirkt darum eingriffsvertiefend.

718 Das Argument des ungezielten Personenbezugs lässt sich auch auf die automatisierte Datenverarbeitung ausweiten. Hier dürfte es vor allem um Fälle gehen, in denen personenbeziehbare Daten lediglich technikbedingt mitverarbeitet werden,[977] ohne dass es dem Verantwortlichen gerade auf Informationen einer betroffenen Person ankommt. Der Personenbezug ist hier zwar herstellbar, aber weder gewollt noch erwünscht. Davon ist aber die Frage abzugrenzen, ob sich die Maßnahme gezielt gegen die Person richtet. Eine ungezielte Maßnahme, die auf mehrere – identifizierte oder gut identifizierbare – Person oder gar auf eine unbestimmte Vielzahl solcher Person gerichtet ist, führt nicht dazu, dass der Eingriff geringer zu gewichten wäre. Aufgrund der inhärenten Streubreite ist eher das Gegenteil der Fall (dazu sogleich, 3.2.3.5.4, S. 304).

---

975 Zur Arbeitnehmerüberwachung *Bäcker* 2012, S. 40. Aus demselben Grund macht es für das Bundesarbeitsgericht keinen Unterschied, ob eine analoge oder digitale Aufzeichnungstechnik zum Einsatz kommt, BAG v. 14.12.2004 – 1 ABR 34/03, AP § 87 BetrVG 1972 Überwachung Nr. 42, Rn. 51 (=RDV 2005, S. 216).

976 EuGH, ECLI:EU:C:2013:670, Rn. 58 f. – *Schwarz*.

977 *Bäcker* 2012, Rn. 34.

3.2.3.5.4 Zahl der betroffenen Personen und der Verarbeiter

719 In eine ähnliche Richtung wie der Umfang der Verarbeitung weist das Kriterium der Zahl der betroffenen Personen.[978] So wurde im Fall der Vorratsdatenspeicherung die enorme Streubreite der Maßnahme besonders hervorgehoben. Sie betraf anlass- und unterschiedslos alle Personen und alle elektronischen Kommunikationsmittel.[979] Dieser Argumentation wird entgegengehalten, dass es für den Einzelnen keine Rolle spiele, ob gleichzeitig noch andere von derselben Maßnahme betroffen sind; für die Schwere des Eingriffs sei allein entscheidend, wie er sich auf die betroffene Person selbst auswirke.[980] Für das Argument der Streubreite spricht jedoch, dass diese zwar nicht die individuelle Betroffenheit im Falle der Maßnahme erhöht, sehr wohl aber die Wahrscheinlichkeit, einem solchen Eingriff ausgesetzt zu sein. Das wirkt zumindest abstrakt eingriffsvertiefend.

720 Bei der Eingriffstiefe ist darüber hinaus auch zu beachten, wie vielen Verarbeitern das betreffende Datum zugänglich gemacht wird. Das folgt allein schon aus dem Umstand, dass jede einzelne Verarbeitung selbst einen Eingriff darstellt. Folglich hat der Europäische Gerichtshof wiederholt daran Anstoß genommen, wenn bei Maßnahmen zur Nachvollziehbarkeit der Verwendung öffentlicher Mittel personenbezogene Daten nicht nur den Aufsichtsbehörden, sondern auch der Öffentlichkeit zugänglich gemacht wurden.[981] Aber auch innerhalb der verantwortlichen Stelle wirkt es eingriffsvertiefend, wenn viele Personen Einsicht in die betreffenden Informationen nehmen.[982] Etwas anderes gilt nur, wenn dies gerade der Missbrauchsbekämpfung im Sinne eines Vier-Augen-Prinzips dient.[983]

---

978 EGMR v. 5.9.2017 – 61496/08, ZD 2017, S. 571, Rn. 121 – *Barbulescu v. Romania*.

979 EuGH, ECLI:EU:C:2014:238, S. 57 f. – *Digital Rights Ireland*; ähnlich auch die Argumentation in EuGH, ECLI:EU:C:2011:771, Rn. 49 ff. – *Scarlet*.

980 Minderheitsvotum BVerfG v. 4.4.2006 – 1 BvR 518/02, E 115, S. 320, 373 – *Rasterfahndung II*.

981 EuGH, ECLI:EU:C:2003:294, Rn. 87 – *ORF*; EuGH, ECLI:EU:C:2010:662, Rn. 79 – *Schecke*.

982 EGMR v. 5.10.2010 – 420/07, S. 12 – *Köpke/Deutschland*; EGMR v. 9.1.2018 – 1874/13, Rn. 63 – *López Ribalda/Spanien*.

983 Zu Verfahrensgarantien allgemein EuGH, ECLI:EU:C:2014:238, Rn. 62 – *Digital Rights Ireland*.

3.2.3.5.5 Transparenz und Zuverlässigkeit der Verarbeitung

Die Schwere eines Eingriffs beurteilt sich weiterhin auch danach, wie transparent der Verantwortliche dabei vorgeht. Dieser Grundsatz kommt u.a. in den Betroffenenrechten in Art. 8 Abs. 2 S. 2 GRC zum Ausdruck und ist auch integraler Bestandteil des Rechts auf Schutz personenbezogener Daten.[984] Der Transparenz kommt dabei eine Schlüsselrolle zu, weil die übrigen Betroffenenrechte nur auf der Grundlage entsprechender Informationen über die Verarbeitung ausgeübt werden können.[985] 721

Eine Verarbeitung, die ohne die Kenntnis der betroffenen Person durchgeführt wird – insbesondere eine heimliche Maßnahme[986] – ist darum stets als besonders schwerer Eingriff zu werten. Ausnahmen hiervon, etwa vom Recht auf Auskunft oder von der Pflicht, die betroffene Person im Falle der zweckändernden Übermittlung der Daten zu unterrichten, sind an äußerst strenge Anforderungen geknüpft und nur möglich, wenn der Verantwortliche seine administrative Überforderung nachweist[987] oder die Ausübung seines eigenen Rechts sonst nicht möglich wäre.[988] 722

Die Transparenzpflichten des Verarbeiters sollen die betroffene Person nicht nur in die Lage versetzen, per se rechtswidrige, weil zu umfangreiche Datenverarbeitung zu unterbinden. Die betroffenen Personen können auch ein Interesse an der Verarbeitung ihrer Daten haben. Nicht nur, aber vor allen in diesen Fällen müssen sie darauf hinwirken können, dass die Daten berichtigt werden. Umgekehrt hat der Verantwortliche selbst dafür Rechnung zu tragen, dass die Verarbeitung möglichst fehlerfrei verläuft. Ein Eingriff ist darum als umso tiefer zu bewerten, je höher die Wahrscheinlichkeit ist, dass falsche Aussagen über die Person getroffen werden. 723

---

984 EuGH, ECLI:EU:C:2009:293, Rn. 49 – *Rijkeboer*, der Europäische Gerichtshof spricht hier zwar vom Schutz der Privatsphäre, in der Sache ist damit aber keine Unterscheidung zum Recht aus Art. 8 GRC gemeint.

985 EuGH, ECLI:EU:C:2009:293, Rn. 51 – *Rijkeboer*; EuGH, ECLI:EU:C:2015:638, Rn. 33 – *Bara*.

986 Zur verdeckten Videoüberwachung EGMR v. 5.10.2010 – 420/07 – *Köpke/Deutschland*; EGMR v. 18.10.2016 – 61838/10, NJW-RR 2018, S. 294, Rn. 67 – *Vukota-Bojić/Schweiz*; EGMR v. 9.1.2018 – 1874/13 – *López Ribalda/Spanien*; zur heimlichen Telekommunikationsüberwachung EGMR v. 16.2.2000 – 27798/95 – *Amann/Schweiz*.

987 Zum Auskunftsrecht EuGH, ECLI:EU:C:2009:293, Rn. 66 – *Rijkeboer*; zum Unterrichtungspflicht EuGH, ECLI:EU:C:2015:638, Rn. 40 f. – *Bara*.

988 EGMR v. 5.10.2010 – 420/07, S. 12 f. – *Köpke/Deutschland*; EGMR v. 9.1.2018 – 1874/13, Rn. 67 ff. – *López Ribalda/Spanien*.

Dieses Risiko besteht vor allem beim – in Massenverfahren notwendigen – Einsatz automatisierter Verarbeitung.[989]

3.2.3.5.6 Die möglichen Folgen der Verarbeitung

724 Ein relevantes Kriterium für die Eingriffstiefe sind schließlich die möglichen Folgen, welche die Datenverarbeitung für die betroffene Person nach sich ziehen kann. Die Bewertung steht in einem engen Zusammenhang mit der Position des Verarbeiters. So verfügen nur unmittelbar grundrechtsgebundene staatliche Stellen über die Befugnisse, besonders gravierende Eingriffe wie im Rahmen der Strafverfolgung vorzunehmen. Unabhängig davon kann aber auch bei privaten Verarbeitern weiter nach diesem Kriterium differenziert werden.

725 Für einen Eingriff in das Recht auf Schutz personenbezogener Daten muss es nicht zu einem Nachteil gekommen sein, der ja ohnehin auch selbst einen Eingriff in das spezifische Grundrecht darstellen würde. Es ist deswegen aber nicht etwa egal, welcher Nachteil typischerweise entstehen könnte. Vorfeldschutz bedeutet nur, dass es noch nicht zu einem Eingriff gekommen sein muss. Je schwerer der Eingriff bei ungehinderter Datenverarbeitung ausfiele, desto schwerer ist auch der Eingriff in das Recht auf Schutz personenbezogener Daten zu bewerten.

726 Für die Verarbeitung im privaten Bereich hat diese Überlegung in ausdrücklicher Form bisher nur punktuell Niederschlag gefunden. So hat der Europäische Gerichtshof die Veröffentlichung von Gehaltsdaten auch deshalb kritisch beurteilt, weil er Nachteile für das spätere berufliche Fortkommen der betroffenen Beschäftigten sah.[990] Noch deutlicher wird dies beim Europäischen Gerichtshof für Menschenrechte, demzufolge bei der Prüfung der Zulässigkeit einer Überwachungsmaßnahme u.a. berücksichtigt werden muss, welchen Folgen der betroffene Beschäftigte daraufhin unterworfen ist, insbesondere dann, wenn diese Folgen gerade das Ziel der Maßnahme waren.[991]

727 Dem kann entnommen werden, dass eine Maßnahme, die auf den Verlust des Arbeitsplatzes hinauslaufen kann, grundsätzlich schwerer wiegt, als

989 EuGH, ECLI:EU:C:2017:592, Rn. 173 – *Fluggastdatenabkommen*.
990 EuGH, ECLI:EU:C:2003:294, Rn. 89 – *ORF*.
991 EGMR v. 5.9.2017 – 61496/08, ZD 2017, S. 571, Rn. 121 – *Barbulescu v. Romania*; ähnlich BAG v. 27.7.2017 – 2 AZR 681/16, E 159, S. 380, Rn. 24 (=NZA 2017, S. 1327).

eine, die lediglich die konkrete Ausgestaltung der beruflichen Tätigkeit berührt, etwa weil sie die betrieblichen Abläufe beeinflusst. Umso wichtiger ist es hier, die Verarbeitung – auch durch technische und organisatorische Maßnahmen – an den ggf. weniger sensiblen oder stärker gerechtfertigten Zweck zu binden (siehe 3.4.1.2.4.3, S. 370).[992]

3.2.4 Die unternehmerische Freiheit des Arbeitgebers

Soweit die Interessen des Arbeitgebers dem Recht des Beschäftigten auf Schutz seiner personenbezogenen Daten gegenüberstehen, kommen die EU-Grundrechte zur Anwendung. Für die genuin arbeitsrechtlichen Fragestellungen sind hingegen allein die Grundrechte des Grundgesetzes anwendbar. Hier kann auf Gliederungspunkt 2.2.2, S. 82 verwiesen werden. Für den Arbeitgeber kommen beim Umgang mit Assistenzsystemen drei EU-Grundrechte in Betracht: die Berufsfreiheit nach Art. 15 GRC, die unternehmerische Freiheit nach Art. 16 GRC sowie das Eigentumsrecht nach Art. 17 GRC. 728

Gerade die Berufsfreiheit und die unternehmerische Freiheit sind eng miteinander verwandt; beide schützen den Erwerb. Das Eigentumsrecht nach Art. 17 GRC schützt zwar auch Aspekte der wirtschaftlichen Betätigung, jedoch nur soweit es um das Erworbene und dessen Substanz geht.[993] Aus der Sicht des Arbeitgebers geht es bei der Datenverarbeitung im Kontext der Verwendung von Assistenzsystemen aber in aller Regel nicht um den Substanzerhalt, sondern um die Erwerbstätigkeit selbst.[994] Sollte dem doch nicht so sein, etwa weil eine Maschine zum Schutz vor Verlust oder Beschädigung überwacht wird, stellt dies keine Besonderheit von Assistenzsystemen dar und soll darum in dieser Arbeit nicht vertieft untersucht werden. 729

Der Europäische Gerichtshof ließ vor Inkrafttreten der Charta nicht immer erkennen, ob er einen Unterschied zwischen der Berufsfreiheit und 730

992 Der Europäische Gerichtshof hat im Fall der Vorratsdatenspeicherung gerügt, dass die weitere Nutzung der Daten keiner ausdrücklichen Bindung an die Verhütung oder Verfolgung von Straftaten unterliegt, EuGH, ECLI:EU:C:2014:238, Rn. 60 f. – *Digital Rights Ireland*.

993 *Jarass* 2016, Art. 17 GRC, Rn. 4.

994 Dazu auch 2.2.2.3.2, S. 86.

der unternehmerischen Freiheit machte[995] – was dem Verständnis des Grundgesetzes[996] entspräche. Teilweise hat er sie aber auch als unterschiedlich dargestellt.[997] Wie bei Art. 7 und 8 GRC spricht nichts dagegen, den umfassenden Gewährleistungsgehalt der Art. 15, 16 GRC auf die einzelnen Grundrechte zu verteilen. Zumindest die selbständige wirtschaftliche Tätigkeit ohne Persönlichkeitsbezug,[998] wie sie mit der Arbeitgebereigenschaft verbunden ist, ist allein unter Art. 16 GRC zu fassen.

3.2.4.1 Schutzbereich und Eingriffe

731 Eine der unternehmerischen Freiheit unterfallende Tätigkeit setzt voraus, dass Güter und Dienstleistungen auf einem Markt angeboten werden, ohne dass es auf die Rechtsform und Finanzierungsart der Einheit ankäme, die dies unternimmt. Die Art der Tätigkeit spielt darüber hinaus keine Rolle.[999] Die wirtschaftliche Tätigkeit wird umfassend geschützt, von ihrer Aufnahme bis zur Beendigung und dazwischen in allen Aspekten der Durchführung. Letzteres betrifft insbesondere die Art und Weise, die wirtschaftlichen, finanziellen und technischen Ressourcen einzusetzen,[1000] die Wahl des Vertragspartners[1001] und die Gestaltung der vertraglichen Beziehungen.[1002] Grundrechtsträger können jedenfalls auch juristische Personen des Privatrechts sein.[1003]

732 Die wirtschaftliche Tätigkeit ist nicht gegen jede nachteilige Einwirkung geschützt. Es gilt vielmehr solche Beeinträchtigungen herauszufiltern, die eher dem Marktumfeld als dem Handeln eines Grundrechtsadressaten zu-

995 Tätigkeit einer Kapitalgesellschaft als „Berufsfreiheit" EuGH, ECLI:EU:C:2008:476, Rn. 183 – *FIAMM*; dagegen als „Gewerbefreiheit" EuGH, ECLI:EU:C:2003:548, Rn. 53 – *Lufthansa*.

996 *Scholz,* in: Maunz/Dürig 2015, Lfg. 47, Art. 12 GG, Rn. 18.

997 EuGH, ECLI:EU:C:1991:65, Rn. 72 – *Zuckerfabrik*; EuGH, ECLI:EU:C:2004:497, Rn. 51 – *Spanien/Parlament*.

998 Für dieses zusätzliche Abgrenzungskriterium *Bernsdorff,* in: Meyer/Hölscheidt 2019, Art. 16 GRC, Rn. 8; a.A. *Jarass* 2016, Art. 16 GRC, Rn. 4a.

999 Zum Ganzen *Jarass* 2016, Art. 16 GRC, Rn. 7 f.

1000 EuGH, ECLI:EU:C:2014:192, Rn. 49 – *UPC*.

1001 EuGH, ECLI:EU:C:2013:521, Rn. 32 – *Alemo-Herron*.

1002 Zum Vertragsinhalt EuGH, ECLI:EU:C:1999:479, Rn. 99 – *Spanien/Kommission*; zum Ganzen *Bernsdorff,* in: Meyer/Hölscheidt 2019, Art. 16 GRC, Rn. 11 f.; *Jarass* 2016, Art. 16 GRC, Rn. 9.

1003 *Bernsdorff,* in: Meyer/Hölscheidt 2019, Art. 16 GRC, Rn. 18; *Jarass* 2016, Art. 16 GRC, Rn. 11; *Ruffert,* in: Calliess/Ruffert 2016, Art. 16 GRC, Rn. 3.16.

zurechnen sind oder die unternehmerische Freiheit nur reflexhaft und nur am Rande berühren. Für die Berufsfreiheit leistet das Merkmal der berufsregelnden Tendenz diese Filterfunktion (siehe 2.2.2.4, S. 87), für die unternehmerische Freiheit nach Art. 16 GRC verwendet der Europäische Gerichtshof die Formel der „hinreichend direkte[n] und bedeutsame[n] Auswirkungen auf die freie Berufsausübung“,[1004] die eine Maßnahme aufweisen müsse.

733 Eine solche Auswirkung kann dann angenommen werden, wenn eine Regelung den in Rede stehenden Nachteil bezweckt oder unmittelbar bewirkt.[1005] Im Falle des Beschäftigtendatenschutzes wäre dies die eingeschränkte Verarbeitbarkeit personenbezogener Beschäftigtendaten, die gerade den Schutz der Persönlichkeitsrechte der Beschäftigten bezweckt und die Beschränkung für den Arbeitgeber unmittelbar bewirkt.

3.2.4.2 Rechtfertigung

734 Ein Eingriff in die unternehmerische Freiheit kann nach den allgemeinen Bedingungen für die Einschränkung von Grundrechten nach Art. 52 Abs. 1 GRC gerechtfertigt werden. Er unterliegt lediglich einem einfachen Gesetzesvorbehalt und kann insbesondere durch das Recht der Betroffenen auf Schutz ihrer personenbezogenen Daten legitimiert werden. Als gesetzliche Regelung gelten dabei auf Unionsebene u.a. Verordnungen[1006] und Richtlinien[1007]. Die Datenschutz-Grundverordnung mit ihren Anforderungen an den für die Datenverarbeitung verantwortlichen Arbeitgeber ist somit eine taugliche Eingriffsgrundlage.

735 Der Wesensgehalt des Grundrechts, der nach Art. 52 Abs. 1 S. 1 GRC zu achten ist, kann z.B. dann betroffen sein, wenn es einem Unternehmer schon grundsätzlich verwehrt ist, die Entwicklung der Faktoren, die über die Arbeitsbedingungen seiner Beschäftigten bestimmen, auszuhandeln,[1008] er also in wesentlichen Bereichen seiner wirtschaftlichen Tätigkeit fremdbestimmt wäre. Der Beschäftigtendatenschutz berührt diesen

1004 EuGH, ECLI:EU:C:2004:552, Rn. 49 – *Springer*.
1005 EuGH, ECLI:EU:C:1998:172, Rn. 28 – *Metronome*.
1006 EuGH, ECLI:EU:C:2010:662, Rn. 66 – *Schecke*; EuGH, ECLI:EU:C:2013:670, Rn. 35 – *Schwarz*.
1007 EuGH, ECLI:EU:C:2014:238, Rn. 39 – *Digital Rights Ireland*; EuGH, ECLI:EU:C:2016:84, Rn. 51 – *J.N.*
1008 EuGH, ECLI:EU:C:2013:521, Rn. 33 ff. – *Alemo-Herron*.

Wesensgehalt nicht. Durch sein Regelungskonzept, an arbeitsvertragliche Pflichten anzuknüpfen (siehe 3.2.2.5.1, S. 279), passt es sich an die konkreten Gegebenheiten und Bedürfnisse an. Darüber hinaus kann der Unternehmer durch Maßnahmen, die den Personenbezug von Daten entfallen lassen (siehe 3.3.4.4, S. 341), das Ausmaß der an ihn gestellten Anforderungen selbst beeinflussen.

736 Die Formulierung in Art. 16 GRC, die Freiheit werde nach dem Unionsrecht und den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten anerkannt, macht deutlich, dass es sich hierbei um ein normgeprägtes Grundrecht handelt. Der Gesetzgeber verfügt darum mehr noch als bei anderen Grundrechten über einen weiten Regelungs- und Ausgestaltungsspielraum. Das bedeutet aber nicht, dass Eingriffe in die unternehmerische Freiheit ohne Weiteres zu rechtfertigen wären. Gerade solche Eingriffe, die nah an dem beschriebenen Wesensgehalt liegen oder Überschneidungen mit der – im Gegensatz zu Art. 16 GRC – nicht normgeprägten Berufsfreiheit aufweisen, bedürfen einer gesteigerten Rechtfertigung.[1009]

3.2.5 Ausgleich der grundrechtsgeschützten Positionen

737 Im Verhältnis von selbst nicht grundrechtsgebundenen Privaten wirken auch die EU-Grundrechte nicht direkt. Sie legen aber eine objektive Wertordnung fest, von der auch das Verhältnis zwischen Privaten nicht unbeeinflusst bleibt. Die grundsätzliche Verschiedenheit des Verhältnisses Bürger-Bürger zu dem Verhältnis Staat-Bürger hat Konsequenzen für die Art und Weise, wie Grundrechte hier wirken, sowohl im Hinblick auf die „Breite" der Bindung als auch auf deren „Tiefe".

3.2.5.1 Konsequenzen grundsätzlich verschiedener Grundrechtsbindungen

738 In der Konsequenz seiner unmittelbaren Grundrechtsgebundenheit gelten für den Staat bei Eingriffen in das Recht auf Schutz personenbezogener Daten der Gesetzesvorbehalt, eine enge Zweckbindung und teilweise strenge Verfahrensvorschriften. Im Verhältnis Privater zueinander gilt lediglich der Vorrang des Gesetzes. Diese Gesetze müssen die Union oder

1009 Zum Ganzen *Jarass* 2016, Art. 16 GRC, Rn. 21.

die Mitgliedstaaten zwar schaffen, wollen sie ihren Schutzpflichten für die betroffenen Personen[1010] nachkommen. Die Pflicht zum staatlichen Eingreifen ändert aber nichts daran, dass die Regelungen zur privaten Datenverarbeitung – anders als im Fall der öffentlichen Datenverarbeitung – keine per se notwendigen Erlaubnistatbestände darstellen, sondern im Gegenteil Einschränkungen für die private Datenverarbeitungsfreiheit.[1011]

739 Dieser Grundsatz wird durch die sekundärrechtlichen bzw. einfachgesetzlichen Vorgaben in der Datenschutz-Grundverordnung und im Bundesdatenschutzgesetz umgekehrt. Die private Datenverarbeitung im Beschäftigungsverhältnis unterliegt gemäß Art. 4 Abs. 1, Art. 6 Abs. 1 DS-GVO und ergänzend § 26 Abs. 7 BDSG 2018 in all ihrem Formen einer prinzipiellen Rechtfertigungsanforderung. In der „Breite" besteht hier folglich kein Unterschied zum staatlichen Handeln. Dass das Regelungskonzept des Datenschutzes dennoch nicht primär- bzw. verfassungswidrig ist, liegt daran, dass sich die Grundrechtsbindung in der „Tiefe", also hinsichtlich der Frage, wie eng die mittelbare Drittwirkung ausfällt, vom staatlichen Handeln unterscheidet.

740 Die lediglich mittelbare Wirkung der Grundrechte im Verhältnis Privater untereinander führt dazu, dass die Grundrechtsbindung hier insgesamt weniger eng und in der Folge die Anforderungen – insbesondere die an die Bestimmtheit des Verarbeitungszwecks[1012] – weniger streng ausfallen.[1013] Das Handeln Privater ist anders als das öffentlicher Stellen nicht davon abhängig, dass ihnen vom Gemeinwesen eine Aufgabe oder – im Falle von Eingriffen – eine Befugnis zugewiesen wird.[1014] Folglich genießen private Datenverarbeiter grundsätzlich die Freiheit, selbst gesetzte Zwecke zu verfolgen. Dies spiegelt sich im Auffangtatbestand des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO wieder. Öffentliche Datenverarbeiter genießen diese Freiheit nicht. Darüber hinaus können Private ihre Vertragsfreiheit dazu nutzen, um die Grundlage der Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO einvernehmlich zu schaffen.

1010 EGMR v. 5.10.2010 – 420/07, S. 9 f. – *Köpke/Deutschland*; EGMR v. 5.9.2017 – 61496/08, ZD 2017, S. 571, Rn. 111 ff. – *Barbulescu v. Romania*; EGMR v. 9.1.2018 – 1874/13, Rn. 60 – *López Ribalda/Spanien*.

1011 Zum Ganzen bezogen auf die Grundrechte des Grundgesetzes *Grimm*, JZ 2013, S. 585, 588; *Masing*, NJW 2012, S. 2305, 2306 f. Dieses Prinzip lässt sich auch auf europäischer Ebene anwenden, *Masing*, NJW 2012, S. 2305, 2310.

1012 *Masing*, NJW 2012, S. 2305, 2307.

1013 Für die Grundrechte des Grundgesetzes *Bäcker* 2012, S. 28 f. Zur Vergleichbarkeit mit Unionsrecht *Masing*, NJW 2012, S. 2305, 2310.

1014 *Grimm*, JZ 2013, S. 585, 587.

741 Eine ähnliche Privilegierung gilt für die Zweckbindung. Die Zweckänderung unterliegt zwar keinen grundsätzlich anderen Mechanismen als bei öffentlichen Stellen. Die Weiterverarbeitung selbst kann aber ebenso zu selbst- bzw. einvernehmlich gesetzten Zwecken erfolgen.

3.2.5.2 Die Abwägung mit Wirtschaftsgrundrechten im Allgemeinen

742 Im Verhältnis Privater untereinander geht es nicht um die Rechtfertigung von Grundrechtseingriffen, sondern um den Ausgleich grundrechtsgeschützter Positionen. Der Europäische Gerichtshof folgt hier dem Prinzip der praktischen Konkordanz. Die Grundrechte sind möglichst in Einklang miteinander zu bringen,[1015] wenigstens ist aber zwischen ihnen ein angemessenes Gleichgewicht herzustellen.[1016] Dieses Gleichgewicht ist gestört, wenn ein Grundrecht ganz oder fast vollständig zurückweichen muss. Der Europäische Gerichtshof spricht dann von einer „qualifizierten Beeinträchtigung", die sich nicht mehr unter Berufung auf das konfligierende Grundrecht rechtfertigen lässt.[1017]

743 Betrachtet man die Grundrechte auf Schutz personenbezogener Daten in Art. 8 GRC und auf unternehmerische Freiheit in Art. 16 GRC, so fällt auf, dass lediglich ersteres mit Art. 8 Abs. 2 und 3 GRC über spezifische Schrankenbestimmungen verfügt. Daraus lässt sich zwar kein generelles Rangverhältnis der Grundrechte zueinander ableiten. Es bringt aber dennoch zum Ausdruck, dass der Persönlichkeitsschutz einen hohen Stellenwert einnimmt.[1018]

744 Der Europäische Gerichtshof hat bisher nur in Ansätzen konkretisiert, wie er das Recht auf Schutz personenbezogener Daten im Verhältnis zu Wirtschaftsgrundrechten gewichtet. Klar ist aber immerhin, dass er unterschiedslos wirkende Maßnahmen ablehnt, weil diese auch und vor allem Personen betreffen, die diese Beeinträchtigung ihres Persönlichkeitsrechts nicht in zurechenbarer Weise verursacht haben. Internetzugangsanbieter und Hosting-Anbieter sind darum nicht verpflichtet, zum Schutz von Ur-

1015 EuGH, ECLI:EU:C:2013:28, Rn. 60 – *Sky Österreich*.
1016 EuGH, ECLI:EU:C:2011:771, Rn. 45 – *Scarlet*; EuGH, ECLI:EU:C:2012:85, Rn. 42 f. – *SABAM*; EuGH, ECLI:EU:C:2013:28, Rn. 60 – *Sky Österreich*.
1017 EuGH, ECLI:EU:C:2011:771, Rn. 48 – *Scarlet*; EuGH, ECLI:EU:C:2012:85, Rn. 46 – *SABAM*; EuGH, ECLI:EU:C:2015:485, Rn. 35 – *Coty*.
1018 *Pötters* 2013, S. 297.

heberrechten präventiv wirkende Filtersysteme einzurichten, die u.a. unterschiedslos auf alle ihre Kunden angewendet würden.[1019]

Ähnlich ließe sich auch die Abwägung im Urteil zum Recht auf Löschung gegenüber einem Suchmaschinenbetreiber verstehen. Der Suchmaschinenbetreiber, dem die Privilegierung für Presse-Archive verwehrt wurde, verarbeitete und veröffentlichte die Daten in seinem Index gewissermaßen „einfach so", d.h. ohne, dass ein Informationsinteresse der Öffentlichkeit an einer längst nicht mehr aktuellen Information erkennbar gewesen wäre. Die wirtschaftlichen Interessen des Suchmaschinenbetreibers genügten angesichts der Schwere des Eingriffs allein nicht.[1020] 745

Das Pendel kann aber auch in die Gegenrichtung ausschwingen. Dem Geheimhaltungsinteresse der betroffenen Person darf kein unbedingter und unbegrenzter Vorrang vor den Wirtschaftsgrundrechten gegeben werden. Auskunftsansprüchen über den Inhaber eines Bankkontos, das im Zusammenhang mit der Verletzung geistigen Eigentums verwendet wurde, kann darum nicht ohne nähere Begründung das Bankgeheimnis entgegengehalten werden.[1021] 746

3.2.5.3 Besonderheiten des Beschäftigungsverhältnisses

Die bisherige Rechtsprechung des Europäischen Gerichtshofs zeigt, dass sich zumindest schwerwiegende Grundrechtsbeeinträchtigungen, wenn überhaupt, dann nur mit einem spezifischen, d.h. aus der konkreten Situation begründeten wirtschaftlichen Interesse ausgleichen lassen. Dies deckt sich mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu verdeckten Überwachungsmaßnahmen des Arbeitgebers. Im Einklang mit der Rechtsprechung des Bundesarbeitsgerichts fordert der Europäische Gerichtshof für Menschenrechte hierfür u.a. einen konkreten Verdacht gegen den betroffenen Beschäftigten, die Interessen des Arbeitgebers – in den entschiedenen Fällen durch eine Straftat zu seinem Nachteil – massiv verletzt zu haben.[1022] Im Umkehrschluss werden also Maßnah- 747

1019 EuGH, ECLI:EU:C:2011:771, Rn. 50 f. – *Scarlet*; EuGH, ECLI:EU:C:2012:85, Rn. 49 – *SABAM*.

1020 EuGH, ECLI:EU:C:2014:317, S. 97 f. – *Google Spain*.

1021 EuGH, ECLI:EU:C:2015:485, Rn. 35 ff. – *Coty*.

1022 EGMR v. 5.10.2010 – 420/07, S. 11 – *Köpke/Deutschland*; EGMR v. 9.1.2018 – 1874/13, Rn. 68 – *López Ribalda/Spanien*; BAG v. 27.3.2003 – 2 AZR 51/02, E 105, S. 356, Rn. 28 (=NZA 2003, S. 1193); BAG v. 22.9.2016 – 2 AZR 848/15,

men gegen Betroffene, die hierzu keine Veranlassung gegeben haben, in der Regel abgelehnt.

748 Im Übrigen muss bei den für die allgemeine Abwägung herangezogenen Fallkonstellationen jedoch beachtet werden, dass es sich überwiegend um Extremsituationen handelt. Die Grenze zur Unzulässigkeit privater Datenverarbeitung wird man zumindest im Beschäftigungsverhältnis nicht erst dort ziehen können, wo das Recht der betroffenen Person auf Schutz personenbezogener Daten nach Art. 8 GRC andernfalls nahezu vollständig weichen müsste. Auch die konzeptionelle Andersartigkeit der Grundrechtsbindung Privater ändert nichts daran, dass auch die von ihnen betriebene Datenverarbeitung die Entfaltungsfreiheit der betroffenen Person erheblich gefährden kann. Dies gilt insbesondere in Situationen, in denen das Machtverhältnis rein tatsächlich oder – wie im Fall des Weisungsrechts des Arbeitgebers – sogar rechtlich begründet sehr ungleich ausfällt.[1023]

749 Beschäftigte sind zur Sicherung ihrer Existenzgrundlage in aller Regel auf die Tätigkeit beim Arbeitgeber angewiesen und können sich dessen Maßnahmen darum nicht effektiv entziehen.[1024] Hieraus erwachsen dem Staat gesteigerte Schutzpflichten, die sich auch in einer strengeren (mittelbaren) Grundrechtsbindung des Arbeitgebers niederschlagen (siehe 2.2.1.2, S. 80). Man kann sich darum nicht darauf beschränken, die Beschäftigten vor einer besonders schwerwiegenden Beeinträchtigung ihrer Grundrechte zu schützen. Das Verhältnismäßigkeitsprinzip gilt für sämtliche Datenverarbeitungsvorgänge, auch für solche, denen für sich genommen kein gesteigertes Gefährdungspotenzial attestiert wird.

3.3 Anwendbarkeit des sekundärrechtlichen Datenschutzrechts

750 Der sekundärrechtliche bzw. einfachgesetzliche Schutz richtet sich überwiegend nach der Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz. Darüber hinaus bestehen noch einzelne speziellere Datenschutzvorschriften, die für den hier betrachteten Bereich des Beschäftigtendatenschutzes in der privatwirtschaftlich organisierten Industrie 4.0 aber keine Rolle spielen.

E 156, S. 370, Rn. 30 (=NZA 2017, S. 112); BAG v. 20.10.2016 – 2 AZR 395/15, E 157, S. 69, Rn. 22 (=NZA 2017, S. 443).

1023 *Bäcker* 2012, S. 29; *Grimm,* JZ 2013, S. 585, 587.

1024 *Bäcker* 2012, S. 29.

3.3.1 Personenbezogene Daten

Allen Datenschutzregelungen gemein ist, dass sie – wie z.B. Art. 2 Abs. 1 DS-GVO bestimmt – lediglich auf die Verarbeitung personenbezogener Daten anwendbar sind. Insofern entspricht ihr Anwendungsbereich dem sachlichen Schutzbereich des Grundrechts auf Schutz personenbezogener Daten in Art. 8 GRC (siehe 3.2.3.3.1, S. 290). 751

Der Begriff des personenbezogenen Datums wird in Art. 4 Nr. 1 DS-GVO definiert. Danach bezeichnet dieser Ausdruck alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. 752

3.3.1.1 Daten statt Informationen

Der Anknüpfungspunkt des Datums hat verschiedentlich für Kritik gesorgt und kann tatsächlich etwas verwirren. Beim Datenschutz geht es im Kern nicht um den Schutz von Daten, sondern um den Schutz der informationellen Selbstbestimmung. Daraus kann aber nicht der Schluss gezogen werden, der Begriff des Datenschutzes sei falsch gewählt.[1025] Informationen sind auf der Bedeutungsebene zu verorten, Daten hingegen lediglich auf der Zeichenebene. Über der Bedeutungsebene steht noch die – für den Datenschutz allerdings irrelevante – Ebene des Wissens, das entsteht, wenn Informationen in einen Kontext gesetzt werden. Unter der Datenebene steht die Stoffebene des Datenträgers, auf dem die Zeichen materialisiert sein müssen, um überhaupt als Daten bezeichnet werden zu können.[1026] Diese Ebenen bauen logisch, aber nicht zwingend technisch aufeinander auf. 753

1025 So aber *Härting/Schneider*, CR 2015, S. 819 f.; *Veil* 2018.

1026 Zur Abgrenzung von Informationen, Daten und Datenträgern *Zech*, CR 2015, S. 137, 138.

754 Informationen und Wissen müssen als solche zwar materialisiert sein, um überhaupt zu existieren, es genügt aber, wenn dies nur flüchtig oder für andere nicht wahrnehm- oder auslesbar geschieht. Je nach dem Zweck der Informationsregulierung werden hier unterschiedliche Anforderungen gestellt. So ist im Urheberrecht zwar vom Werk in seinem immateriellen Gehalt die Rede, der sich nicht zwingend in einem Werkträger materialisieren muss. Der immaterielle Gehalt kann aber nur geschützt werden, wenn er sich in irgendeiner Art und Weise geäußert hat. Selbst eine Rede nach § 2 Abs. 1 Nr. 1 UrhG muss gesprochen werden und sich so mindestens in den in Schwingung versetzten Luftmassen – wenn auch nur kurz – materialisieren.

755 Aus Sicht der informationellen Selbstbestimmung reicht im Grunde genommen schon die Materialisierung im Gehirn des Informierten aus, damit sich die hemmende Wirkung auf die Selbstbestimmung des Individuums entfaltet. Bei einer solchen nicht wahrnehm-, geschweige denn auslesbaren Verstofflichung ist aber die Gefahrenschwelle noch nicht überschritten, ab der der Gesetzgeber eingreifen darf, wahrscheinlich sogar eingreifen kann. Die Gedanken sind bekanntermaßen frei. Die Gefahrenschwelle wird erst überschritten, wenn Informationen auf der Zeichenebene – also in einer natürlich wahrnehmbaren oder technisch auslesbaren Form – in Daten festgehalten werden.[1027] Dazu werden sie typischerweise aufgeschrieben, elektronisch gespeichert oder im Falle der Langzeitarchivierung auf Mikrofilm abgelichtet. Es ergibt also durchaus Sinn, zum Schutz der informationellen Selbstbestimmung erst an personenbezogene Daten und nicht bereits an personenbezogene Informationen anzuknüpfen.

3.3.1.2 Informationen über eine Person

756 Die Tatbestandsvoraussetzung der Information bereitet selten Probleme. Sie umfasst sämtliche denkbaren Angaben, seien sie richtig oder falsch, Meinung oder Tatsache, gesicherte Erkenntnis oder lediglich Wahrscheinlichkeitswert. Auch auf den Aussagegehalt, insbesondere die Sensibilität der jeweiligen Information, kommt es nicht an.[1028] Ein Abgrenzungsbe-

1027 *Bäcker* 2012, S. 23 f.

1028 Zum Begriff des personenbezogenen Datums auf der Grundlage der Datenschutzrichtlinie EuGH, ECLI:EU:C:2014:238, Rn. 33 – *Digital Rights Ireland*; EuGH, ECLI:EU:C:2015:650, Rn. 87 – *Schrems*; EuGH, ECLI:EU:C:2017:592, Rn. 124 – *Fluggastdatenabkommen*; noch zum Grundsatz-Grundrecht, abgeleitet

darf besteht hier lediglich zu Vorgängen und Zuständen in der realen Welt, die nicht im weitesten Sinne informationstechnisch erfasst sind.[1029] Aus der Konzeption des Rechts auf Schutz personenbezogener Daten nach Art. 8 GRC ergibt sich nämlich, dass die betreffende Information in irgendeiner Form codiert und dadurch verarbeitbar sein muss (siehe 3.3.1.1, S. 315). Für die Industrie 4.0, die sich gerade durch die umfangreiche Datenerfassung auszeichnet, spielt dies aber keine Rolle.

Ungleich bedeutsamer ist dagegen die Frage, ob die betreffende Information eine solche über eine natürliche Person ist. So geht es in weiten Bereichen der Industrie 4.0 lediglich darum Maschinendaten zu erfassen, die nicht notwendigerweise Informationen über eine natürliche Person enthalten müssen. Hier ist eine genaue Abgrenzung nur schwer zu ziehen. 757

3.3.1.2.1 Eindeutige Fälle: Gesamtheit von Personen und Inhaltselement

Unproblematisch keine personenbezogenen Daten sind Informationen, die Aussagen über eine Gesamtheit von Personen enthalten, etwa über die gesamte Belegschaft oder eine Abteilung. Solche aggregierten Daten enthalten keine Informationen über eine Person, geschweige denn über eine identifizierbare Person und sind darum in keiner Weise datenschutzrelevant.[1030] In vielen Fällen wird sich ein Datum aber doch einer – nicht notwendigerweise identifizierbaren, d.h. womöglich unbekannten – natürlichen Person zuordnen lassen. Dann stellt sich die Frage, ob dieses Datum Informationen über diese Person enthält. 758

---

aus Art. 8 EMRK, EuGH, ECLI:EU:C:2003:294, Rn. 75 – *ORF*; *Klar/Kühling,* in: Kühling/Buchner 2018, Art. 4 Nr. 1 DS-GVO, Rn. 8 ff.

1029 Zum alten Recht *Dammann,* in: Simitis 2014, § 3 BDSG, Rn. 5 Diese Erwägungen sind im Hinblick auf das Datum als Anknüpfungspunkts des grundrechtlichen Schutzes (siehe 3.2.3.3.1, S. 290) weiterhin relevant.

1030 Hierzu eingängig *Roßnagel/Scholz,* MMR 2000, S. 721, 723: „Enthalten Daten keine Angaben über eine Person, so sind sie in keiner Weise datenschutzrelevant. Es hat auch keinen Sinn, solche Daten anonym zu nennen. Es sind keine Angaben zu einer Person, die "dem Namen nach unbekannt" ist, sondern Angaben, die zu keiner Person gehören. Unzutreffend ist es daher, wenn in der datenschutzrechtlichen Literatur solche Daten als anonyme Daten bezeichnet werden oder gar Anonymität für Daten ohne Personenangaben vorbehalten wird. Anonyme Daten enthalten somit mindestens eine Einzelangabe über eine Person, ohne dass die Person allerdings bekannt ist."

759 Ebenso unproblematisch – jedoch in die andere Richtung – sind Informationen, die ein sog. Inhaltselement aufweisen. Damit sind offensichtliche Fälle gemeint, in denen etwa Daten einem Kundenkonto oder einer Personalakte zugewiesen werden. Hier liegen Daten über eine Person vor, unabhängig davon, zu welchem Zweck die Informationen verwendet werden, oder ob dies Auswirkungen für die betroffene Person haben kann.[1031]

3.3.1.2.2 Grenzfälle: Zweckelement und Ergebniselement

760 Für die Grenzfälle, in denen solch ein klares Inhaltselement fehlt, soll es darauf ankommen, ob die Informationen ein Zweckelement oder ein Ergebniselement aufweisen.[1032] Die Informationen beziehen sich hier meist auf Gegenstände, die wiederum ganz oder teilweise einer Person zugeordnet sind, etwa weil die Person die Gegenstände ausschließlich oder zusammen mit anderen nutzt. Vergleichsweise einfach ist dabei noch das Zweckelement zu bestimmen. Es liegt vor, wenn diese doppelte Zuordnung – Information zu Gegenstand zu Person – vorgenommen werden soll, etwa um die Person zu beurteilen, sie in irgendeiner Weise zu behandeln oder ihr Verhalten zu beeinflussen.[1033] In solchen Situationen kommt es dann auch nicht mehr entscheidend darauf an, dass die Information sich auf eine andere Person beziehen könnte. Soll sie dazu verwendet werden, um eine auf die Person gerichtete Maßnahme zu veranlassen, stellt spätestens dies den Bezug her.

761 Besonders problematisch ist der Personenbezug, wenn er lediglich auf einem Ergebniselement beruht. Das wäre der Fall, wenn die doppelte Zuordnung zwar nicht bezweckt wird, aber doch möglich ist.[1034] Das wird man bei einigem Aufwand zumindest im Beschäftigungskontext von nahezu jeder Information behaupten können, die innerhalb eines Betriebs anfällt. Aus der Verbindung protokollierter Maschinenzustände, ggf. dokumentierten Arbeitsaufträgen und Dienstplänen ließe sich wohl in vielen Punkten der Arbeitsalltag eines Beschäftigten rekonstruieren.

1031 *Art. 29-Grp.*, WP 136, S. 11.
1032 *Art. 29-Grp.*, WP 136, S. 10 ff.; bezugnehmend darauf *Eßer*, in: Auernhammer 2020, Art. 4 DS-GVO, Rn. 9; *Klar/Kühling*, in: Kühling/Buchner 2018, Art. 4 Nr. 1 DS-GVO, Rn. 14.
1033 *Art. 29-Grp.*, WP 136, S. 11 ff.
1034 *Art. 29-Grp.*, WP 136, S. 13 f.

Der Anwendungsbereich des Datenschutzrechts sollte aber nicht bereits bei jeder noch so entfernten Möglichkeit eines Personenbezugs eröffnet sein. Schon das Grundkonzept des Rechts auf Schutz personenbezogener Daten nach Art. 8 GRC entspricht einem risikobasierten Ansatz, nämlich der Annahme, dass nur in Daten materialisierte Informationen aufgrund ihrer besseren Verarbeitbarkeit regulierungsbedürftig sind (siehe 3.2.3.3.1, S. 290). Gleiches muss für den Personenbezug gelten. Wenn es anhand der Daten nur entfernt möglich ist, eine Aussage über eine Person zu treffen, und wenn diese Möglichkeit auch nicht durch eine entsprechende Zwecksetzung erhöht wird, ist es nicht gerechtfertigt, die – gerade was die Informations- und Dokumentationspflichten betrifft – teilweise undifferenzierten Regelungen des Datenschutzes anzuwenden. 762

Ein Ergebniselement kann daher nur bejaht werden, wenn eine nicht nur theoretische Möglichkeit besteht, dass die zu beurteilende Information für individuelle Maßnahmen gegenüber einer Person herangezogen werden. Die *Art. 29-Datenschutzgruppe* nennt hier das Beispiel einer Ortungsanlage für Taxis, mit der auch die Leistung der Taxifahrer kontrolliert werden könnte, etwa ob sie Geschwindigkeitsbegrenzungen einhalten und geeignete Fahrtstrecken auswählen. Diese Kontrolle dürfte hier schon deswegen nicht fernliegend sein, weil die Auswertungsmöglichkeit für das Taxiunternehmen und der damit verbundene Nutzen auf der Hand liegen und es folglich nicht unwahrscheinlich ist, dass die Daten Begehrlichkeiten wecken. Insofern wird man hier von Informationen über eine Person ausgehen müssen. Dies gilt aber nicht wegen der abstrakten Möglichkeit, sondern wegen des Ergebnisses der – wenngleich hier nur kursorischen – Risikoanalyse. 763

3.3.1.3 Die Identifikation einer Person

Die Kernfrage für das Vorliegen personenbezogener Daten, unter welchen Umständen eine Person identifiziert oder identifizierbar ist, ist umstritten. Eine Unterscheidung der Merkmale identifiziert und identifizierbar ist zwar aufgrund ihrer Gleichrangigkeit nicht geboten.[1035] Für die Anwendbarkeit des Datenschutzrechts ist vielmehr die Abgrenzung von immer noch zu nicht mehr identifizierbaren Personen entscheidend. Ohne die 764

1035 *Klar/Kühling*, in: Kühling/Buchner 2018, Art. 4 Nr. 1 DS-GVO, Rn. 17.

Anforderungen an die Identifikation zu kennen, können jedoch auch keine Aussagen über die Identifizierbarkeit getroffen werden.

765 Eine Person ist identifiziert, wenn ihre Identität[1036] bekannt ist. Der Verordnungsgeber fasst den Betriff sehr weit und spricht in Art. 4 Nr. 1 DS-GVO von der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität. Für die Frage, ab welchem Punkt man eine Person als identifiziert betrachten kann, lässt sich aus dieser Aufzählung aber nichts ableiten. Sie spiegelt lediglich den weiten Schutzbereich des Rechts auf Schutz personenbezogener Daten in Art. 8 GRC wieder und macht deutlich, dass Informationen aus sämtlichen Lebensbereichen personenbezogene Daten sein können – nicht aber, unter welchen Umständen sie es tatsächlich sind.

3.3.1.3.1 Informationen und Merkmale

766 Die Identifikation einer Person kann gemäß Art. 4 Nr. 1 DS-GVO auf zwei verschiedenen Wegen erfolgen, durch die Zuordnung zu einer Kennung oder zu einem oder mehreren besonderen Merkmalen. Als Beispiel für Kennungen zählt die Verordnungen Namen, Kennnummern, Standortdaten und Online-Kennungen auf. Ihnen gegenüber stehen Merkmale, die sich anders als Kennungen zusätzlich auf eine Identitätsform beziehen, also Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der betreffenden natürlichen Person sein müssen. Bei Kennungen wird auf diese Anforderung verzichtet, weil sie anders als Merkmale von sich aus bereits eindeutig und darum für die Person typisch sind. Merkmale können typisch sein, sind es aber nicht von sich heraus. So verstanden bilden Kennungen einer Untergruppe der besonderen Merkmale.

767 Zählt man – wie im Folgenden – Kennungen zu den Merkmalen, kann man begrifflich und funktional zwischen Merkmalen auf der einen und Informationen auf der anderen Seite unterscheiden. Erstere werden zur Identifizierung der Person verwendet, letztere dazu, Aussagen über die identifizierte Person zu treffen.

768 Diese Abgrenzung ist hinsichtlich des auf Daten beschränkten Schutzbereichs des Rechts auf Schutz personenbezogener Daten nach Art. 8 GRC relevant (siehe 3.2.3.3.1, S. 290). Informationen über eine Person müssen

1036 Zum Begriff der Identität *Hornung* 2005, S. 30 ff.

als Daten codiert vorliegen bzw. erhoben werden. Es genügt nicht, wenn sie lediglich „im Kopf" des Verarbeiters oder seiner Mitarbeiter existieren. Bei Merkmalen ist es hingegen egal, wie sie beim Verantwortlichen vorliegen. Schon das ansonsten undokumentierte Wissen eines Mitarbeiters kann ausreichen, eine Person zu identifizieren. Auch in diesem Fall muss die Identifizierung aber hinreichend wahrscheinlich sein (siehe 3.3.1.4.1, S. 323).

Diese Abgrenzung ist einseitig durchlässig. Die betroffene Person kann an- 769
hand der über sie getätigten Aussage identifiziert werden, umgekehrt kann das sie identifizierende Merkmal auch eine Aussage über die betroffene Person treffen. Ein codiertes Datum kann darum beides sein, Information und Merkmal. Eine nicht codierte Information kann dagegen allenfalls ein identifizierendes Merkmal sein.

3.3.1.3.2 Anforderungen an die Merkmale

Die Grundvoraussetzung für die Identifikation einer Person ist deren Un- 770
terscheidbarkeit gegenüber anderen Personen. Dass dies allein nicht reicht, liegt jedoch auf der Hand. Diese Anforderung wäre nämlich schon bei schlichtem Durchnummerieren der Personen erfüllt. Die Merkmale müssen vielmehr eine gewisse Qualität aufweisen. Da es sich bei der Identifikation um den Referenzpunkt des Begriffs des personenbezogenen Datums handelt, also um den Punkt, ab dem eine Person nicht mehr nur identifiziert werden kann – was für einen Personenbezug ebenfalls ausreicht –, sondern bereits identifiziert worden ist, darf hier kein geringer Maßstab angelegt werden.

Für die Identifikation einer Person genügt es demnach nicht, sie lediglich 771
aus einer Menge herausgreifen zu können.[1037] Man wird vielmehr Merkmale verlangen müssen, die aus sich selbst heraus[1038] und kontextunabhängig die Person von allen anderen Menschen unterscheidet. Dazu kann man Anleihen am Meldewesen nehmen, bei dem es gemäß § 2 Abs. 1 BMG ja gerade darum geht, Personen zu registrieren, um deren Identität festzustellen. Je nach individueller Unterscheidungskraft wird darum erst der Name

1037 Darauf deutete aber für die DS-GVO-E die Formulierung „to identify or single out" in ErwG 23 in der durch den Beschluss des Parlaments vom 12.3.2012 (T7–0212/2014) geänderten Fassung hin.

1038 Zur insofern inhaltsgleichen Vorgängerregelung in Art. 2 lit. a DSRL EuGH, ECLI:EU:C:2016:779, Rn. 38 – *Breyer*.

in Kombination mit einem oder mehrerer Merkmale wie einer ladungsfähigen Anschrift, dem Geburtsort und -datum oder gar biometrischer Merkmale zur sicheren Identifikation einer Person führen.[1039] Alles, was unterhalb dieses Niveaus liegt, ist der (ggf.: fehlenden) Identifizierbarkeit zuzuordnen.

3.3.1.4 Die Identifizierbarkeit einer Person

772 Nach Art. 4 Nr. 1 DS-GVO kann eine Person entweder direkt oder indirekt identifiziert werden. Dies ist terminologisch etwas ungeschickt, wird doch nicht klar, wo der Unterschied liegen soll, ob eine Person bereits identifiziert ist oder nur direkt identifiziert werden kann. Der Begriff direkt steht ja gerade dafür, dass es keine weiteren Zwischenschritte bedarf; dann ist die Person aber bereits identifiziert. Dem Verordnungsgeber war es aber hier wohl wichtig, klarzustellen, dass auch indirekt identifizierbare Personen unter dem Schutz der Verordnung stehen.

773 Diese Unschärfe führt aber dazu, dass teilweise nicht zwischen Identifikation und Identifizierbarkeit, sondern stattdessen nur zwischen direkter und indirekter Identifizierbarkeit unterschieden wird.[1040] Dieses unterschiedliche Begriffsverständnis ist wohl dem Umstand geschuldet, dass es für die Frage des Personenbezugs einer Information letztlich keine Rolle spielt, ob die betroffene Person direkt oder indirekt identifiziert werden kann oder gar schon identifiziert ist. Der Aussagegehalt dieser Formulierung in Art. 4 Nr. 1 DS-GVO beschränkt sich insofern darauf, dass sich die Identität der betroffenen Person nicht aus dem besonderen Merkmal oder der Merk-

---

1039 Ähnlich *Klar/Kühling*, in: Kühling/Buchner 2018, Art. 4 Nr. 1 DS-GVO, Rn. 18.

1040 Siehe z.B. BeckOK DSR/*Schild*, Art. 4 DS-GVO, Rn. 16 f. Zur direkten Identifizierbarkeit werden lebenslang unveränderliche Merkmale wie die Sozialversicherungs- oder die Steueridentifikationsnummer gezählt, aber auch die Kombination aus dem Namen und weiterer Merkmale, die nach der hier vertretenen Auffassung bereits dazu führen, dass die Person identifiziert ist. Als Beispiel für die indirekte Identifizierbarkeit werden veränderliche Merkmale wie die Reisepass- oder Personalausweisnummer genannt. Diese Differenzierung ändert aber nichts daran, dass es sich bei den genannten Nummern im Grunde um – wenn auch u.U. einer Vielzahl von Personen bekannte – Pseudonyme handelt, die a priori nur jene Behörde auflösen kann, die sie auch vergeben hat. Kontextunabhängig sind diese Merkmale gerade nicht. Das unterscheidet sie z.B. von einer Merkmalskombination aus Namen, Geburtsort und -datum, die hier der Identifikation zugeordnet wird.

malskombination ergeben muss, dem bzw. der die jeweilige Information zugeordnet ist. Es genügt, wenn diesem Merkmal wiederum eines oder mehrere Merkmale – direkt oder abermals indirekt – zugeordnet sind, sodass im Ergebnis ein Rückschluss auf die Identität der betroffenen Person gezogen werden kann.[1041]

774 Für den Personenbezug ist darum entscheidend, unter welchen Voraussetzungen diese Zuordnung im Sinne der Verordnung möglich ist, unter welchen Voraussetzungen die weiteren Merkmale zu Identifizierung der Person also verfügbar sein müssen. Der Legaldefinition in Art. 4 Nr. 1 DS-GVO lässt sich dies nicht entnehmen, in den Erwägungsgründen hat der Verordnungsgeber aber einige Hinweise auf diesen Maßstab der Identifizierbarkeit gegeben.

3.3.1.4.1 Allgemeiner Maßstab

775 Anhand der Legaldefinition in Art. 4 Nr. 1 DS-GVO steht lediglich fest, dass ein Personenbezug ausscheidet, wenn die notwendigen weiteren Merkmale selbst unter theoretischen Bedingungen nicht zu erlangen sind. Da in der Praxis völlige Gewissheit in Bezug auf das Nichtbestehen des Personenbezugs jedoch nicht zu erreichen ist,[1042] kann es stets nur um verschieden hohe Wahrscheinlichkeiten der Identifizierbarkeit gehen. Dies entspricht auch der Konzeption des Rechts auf Schutz personenbezogener Daten (siehe die Argumentation in 3.3.1.2.2, S. 318).

776 Der Grad der Wahrscheinlichkeit wird in ErwG 26 S. 3 DS-GVO aufgegriffen, demzufolge „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern." Die Erwägung entspricht weitgehend der Formulierung in ErwG 26 S. 2 der Datenschutzrichtlinie 95/46/EG, in dem die Bestimmbarkeit einer Person behandelt wurde.

777 Auffällig ist zunächst nur der verunglückte Versuch, das im Gesetzgebungsprozess abgelehnte Merkmal des Aussonderns[1043] irgendwie in der Verordnung zu erwähnen. Darüber hinaus ging es in ErwG 26 DS-RL aber

1041 Ähnlich zu Art. 2 lit. a DSRL EuGH, ECLI:EU:C:2016:779, Rn. 41 – *Breyer*.
1042 So bereits *Dittrich/Schlörer,* DuD 1987, S. 30, 32.
1043 Siehe 3.3.1.3, S. 319, dort Fn. 1037.

auch noch darum, ob Mittel „vernünftigerweise […] eingesetzt werden könnten", in ErwG 26 DS-GVO nun aber darum, ob sie „wahrscheinlich genutzt werden". Damit ist aber kein wesentlicher Bedeutungswechsel verbunden. Was ein Verantwortlicher oder ein Dritter wahrscheinlich tun wird, kann man nämlich im Zweifel nur danach bestimmen, wie sich eine vernünftig handelnde Person in ihrer Situation verhielte. Auf der Basis von Unvernunft kann man keine belastbaren Prognosen treffen. Die zur alten Rechtslage geäußerten Auffassungen und insbesondere die dazu ergangene Rechtsprechung[1044] lassen sich darum auf Art. 4 Nr. 1 DS-GVO übertragen.[1045]

778 Ein Personenbezug ist bereits dann zu verneinen, wenn die Wahrscheinlichkeit, die Person zu bestimmen, praktisch irrelevant erscheint.[1046] Dabei sind nach ErwG 26 S. 4 DS-GVO „alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand", heranzuziehen. Gerade in Grenzfällen muss der Personenbezug darum auf der Grundlage einer Risikoanalyse bestimmt werden, bei der die Gefahr der Identifikation – bei anonymisierten Daten auch in Form der Re-Identifikation – geprüft werden muss. Da hier allein objektive Faktoren eine Rolle spielen sollen, muss die Situation unabhängig von der tatsächlichen Intention des Verantwortlichen beurteilt werden.[1047] Nichtsdestotrotz wird man berücksichtigen müssen, dass der Verantwortliche bei objektiver Betrachtung in bestimmten Situationen typischerweise ein Interesse an der Identifizierung der Person hat, in anderen hingegen typischerweise nicht. Entsprechend steigt oder sinkt die Wahrscheinlichkeit, dass er für ihn verfügbare Mittel auch einsetzt.

779 In der Risikoanalyse sind schließlich gemäß ErwG 26 S. 4 DS-GVO „die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologi-

1044 Vor allem EuGH, ECLI:EU:C:2016:779 – *Breyer*.

1045 *Klar/Kühling,* in: Kühling/Buchner 2018, Art. 4 Nr. 1 DS-GVO, Rn. 20, die auf das „Aussondern" allerdings nicht eingehen. ErwG 26 S. 2 DSRL: „Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen." A.A. *Krügel,* ZD 2017, S. 455, 459 unter Verweis auf die geänderte Formulierung.

1046 EuGH, ECLI:EU:C:2016:779, Rn. 46 – *Breyer*. Anders noch *Pahlen-Brandt,* DuD 2008, S. 34, 38, der zufolge die Beschränkung auf vernünftige Mittel im EG 26 DSRL nur eine Empfehlung ist, z.B. keine hellseherischen Kräfte (sic!) zu berücksichtigen.

1047 *Klar/Kühling,* in: Kühling/Buchner 2018, Art. 4 Nr. 1 DS-GVO, Rn. 22 f.

sche Entwicklungen zu berücksichtigen". Daraus ergibt sich zum einen, dass nicht nur die vom Verantwortlichen tatsächlich eingesetzten, sondern sämtliche am Markt allgemein verfügbaren technischen Mittel in die Prüfung miteinbezogen werden müssen.[1048] Zum anderen wird klargestellt, dass die Beurteilung ex ante und nach dem damaligen Stand der Technik[1049] vorzunehmen ist. Eine „Schutzreserve" für zukünftige Technologien[1050] mag praktisch sinnvoll sein, widerspricht aber klar den in ErwG 26 S. 4 DS-GVO artikulierten Vorstellungen des Verordnungsgebers.

Diese Beschränkung auf aktuelle Möglichkeiten ergibt nur Sinn, wenn auch das Speichern als einmaliger Akt und nicht als fortwährend andauernde und sich darum stets aktualisierende Verarbeitung eingestuft wird. Kommt es also aufgrund technischer Entwicklungen oder zufälliger Zuordnungen, die zum Zeitpunkt der Verarbeitung nicht vorhersehbar waren, zur Identifizierung einer Person, sind die betreffenden Daten aus Sicht der verarbeitenden Stelle dennoch nicht als personenbezogen zu betrachten.[1051] 780

3.3.1.4.2 Zusatzwissen bei demselben Verantwortlichen

Als Quellen für mögliche weitere Merkmale sind jedenfalls der eigene Datenbestand des Verantwortlichen sowie frei zugängliche Informationen zu berücksichtigen. Ein wesentlicher Punkt für die Identifizierbarkeit der betroffenen Person ist folglich die Kontur und Reichweite des Verantwortlichen. Danach entscheidet sich, ob ihm das betreffende Merkmal zur Identifizierung der betroffenen Person ohne Weiteres oder nur nach den Regeln über das Zusatzwissen Dritter zugerechnet wird. 781

Ein Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO stets eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle. Im privaten Bereich kommt es also auf den Rechtsträger an. Auch miteinander verbundene Unternehmen, die aber alle eine eigene Rechtspersönlichkeit haben, stellen eigenständige Verantwortliche dar und sind untereinander grundsätzlich Dritte. So besteht kein Konzernprivileg, dass die konzernweite Verarbeitung personenbezogener Daten zu den Bedingungen der 782

1048 *Klar/Kühling,* in: Kühling/Buchner 2018, Art. 4 Nr. 1 DS-GVO, Rn. 23.
1049 *Kühling/Klar,* NJW 2013, S. 3611, 3613 f.; a.A., noch zur Rechtslage vor der Datenschutzreform *Art. 29-Grp.,* WP 136, S. 18; *Roßnagel,* ZD 2013, S. 562, 563.
1050 *Roßnagel,* ZD 2018, S. 243, 247; *Schaar,* ZD 2016, S. 224, 225.
1051 *Art. 29-Grp.,* WP 136, S. 23; *Scholz* 2003, S. 198; *Kroschwald,* ZD 2014, S. 75, 76.

unternehmensinternen Verarbeitung ermöglichen würde.[1052] Bei der Zurechnung von Wissen für die Frage des Personenbezugs kann jedoch nicht außer Acht gelassen werden, dass die Unternehmensgrenze bei Konzernunternehmen leicht überwunden werden kann, sei es direkt per Weisung des beherrschenden an das beherrschte Unternehmen oder auf umgekehrten Wege durch entsprechende Vereinbarungen. Das betrifft aber nicht die Frage, wer Dritter ist, sondern die, ob das Wissen dieses Dritten dem potenziellen Verarbeiter zugerechnet werden muss (dazu sogleich, 3.3.1.4.3, S. 326).

783 Innerhalb der (privaten) juristischen Person gibt es keine relevanten Grenzen. Insbesondere das Wissen anderer Abteilungen[1053] und auch des Betriebsrats[1054] ist bei der Bestimmung des Personenbezugs ohne Weiteres mit heranzuziehen. Dies ergibt sich auch aus den Erwägungen des Verordnungsgebers zur internen Pseudonymisierung in ErwG 29 (siehe 3.3.4.5.1, S. 342).

3.3.1.4.3 Zusatzwissen Dritter

784 Ob und inwiefern über den Datenbestand des Verantwortlichen hinaus auch der Datenbestand Dritter und das hieraus generierbare Zusatzwissen bei der Beurteilung der Bestimmbarkeit der Person Berücksichtigung finden soll, ist ebenso umstritten wie bedeutsam. Oft steht oder fällt mit ihr die Anwendbarkeit des Datenschutzrechts.

785 In der Vergangenheit ist diese Frage vor allem im Zusammenhang mit dem Personenbezug dynamischer IP-Adressen diskutiert worden (dazu 3.3.1.4.3.6, S. 332). Im Bereich der Assistenzsysteme ist sie allgemein vor allem für solche Systeme relevant, die Daten extern pseudonymisieren (siehe 3.3.4.5.2, S. 343), bei denen also Informationen und Merkmale getrennt bei verschiedenen Stellen verarbeitet werden.

1052 Statt Vieler BeckOK DSR/*Schild*, Art. 4 DS-GVO, Rn. 88.

1053 *Roßnagel,* ZD 2018, S. 243, 245; BeckOK DSR/*Schild*, Art. 4 DS-GVO, Rn. 76.

1054 Die Überlassung von personenbezogenen Daten durch den Arbeitgeber an den Betriebsrat ist keine Übermittlung, sondern eine Nutzung, BAG v. 7.2.2012 – 1 ABR 46/10, E 140, S. 350, Rn. 43 (=NZA 2012, S. 744); BAG v. 14.1.2014 – 1 ABR 54/12, NZA 2014, S. 738, Rn. 28; *Kort,* NZA 2015, S. 1345, 1347.

3.3.1.4.3.1 Die Relativität des Personenbezugs

Die Grundlage der Diskussion zur Zurechnung von Wissen bildet die Formulierung in ErwG 26 S. 3 DS-GVO, in der als relevante Person sowohl der Verantwortliche als auch eine andere Person genannt werden. Da für beide Akteure aber nur die nach allgemeinem Ermessen wahrscheinlich genutzten Mittel berücksichtigt werden, ist dem einen nicht sämtliches Wissen des anderen zuzurechnen, sondern eben nur diejenigen weiteren Merkmale, die dieser ihm auch wahrscheinlich weitergeben würde.[1055] 786

Aus der Sicht des Verantwortlichen gilt folglich auch für die weiteren Merkmale, die nur ein Dritter kennt, der allgemeine Maßstab für die Identifizierbarkeit einer Person.[1056] Der Personenbezug ist keine absolute Größe, sondern nach völlig einhelliger Meinung stets relativ, d.h. für jeden Verantwortlichen getrennt zu bestimmen. Die immer wieder referenzierte[1057] Gegenmeinung, wonach das Wissen jedes beliebigen Dritten – also gewissermaßen das „Weltwissen" – für die Beurteilung der Identifizierbarkeit herangezogen werden muss, wurde schon vor der Klarstellung durch den Europäischen Gerichtshof von nur einer Autorin[1058] vertreten. Die übrigen Vertreter, die die Identifizierbarkeit weit verstehen, sprechen nicht von einem absoluten,[1059] sondern von einem objektiven Personenbezug und erkennen durchaus Konstellationen an, in denen es unwahrscheinlich ist, dass der Verantwortliche an die zur Identifizierung notwendigen Erkenntnisse gelangt.[1060] Die Frage lautet also nicht, ob das Zusatzwissen Dritter als Informationsquelle für die Identifizierung einer Person in Be- 787

1055 GA Campos Sánchez-Bordona, ECLI:EU:C:2016:339, Rn. 68.

1056 EuGH, ECLI:EU:C:2016:779, Rn. 46 – *Breyer*.

1057 Siehe z.B. *Brink/Eckhardt*, ZD 2015, S. 205 f.; *Eßer*, in: Auernhammer 2020, Art. 4 DS-GVO, Rn. 20; *Klar/Kühling*, in: Kühling/Buchner 2018, Art. 4 Nr. 1 DS-GVO, Rn. 25.

1058 *Pahlen-Brandt*, DuD 2008, S. 34, 38; *Pahlen-Brandt*, K&R 2008, S. 286, 289.

1059 So verkennt z.B. *Weichert*, in: Däubler et al. 2020, Art. 4 DS-GVO, Rn. 19, dass der vom ihm propagierte objektive Maßstab keinen Gegensatz zur Relativität des Personenbezugs darstellt.

1060 Die Aufsichtsbehörden verneinten die Identifizierbarkeit, wenn der Zweck der Datenverarbeitung nicht in der Identifizierung der Person bestand und technische und organisatorische Maßnahmen getroffen wurden, *Art. 29-Grp.*, WP 136, S. 19 ff. *Weichert*, will Zusatzwissen Dritter z.B. dann nicht mit einbeziehen, wenn nur wenige Stellen darüber verfügen und es durch technisch-organisatorische Maßnahmen gesichert ist, *Weichert*, in: Däubler et al. 2020, Art. 4 DS-GVO, Rn. 20.

tracht kommt, sondern vielmehr unter welchen Voraussetzungen dies der Fall ist.

3.3.1.4.3.2 Zur Berücksichtigung rechtlich unzulässiger Mittel

788 Auch für die Zurechnung des Zusatzwissens Dritter gilt der allgemeine Maßstab zur Beurteilung der Identifizierbarkeit einer Person, wie er in ErwG 26 S. 3 DS-GVO zum Ausdruck kommt. Entscheidend ist danach, ob der potenzielle Verantwortliche über Mittel verfügt, die er wahrscheinlich dazu einsetzen wird, um die betroffene Person zu identifizieren. Der Ausgangspunkt der Diskussion ist darum klar. Der Streit entzündet sich vor allem an der Frage, ob auch rechtlich unzulässige Mittel als wahrscheinlich betrachtet werden können.

789 Einer verbreiteten Meinung zufolge soll es für die Identifizierbarkeit einer Person allein auf die faktische Verfügbarkeit der Merkmale ankommen. Nur wenn die Identifizierung aus der Sicht eines potenziellen Verantwortlichen praktisch nicht durchführbar sei, bestehe kein Personenbezug.[1061] Ob der Verantwortliche bei der Nutzung dieser Maßnahmen rechtliche Grenzen überschreiten müsste, spielte dann keine Rolle.

790 Dieser sehr strikten Meinung muss ihre eigene Inkonsistenz entgegengehalten werden. Sie ist nämlich nur plausibel, wenn man unterstellt, dem potenziellen Verantwortlichen sei letztlich nicht zu trauen, weil er sich auch über Verbote hinwegsetzen würde. Verarbeitungsverbote hätten auf ihn keine abschreckende Wirkung und müssten folglich auch in der Wahrscheinlichkeitsprognose nach ErwG 26 S. 3 DS-GVO nicht beachtet werden. Konsequenz zu Ende gedacht kann dann aber auch nicht damit gerechnet werden, dass der Verantwortliche die Anforderungen des Datenschutzrechts einhalten wird. Wer verbotswidriges Handeln nicht scheut und wen die damit verbundenen abstrakten Bußgelddrohungen der Datenschutz-Grundverordnung kalt lassen, wird die Anforderungen des Datenschutzrechts ignorieren, wenn sie für ihn mit Aufwand verbunden sind.

1061 Für die Unerheblichkeit rechtlicher Grenzen und die alleinige Berücksichtigung faktisch verfügbarer Daten LG Berlin v. 6.9.2007 – 23 S 3/07, MMR 2007, S. 799, 800; *Buchner,* in: Taeger/Gabel 2013, § 3 BDSG, Rn. 13; BeckOK DSR/*Schild*, § 3 BDSG, Rn. 17; *Weichert,* in: Däubler et al. 2020, Art. 4 DS-GVO, Rn. 24 f.; *Art. 29-Grp.,* WP 136, S. 17 ff.; *Bergt,* ZD 2015, S. 365, 370; *Breyer,* ZD 2014, S. 400, 402 ff.; *Brink/Eckhardt,* ZD 2015, S. 205, 208 f.; *Karg,* MMR 2011, S. 345 f.; *Pahlen-Brandt,* K&R 2008, S. 286, 289.

Dann stellt sich aber die Frage, warum in der Datenschutz-Grundverordnung Verbote ausgesprochen und Bußgelder in Aussicht gestellt werden, würden sie den potenziellen Verantwortlichen doch ohnehin nicht beeinflussen.

Da man den potenziellen Verantwortlichen schlecht mit dem Argument, er werde Regeln missachten, regeln unterwerfen kann, ist die auf rein faktische Verfügbarkeit der Daten abstellende Meinung abzulehnen. Die Annahme, dass gesetzliche Verbote auf das Verhalten der (potenziellen) Verantwortlichen Einfluss haben gilt nicht nur innerhalb des Datenschutzrechts, sondern auch für die Frage, ob das Datenschutzrecht Anwendung findet. Im Sinne des ErwG 26 S. 3 DS-GVO ist ein gesetzlich verbotenes Mittel keines, dass der potenzielle Verantwortliche wahrscheinlich nutzen wird, um eine natürliche Person zu identifizieren. Mit dem Generalanwalt sind folglich zumindest gesetzliche Verbote als wirksame Grenze anzusehen, welche die Zurechnung von Zusatzwissen Dritter verhindern und einen Personenbezug ausschließen.[1062] 791

3.3.1.4.3.3 Anforderungen an Verarbeitungsverbote

Verarbeitungsverbote für das Übermitteln und Erheben von Daten können demnach grundsätzlich verhindern, dass – trotz faktischer Verfügbarkeit der einschlägigen Merkmale bei einem Dritten – aus der Sicht des potenziellen Verantwortlichen ein Personenbezug entsteht. Damit allein ist es aber nicht getan. Es liegt vielmehr nahe, dass die Verarbeitungsverbote selbst einigen Anforderungen genügen müssen, um zu bewirken, dass die beiden Wissensstände wahrscheinlich auch getrennt bleiben. Aus der prinzipiellen Anerkennung von Verarbeitungsverboten als rechtliche Grenzen, können diese Anforderungen aber nicht abgeleitet werden. 792

Die genauen Anforderungen an eine rechtliche Begrenzung wurden trotz der lebhaften Debatte[1063] über den Personenbezug bisher kaum näher diskutiert. *Dammann* verlangt bspw. die tatsächliche Durchsetzung des Verbotes. Seine Nichtbeachtung müsse nach der praktischen Lebenserfahrung auch eine Sanktion nach sich ziehen. Dies wird besonders für lediglich vertraglich abgesicherte Grenzen bezweifelt.[1064] Aber auch bußgeldbewehrte 793

1062 GA Campos Sánchez-Bordona, ECLI:EU:C:2016:339, Rn. 68.
1063 Einen Überblick hierüber liefert *Bergt,* ZD 2015, S. 365–371.
1064 *Dammann,* in: Simitis 2014, § 3 BDSG, Rn. 27; *Kroschwald,* ZD 2014, S. 75, 77 f.

Grenzen seien nicht per se als wirksam anzusehen, wenn die Wahrscheinlichkeit, tatsächlich sanktioniert zu werden, als gering einzustufen ist.[1065] Für andere genügen hingegen die Verarbeitungsverbote, die durch das allgemeine Datenschutzrecht ausgesprochen werden.[1066]

794 Die Skepsis gegenüber rechtlichen Grenzen dürfte vor allem dem Vollzugsdefizit des damaligen Datenschutzrechts[1067] geschuldet sein. Ob sich dies nach der europäischen Datenschutzreform ändert, wird man abwarten müssen. Zumindest die abstrakten Sanktionsdrohungen mit Geldbußen von bis zu 20 Millionen € oder 4 % des weltweit erzielten Jahresumsatzes nach Art. 83 DS-GVO scheinen aber zu verfangen.[1068] Es spricht darum viel dafür, das gesetzliche Verbot, welches es nach allgemeinen Ermessen unwahrscheinlich macht, dass der Verantwortliche die zu Identifizierung der betroffenen Person notwendigen Daten von einem Dritten erhält, im Datenschutzrecht selbst zu suchen.

3.3.1.4.3.4 Das Verbotsprinzip als relevante Grenze

795 Ein gesetzliches Verbot, welches verhindert, dass zwischen zwei rechtlich selbständigen Stellen identifizierende Merkmale ausgetauscht werden, welches also die Zurechnung von Zusatzwissen unterbindet und so den Personenbezug von Daten entfallen lässt, findet sich bereits im sog. allgemeinen Verbotsprinzip des Datenschutzrechts. In der Datenschutz-Grundverordnung kommt dieses Prinzip in Art. 5 Abs. 1 lit. a und Art. 6 Abs. 1 UAbs. 1 DS-GVO (siehe 3.4.1.6.1, S. 418) zum Ausdruck. Danach ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie die Voraussetzungen eines gesetzlich normierten Erlaubnistatbestands erfüllt. Zu den von diesem Erfordernis erfassten Verarbeitungsvorgängen zählen dabei insbesondere die Übermittlung und – auf der Empfängerseite – die Erhebung von Daten.

796 Ob die Weitergabe von Daten als Übermittlung personenbezogener Daten zu qualifizieren ist und in der Folge dem Verbotsprinzip unterliegt, ist –

1065 *Dammann*, in: Simitis 2014, § 3 BDSG, Rn. 28.

1066 Meyerdierks stellte auf das – nach § 43 Abs. 2 Nr. 1 BDSG 2003 bei Vorsatz oder Fahrlässigkeit – bußgeldbewährte Gebot der Direkterhebung nach § 4 Abs. 2 BDSG 2018 ab, *Meyerdierks*, MMR 2009, S. 8, 11.

1067 Siehe nur *Simitis* 2010.

1068 Siehe nur *Heide/Neuerer*, Handelsblatt, Ausgabe 98 v. 24.5.2018, S. 8–9. Teilweise ist sogar von Hysterie die Rede, *Kühl*, Zeit Online, 25.5.2018.

wie der Personenbezug selbst – relativ zu beurteilen. Bei einer Übermittlung kommt es dabei auf den Informationsstand des Empfängers an.[1069] Insofern kann das Datenschutzrecht für eine übermittelte Stelle Anwendung finden, obwohl die betreffende Information für sie selbst – mit ihrem Wissensstand allein – kein personenbezogenes Datum darstellt.

797 Ob ein potenzieller Verantwortlicher im Verhältnis zu dem Dritten nach ErwG 26 S. 3 DS-GVO über Mittel verfügt, die er wahrscheinlich dazu benutzt, die betroffene natürliche Person zu identifizieren, hängt demnach maßgeblich davon ab, ob der Dritte die Daten übermitteln dürfte. Hierfür benötigt dieser Dritte einen der in Art. 6 Abs. 1 UAbs. 1 DS-GVO normierten Erlaubnistatbestände. Andernfalls unterliegt er dem allgemeinen Verarbeitungsverbot in Art. 5 Abs. 1 lit. a und Art. 6 Abs. 1 UAbs. 1 DS-GVO. Ohne einen Erlaubnistatbestand kann folglich das Zusatzwissen eines Dritten dem potenziellen Verantwortlichen nicht zugerechnet werden. Dass der Dritte die identifizierenden Merkmale verbotswidrig übermitteln oder der potenzielle Verantwortliche sich die Merkmale verbotswidrigerweise bei dem Dritten besorgen könnte, spielt dann keine Rolle.

3.3.1.4.3.5 Die Bedeutung vertraglicher Verbote

798 Als wirksame rechtliche Grenze, welche verhindert, dass dem Verantwortlichen Zusatzwissen Dritter zugerechnet und so ein Personenbezug hergestellt wird, sind bisher nur gesetzliche Verbote angesprochen. Wie (siehe 3.3.1.4.3.3, S. 329) oben bereits erwähnt, wird auch die Tauglichkeit vertraglicher Verarbeitungsverbote als rechtliche Grenzen diskutiert.

799 Für vertragliche Verbote gilt zunächst nichts anderes als für gesetzlich festgelegte Verbote. Entscheidend ist, ob man annehmen kann, dass sie die Wahrscheinlichkeit einer Weitergabe des Zusatzwissens wirksam senken. Das wird man zumindest für vertragliche Verbote tun dürfen, die mit – aller Voraussicht nach auch durchgesetzten – Vertragsstrafen verbunden sind.[1070] Diese Verbote wirken gewissermaßen aus sich selbst heraus und lassen einen Personenbezug entfallen.

1069 *Dammann*, in: Simitis 2014, § 3 BDSG, S. 33 f.; *Krüger/Maucher*, MMR 2011, S. 433, 437; *Kühling/Klar*, NJW 2013, S. 3611, 3615; a.A. *Bergt*, ZD 2015, S. 365, 369, der allerdings ohnehin einen deutlich weitreichenderen Begriff der Identifizierbarkeit bevorzugt.

1070 *Arning/Rothkegel*, in: Taeger/Gabel 2019, Art. 4 DS-GVO, Rn. 31.

800 In einigen Situationen ist dieser Umweg über vertraglich festgesetzte Sanktionen aber gar nicht notwendig. Vertragliche Verbote beeinflussen nämlich die gesetzliche Zulässigkeit der Datenverarbeitung, sodass ein – wirksames, d.h. im Bereich des dispositiven Rechts vereinbartes – vertragliches Verbot im Datenschutz zugleich auch gesetzlich abgesichert sein kann. Dieser Effekt ergibt sich zumindest für den als Auffangtatbestand konzipierten Erlaubnistatbestand in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Danach ist eine Datenverarbeitung zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Ein berechtigtes Interesse wird aber dann zu verneinen sein, wenn zwischen den Beteiligten ein vertragliches Verarbeitungsverbot besteht.

801 Insgesamt wird man vertraglichen Verarbeitungsverboten nicht den Stellenwert gesetzlicher Verbote einräumen können. Sie allein bilden in der Regel keine wirksame Grenze, welche die Zurechnung von Zusatzwissen Dritter verhindern könnte. Ausgenommen hiervon sind Situationen, in denen vertragliche Verarbeitungsverbote die abschreckende und verhaltensleitende Wirkung gesetzlicher Verbote erreichen, weil sie mit starken vertraglichen Sanktionen verbunden sind oder über das allgemeine gesetzliche Verbotsprinzip abgesichert sind.

3.3.1.4.3.6 Positive Mittel zur Identifizierung

802 Nach den bisherigen Erläuterungen steht nur fest, unter welchen Umständen es sicher unwahrscheinlich ist, dass der potenzielle Verantwortliche die betroffene natürliche Person identifizieren kann. Um einen Personenbezug zu bejahen, genügt es aber nicht, dass eine Identifizierung nicht sicher unwahrscheinlich ist. Sie muss vielmehr positiv wahrscheinlich sein. Ein Dritter wird dem potenziellen Verantwortlichen nämlich die Merkmale nicht allein deswegen mitteilen, weil er es dürfte. Er muss vielmehr auch einen Grund haben, dies zu tun.

803 Hier kann man zwei Motivationen unterscheiden: Den wirtschaftlichen Druck, Daten zu übermitteln auf der einen und den rechtlichen Druck, dies zu tun, auf der anderen Seite. Die erste Kategorie hängt von den tatsächlichen Machtverhältnissen zwischen den Beteiligten ab und lässt sich rechtlich nicht abstrakt fassen. Die zweite Kategorie ist dagegen rechtlich sehr wohl fassbar. Nach der Rechtsprechung des Europäischen Gerichtshofs ist zumindest dann von einem wirksamen rechtlichen Mittel im Sin-

ne von ErwG 26 S. 2 DS-GVO auszugehen, wenn potenzielle Verantwortliche ggf. über einen Auskunftsanspruch gegenüber dem Dritten verfügen.[1071]

804 Die vom Gerichtshof zu beantwortende Vorlagefrage betraft die Speicherung dynamischer IP-Adressen durch den Betreiber eines Webservers. IP-Adressen sind jene Adressen, unter denen sich Rechner im Internet kontaktieren können. Viele Internetzugangsanbieter ordnen diese Adressen meist nicht statisch den Anschlüssen ihrer Kunden zu, sondern vergeben sie in regelmäßigen Abständen neu – darum dynamische IP-Adressen.[1072] Der Betreiber eines Webservers hatte die die dynamischen IP-Adressen gespeichert, um Angriffe abzuwehren und die strafrechtliche Verfolgung von Angriffen zu ermöglichen.[1073] Droht eine Schädigung, kann der Betreiber die zur Gefahrenabwehr zuständigen Behörden einschalten; ist es bereits zu einer Schädigung bekommen, kann er Strafanzeige stellen. Gemäß § 113 Abs. 1, 3 Nr. 2 TKG und der korrespondierenden Vorschrift in den Sicherheitsgesetzen des jeweiligen Landes bzw. § 113 Abs. 1, 3 Nr. 1 TKG und § 100j StPO können die Behörden dann bei dem Internetzugangsanbieter Auskunft über den Anschlussinhaber verlangen.

805 Dieser Auskunftsanspruch führt nach der Auffassung des Gerichtshofs dazu, dass der Betreiber des Webservers über (rechtliche) Mittel verfügt, den Anschlussinhaber hinter der IP-Adresse zu identifizieren.[1074] Seine Wirkung erschöpft sich folglich nicht darin, das allgemeine Übermittlungsverbot in § 95 Abs. 1 S. 3 TKG entfallen zu lassen, demzufolge Bestandsdaten nur an Dritte übermittelt werden dürfen, wenn dies zugelassen ist oder der Teilnehmer einwilligt. Er führt auch positiv dazu, dass eine Übermittlung der identifizierenden Merkmale wahrscheinlich wird und ein Personenbezug in der Folge zu bejahen ist.

806 Dass die Tatbestandsvoraussetzungen dieses Auskunftsanspruchs (noch) nicht vorliegen und der Betreiber des Webservers zusätzlich noch die Hilfe staatlicher Stellen benötigt,[1075] hält den Gerichtshof nicht davon ab, einen Personenbezug zu bejahen. Dabei dürfte aber auch eine Rolle gespielt ha-

---

1071 EuGH, ECLI:EU:C:2016:779, Rn. 47 – *Breyer*.
1072 EuGH, ECLI:EU:C:2016:779, Rn. 15 f. – *Breyer*.
1073 BGH v. 16.5.2017 – VI ZR 135/13, Z 215, S. 55, Rn. 2 (=ZD 2017, S. 424).
1074 EuGH, ECLI:EU:C:2016:779, Rn. 47 – *Breyer*.
1075 Weil an den Auskunftsverfahren die Staatsanwaltschaft oder (bei urheberrechtlichen Ansprüchen) das Gericht mitwirken müsse, hat z.B. das OLG Hamburg v. 3.11.2010 – 5 W 126/10, MMR 2011, S. 281, 282 einen Personenbezug der Daten noch verneint.

ben, dass die IP-Adressen gerade zu dem Zweck gespeichert wurden, den Auskunftsanspruch später ggf. geltend zu machen.[1076] Dieses Zweckelement[1077] lässt sich bei dem Sachverhalt erkennen, welcher dem Urteil des Europäischen Gerichtshofs zugrunde lag. Betont wurde es jedoch nicht.

3.3.1.4.3.7 Zusammenfassung

807 Die Anforderungen an ein Mittel zur Identifizierung einer natürlichen Person sind demnach zweigeteilt. Zunächst muss das bestehende Übermittlungsverbot überwunden werden. Das kann das allgemeine datenschutzrechtliche Verarbeitungsverbot in Art. 5 Abs. 1 lit. a und Art. 6 Abs. 1 UAbs. 1 DS-GVO oder auch ein spezielleres Verbot sein. Die Voraussetzungen hierfür sind dem Verbot selbst zu entnehmen.

808 Zusätzlich bedarf es eines positiven Grunds für den Dritten, die Merkmale zu übermitteln. Das kann ein Auskunftsanspruch des potenziellen Verarbeiters sein, der bereits das Übermittlungsverbot überwindet. Es kann aber auch jede andere wirtschaftlich oder rechtlich begründete Motivation genügen.

3.3.2 Sonstiger sachlicher und räumlicher Anwendungsbereich

809 Die Datenschutz-Grundverordnung gilt gemäß Art. 2 Abs. 1 DS-GVO sowohl für die automatisierte als auch für die nichtautomatisierte Verarbeitung personenbezogener Daten. Für die nichtautomatisierte Verarbeitung gilt dies aber nur, wenn sie personenbezogene Daten betrifft, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Diese Einschränkung wird im Beschäftigungskontext durch § 26 Abs. 7 BDSG 2018 aufgehoben, wonach die dort in Absatz 1 bis 6 getroffenen Regelungen auch dann anzuwenden sind, wenn die Daten nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen (siehe 3.1.3, S. 242).

1076 Nach *Klar/Kühling,* in: Kühling/Buchner 2018, Art. 4 Nr. 1 DS-GVO, Rn. 28 darf die Geltendmachung des Auskunftsanspruchs nicht fernliegen.

1077 Unter Verweis auf das Zweckelement hat das Schweizer Bundesverwaltungsgericht den Personenbezug von dynamischen IP-Adressen unter Hinweis auf die Auskunftsansprüche bei Verletzung des Urheberrechts bejaht (nach deutscher Rechtslage § 101 Abs. 2, 9 UrhG), BVGer Bern v. 27.5.2009 – A-3144/08, BeckRS 2009, S. 22471.

Als problematisch erweist sich, dass § 26 Abs. 1 S. 1 BDSG 2018 den Anforderungen der Öffnungsklausel in Art. 88 DS-GVO nicht genügt und insofern gegenüber Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO nicht anwendbar ist (siehe 3.1.5.2, S. 248). Die Datenverarbeitung zur Erfüllung des Arbeitsvertrags – inklusive dessen Begründung und Beendigung – richtet sich folglich nicht nach § 26 Abs. 1 S. 1 BDSG 2018, sondern nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO. Den Anwendungsbereich der Datenschutz-Grundverordnung kann die Regelung in § 26 Abs. 7 BDSG 2018 nicht ausweiten, sodass die Datenschutz-Grundverordnung auf Datenverarbeitung, die weder automatisiert noch dateisystembezogen erfolgt, keine Anwendung findet. 810

Im Verhältnis europäischen und mitgliedstaatlichen Datenschutzrechts ist allerdings zu beachten, dass der Anwendungsvorrang des Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO nicht umfassend ist, sondern eben nur so weit reicht, wie die Verordnung selbst nach Art. 2 Abs. 1 DS-GVO anwendbar ist. Für die Datenverarbeitung, die weder automatisiert noch dateisystembezogen durchgeführt wird, ist darum weiterhin § 26 Abs. 1 S. 1 BDSG 2018 anwendbar, in der Gestalt des durch § 26 Abs. 7 BDSG 2018 erweiterten Anwendungsbereichs. In der Sache werden damit alle denkbaren Datenverarbeitungsvorgänge im Beschäftigungsverhältnis abgedeckt. 811

Der räumliche Anwendungsbereich der Datenschutz-Grundverordnung bereitet schließlich keine Probleme. Hier soll lediglich die Tätigkeit von Industriearbeitgebern in Deutschland betrachtet werden. Diese operieren jedenfalls mit einer Niederlassung innerhalb der Union, weshalb die Verordnung gemäß Art. 3 Abs. 1 DS-GVO und § 1 Abs. 4 BDSG 2018 örtlich Anwendung findet. 812

3.3.3 Datenschutzrechtliche Verantwortlichkeit

Adressat der Pflichten nach der Datenschutz-Grundverordnung ist in erster Linie der Verantwortliche. Ihn trifft u.a. die Pflicht nach Art. 5 Abs. 2 DS-GVO, die Einhaltung der Grundsätze des Datenschutzrechts nachzuweisen, er ist der Adressat der Betroffenenrechte nach Art. 12 ff. DS-GVO und er muss die technischen und organisatorischen Maßnahmen nach Art. 24 f. DS-GVO treffen, um sicherzustellen, dass die Verarbeitung personenbezogener Daten gemäß den Vorgaben der Datenschutz-Grundverordnung erfolgt. 813

Bei dem Verantwortlichen handelt es sich gemäß Art. 4 Nr. 7 Hs. 1 DS-GVO um die natürliche oder juristische Person, Behörde, Einrichtung 814

oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Kontext des Beschäftigungsverhältnisses ist dies stets der Arbeitgeber. Die Entscheidung, zu welchem Zweck und mit welchen Mitteln welche personenbezogenen Daten der Beschäftigten verarbeitet werden, ist ihm aufgrund seiner Leitungs- und Organisationsmacht (siehe 2.4, S. 189) auch dann zuzurechnen, wenn er sie faktisch nicht selbst trifft.

815 Die Entscheidungsfreiheit des Arbeitgebers ist dabei aber nicht grenzenlos. Gerade in Bereichen, in denen er gesetzlich verpflichtet ist, Daten zu einem bestimmten Zweck zu erheben, ist zumindest dies vorgegeben. In so einem Fall bestimmt sich die Verantwortlichkeit gemäß Art. 4 Nr. 7 Hs. 2 DS-GVO aus der gesetzlichen Verpflichtung selbst. Ein Beispiel hierfür ist die Pflicht nach § 16 Abs. 2 ArbZG, Arbeitszeitnachweise zu führen. Dass er für die damit einhergehende Datenverarbeitung verantwortlich ist, ergibt sich aus seiner Stellung als Adressat dieser Pflicht.

3.3.4 Anwendbarkeit bei Assistenzsystemen

816 Es ist davon auszugehen, dass beim Betrieb vieler Assistenz- und Produktionssysteme der Industrie 4.0 personenbezogene Beschäftigtendaten verarbeitet werden.[1078] Nicht selten wird der Personenbezug der verarbeiteten Daten dabei auf der Hand liegen, vor allem dann, wenn die Systeme dazu eingesetzt werden, Informationen über die einzelnen Beschäftigten zu ermitteln. In vielen Fällen wird dagegen der Umgang mit Maschinendaten im Vordergrund stehen; personenbezogene Daten werden hier nur beiläufig erhoben. Fraglich ist, inwiefern sich dieser Unterschied auch im Datenschutzrecht abbildet und wie typische Maßnahmen zu bewerten sind, die am Personenbezug der Daten ansetzen.

3.3.4.1 Personalisierte Systeme

817 Am deutlichsten zeigt sich der Personenbezug von Daten, wenn diese in Systemen verarbeitet werden, die auf personenbezogene, d.h. den einzelnen Beschäftigten zugeordnete Nutzerkonten zugreifen.[1079] Der Personen-

1078 Dazu auch *Dehmel/Diekmann,* PinG 2016, S. 141, 142.

1079 *Varadinek, et al.* 2018, S. 20. Dazu auch das Beispiel bei *Müller* 2014, siehe 3.4.2.2.7.2, S. 461.

bezug der Daten, die mit dem Nutzerkonto verknüpft werden, hängt davon ab, welche Daten dort bereits gespeichert sind. Ist das Konto unmittelbar einem bestimmten Beschäftigten zugeordnet, sind auch die damit verknüpften Daten ohne Weiteres als personenbezogen einzustufen. Dieser Effekt kann vermieden werden, wenn das Nutzerkonto anonym oder pseudonym geführt wird (siehe 3.3.4.4, S. 341).

818 Unabhängig davon kann ein Personenbezug gerade im Beschäftigungsverhältnis typischerweise noch in zwei Konstellationen hergestellt werden: Als erste Möglichkeit können Informationen herangezogen werden, die zwar außerhalb des Systems, aber doch beim Verantwortlichen existieren. Das dürfte in der industriellen Produktion nicht selten der Dienstplan[1080] sein, in dem verzeichnet ist, wer wann in welchem Bereich gearbeitet hat. Daraus ergibt sich, welcher Beschäftigte zu dem betreffenden System Zugang hatte, wem die Eingaben also im Zweifel zuzuordnen sind. Als zweite Möglichkeit können für sich genommen nicht personenbezogene Daten so miteinander verknüpft werden, dass sie in der Gesamtschau die Identifizierung der betroffenen Person zulassen.[1081] Insbesondere große Datenbestände dürften von dieser Art des Personenbezugs „bedroht" sein

3.3.4.2 Gezielte Datenerhebung über eine Person

819 Personenbezogene Daten liegen am ehesten vor, wenn die betreffenden Informationen gezielt im Hinblick auf eine Person erhoben werden. Dabei muss es sich nicht zwingend um eine bereits identifizierbare Person handeln. Die entscheidende Abgrenzung zu vornehmlich maschinen- oder betriebsbezogenen Daten (siehe 3.3.4.3, S. 338) liegt darin, dass die Erhebung auf Daten zielt, von denen klar ist, dass sie als Informationen über eine Person (siehe 3.3.1.1, S. 315) Verwendung finden könnten.

1080 Zum Dienstplan einem Assistenzsystem für Busfahrer BAG v. 17.11.2016 – 2 AZR 730/15, NZA 2017, S. 394, Rn. 28; allgemein *Varadinek, et al.* 2018, S. 20.

1081 *Mantz/Spittka,* in: Sassenberg/Faber 2019, § 6, Rn. 18; *Schefzig,* K&R 2014, S. 772, 773 f.; *Skistims et al.,* DuD 2012, S. 31, 35.

3.3.4.3 Vornehmlich maschinen- oder betriebsbezogene Daten

820 Anders als die Daten in Assistenzsystemen wird die weit überwiegende Zahl der Daten in der Industrie 4.0 – etwa die in Produktionssystemen – keinen gezielten Personenbezug aufweisen, sondern vornehmlich schlicht maschinen- oder betriebsbezogen sein. Auch hier ergeben sich prinzipiell dieselben Möglichkeiten, einen Personenbezug herzustellen, wie bei Daten, die gezielt im Hinblick auf eine Person verarbeitet werden. Die Wahrscheinlichkeit, dass die Daten einer identifizierten Person zugeordnet werden können, ist aber als wesentlich geringer einzustufen. Hierzu ist nochmals zwischen der ungezielten Verarbeitung von Daten und der Verarbeitung ohne gezielten Personenbezug zu unterscheiden.

3.3.4.3.1 Ungezielte Verarbeitung

821 Bei der ungezielten Verarbeitung will der Verantwortliche die betreffende Information überhaupt nicht verarbeiten. Die Verarbeitung geschieht entweder unbeabsichtigt oder wird ihm sogar gewissermaßen aufgedrängt. Dies wäre z.B. der Fall, wenn ein leistungsstarkes RFID-Lesegerät im Rahmen der Warenlogistik mehrere lediglich Behälter markierende Transponder auf einmal im Pulk ausliest, und dabei versehentlich auch der personenbezogene Transponder eines sich in der Nähe befindenden Beschäftigten erfasst wird. Hier wurde schon die betreffende Information – Transponder X befindet sich zurzeit Y in Reichweite des Lesegeräts Z – versehentlich erfasst.[1082]

822 Die Frage lautet in diesem Fall, ob ein Verantwortlicher, der Informationen über den betreffenden Beschäftigten sucht, vernünftiger-, weil erfolgversprechenderweise auch in dieser gar nicht für die Speicherung personenbezogener Daten vorgesehener Datenquelle nachforschen würde. Dies dürfte so unwahrscheinlich sein, dass keine grundrechtlich relevante Gefährdungslage entsteht.[1083] Die Information verschwindet hier als sprichwörtliche Nadel im Heuhaufen, sodass die Gefährdungslage mit der Situation vergleichbar ist, in der Daten ungezielt und allein technikbedingt zu-

1082 *Holznagel/Bonnekoh* 2007, S. 375 verneinen im dem vergleichbaren Fall an einer Supermarktkasse den Tatbestand des Erhebens.

1083 *Bäcker* 2012, S. 34.

nächst miterfasst, im Zuge der Verarbeitung des eigentlichen Ziels aber wieder spurlos gelöscht werden.[1084]

In solchen Fällen der rein technisch bedingten ungezielten Miterfassung von Daten wird ein Grundrechtseingriff verneint.[1085] Das Bundesverfassungsgericht hat seine Rechtsprechung zwar dahingehend geändert, dass es sehr wohl einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, wenn die Erfassung eines größeren Datenbestands letztlich nur Mittel zum Zweck für eine weitere Verkleinerung der Treffermenge bildet.[1086] Insbesondere die automatisierte Erfassung von Kfz-Kennzeichen, um diese mit der Fahndungsdatenbank abzugleichen, stellt darum entgegen der bisherigen Rechtsprechung[1087] einen Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Entscheidend sei der durch den Überwachungs- und Verwendungszweck bestimmte Zusammenhang der Datenverarbeitung.[1088] Für das ungezielte und allein technikbedingte miterfassen der Daten hat das Bundesverfassungsgericht aber die fehlende Eingriffsqualität der Maßnahme bekräftigt.[1089] 823

Diese Erwägungen gelten in ihrer Allgemeinheit auch für das Recht auf Schutz personenbezogener Daten in Art. 7, 8 GRC. Bei der ungezielten Datenverarbeitung besteht keine grundrechtlich relevante Gefährdungslage. Ohne sie rechtfertigen es die die staatlichen Schutzpflichten aber nicht, eine solche Situation den Anforderungen des sekundärrechtlichen Datenschutzes zu unterwerfen. Dies muss bei der Auslegung der Regelungen über die Anwendbarkeit der Datenschutz-Grundverordnung in Art. 4 Nr. 1 DS-GVO beachtet werden. Darum kann hier nicht von der Verarbeitung personenbezogener Daten die Rede sein. 824

1084 Für flüchtige Daten im vernetzten Automobil *Buchner,* DuD 2015, S. 372, 374.

1085 BVerfG v. 14.7.1999 – 1 BvR 2226/94, E 100, S. 313, 366 – *Telekommunikationsüberwachung I;* BVerfG v. 4.4.2006 – 1 BvR 518/02, E 115, S. 320, 343 – *Rasterfahndung II;* BVerfG v. 11.3.2008 – 1 BvR 2074/05, E 120, S. 378, 399 – *Kfz-Kennzeichenerfassung I;* BVerfG v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244, Rn. 43 – *Kfz-Kennzeichenerfassung II*.

1086 BVerfG v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244, Rn. 43 – *Kfz-Kennzeichenerfassung II*.

1087 BVerfG v. 11.3.2008 – 1 BvR 2074/05, E 120, S. 378, Rn. 399 – *Kfz-Kennzeichenerfassung I*.

1088 BVerfG v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244, Rn. 43 – *Kfz-Kennzeichenerfassung II*.

1089 BVerfG v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244, Rn. 43 – *Kfz-Kennzeichenerfassung II*.

3.3.4.3.2 Daten ohne gezielten Personenbezug

825 Von der ungezielten Verarbeitung ist die Verarbeitung ohne gezielten Personenbezug[1090] dadurch zu unterscheiden, dass hier sehr wohl klar ist, dass Daten über eine Person verarbeitet werden. Der Fokus liegt aber nicht auf personenbezogener, sondern auf maschinenbezogener Datenverarbeitung. Die Daten – etwa über den Bediener der Maschine – werden nebenbei erhoben und typischerweise keiner Person zugeordnet. Das Ungezielte dieser Verarbeitung bezieht sich in der Terminologie von Art. 4 Nr. 1 DS-GVO also nicht auf die Information, sondern auf das Merkmal (siehe 3.3.1.3, S. 319).

826 Auch hier stellt sich die Frage nach der Wahrscheinlichkeit, mit der ein geneigter Verantwortlicher diese Datenquelle in seine Nachforschungen einbeziehen würde. Da diesmal aber feststeht, dass hier Informationen über eine Person gespeichert sind, wird man die Identifizierbarkeit der Daten bejahen müssen. Gezielter und ungezielter Personenbezug sind insofern keine Kategorie für die Anwendbarkeit datenschutzrechtlicher Regelungen. Die Unterscheidung bleibt trotzdem nicht folgenlos. Sie ist vielmehr innerhalb des Datenschutzrechts zu berücksichtigen.

827 Die Anwendbarkeit des Datenschutzrechts für Daten ohne gezielten Personenbezug zu verneinen, wäre darüber hinaus nicht interessengerecht. In der Diskussion zum Ubiquitous Computing (siehe 1.1.1, S. 49) ist für solche Fälle eine Befreiung von der vorherigen Informationspflicht und der Auskunftspflicht vorgeschlagen worden. Dies sollte kontraproduktive Protokollierungsverfahren vermeiden. Stattdessen sollte über die Struktur der Datenverarbeitung Transparenz hergestellt werden.[1091] Um diesen Effekt zu erzielen muss man indessen nicht im Bereich der Anwendbarkeit ansetzen.

828 Im Rahmen der Datenschutz-Grundverordnung lässt sich hiervon aber bereits einiges umsetzen. So ist es mangels ausdrücklich geregeltem Direkterhebungsgrundsatz (siehe 3.4.1.5.2, S. 410) strittig, ob es zwingend einer vorherigen Information nach Art. 13 DS-GVO bedarf (siehe 3.4.1.5.3, S. 410). Es ist stattdessen auch denkbar, gemäß Art. 14 Abs. 3 DS-GVO nachträglich zu informieren. Diese Pflichten entfallen nach Art. 14 Abs. 5 lit. b DS-GVO, wenn die Information unverhältnismäßig aufwändig wäre, was man angesichts der geringen Risiken bejahen könnte.

1090 Zu dem Begriff *Roßnagel, et al.* 2001, S. 69.
1091 *Roßnagel* 2007a, S. 182 f.; *Roßnagel* 2007b, S. 273 f., 280 f.

Nach der hier vertretenen Meinung kann der Verantwortliche dagegen kaum beeinflussen, welchen Informationspflichten er unterliegt. Der vorherigen Information nach Art. 13 DS-GVO bedarf es stets dann, wenn die betroffene Person als – aktiv mitwirkende oder nur passiv beteiligte – Informationsquelle dient. Die Union oder die Mitgliedstaaten könnten dieses Betroffenenrecht aber nach Art. 23 DS-GVO beschränken und ähnliche Ausnahmen wie in Art. 14 Abs. 5 DS-GVO normieren. Damit der Grundsatz der Transparenz nach Art. 5 Abs. 1 lit. a DS-GVO aber dennoch gewahrt bliebe, müssten bei einer dauernd stattfindenden Datenverarbeitung wie der im Beschäftigungsverhältnis unbenannte Transparenzpflichten an die Stelle der in Art. 13 DS-GVO geregelten treten. Dies könnte dann die vorgeschlagene Transparenz über die Struktur der Datenverarbeitung sein 829

3.3.4.4 Anonymisierung

Soweit die Daten bei interner Verarbeitung als personenbezogen zu beurteilen sind, bieten sich schließlich verschiedene Möglichkeiten an, den Personenbezug zu beseitigen oder zu verringern. Zu ersterem führt das Anonymisieren der Daten, dessen Erfolg sich entsprechend der allgemeinen Maßstäbe danach richtet, ob die Daten faktisch nicht mehr einer Person zugeordnet werden können. Nicht selten wird dieser Schritt aber zumindest dem Dokumentationsinteresse des Arbeitgebers widersprechen. 830

3.3.4.5 Pseudonymisierung

Vor diesem Hintergrund dürfte oft nur eine Pseudonymisierung der Daten nach Art. 4 Nr. 5 DS-GVO in Betracht kommen. Sie wird bei den Regeln zur Zweckänderung in Art. 6 Abs. 4 lit. e DS-GVO sowie bei denen zum technischen Datenschutz nach Art. 25 Abs. 1 DS-GVO ausdrücklich als Maßnahme zur Risikosenkung anerkannt. Daraus könnte man zwar den Schluss ziehen, dass der Verordnungsgebers selbst davon ausgeht, dass das Datenschutzrecht auch auf pseudonymisierte Daten Anwendung findet. Risikosenkung muss hier aber in einem weiteren Sinn verstanden werden. Das Risiko könnte nämlich unterhalb die Schwelle zum Personenbezug gesenkt werden, sodass das Datenschutzrecht – mangels relevanten Risikos für die betroffene Person – gar nicht anwendbar wäre. 831

832 Bei der Pseudonymisierung werden die Merkmale, die eine Person identifizieren durch solche Merkmale[1092] ersetzt, welche die betroffene Person allenfalls identifizierbar machen. Die Schutzwirkung ergibt sich daraus, dass die Zuordnungsregel gesondert aufbewahrt und entsprechend technisch und organisatorisch gesichert wird. Der Personenbezug erschließt sich also nicht für jeden, sondern nur für den, der – nach definierten Bedingungen – den Datensatz und das zusätzliche Merkmal zusammenführt.

3.3.4.5.1 Interne Pseudonymisierung

833 Die Schutzwirkung einer Pseudonymisierung bestimmt sich nach den allgemeinen Regeln, nämlich nach der Wahrscheinlichkeit, dass Datensatz und zusätzliches Merkmal zusammengeführt werden (siehe 3.3.1.4.1, S. 323).[1093] Eine rein interne Pseudonymisierung, bei der das zusätzliche Merkmal – wenn auch organisatorisch getrennt und technisch abgesichert – beim Verantwortlichen verbleibt, hebt jedoch den Personenbezug nicht auf. Der verantwortliche Arbeitgeber verfügt hier allein schon kraft seines Leitungs- und Organisationsrechts über die notwendigen Mittel, das relevante Wissen erforderlichenfalls in einer natürlichen Person zu vereinen. Insofern ist der betroffene Beschäftigte weiterhin nach Art. 4 Nr. 1 DS-GVO identifizierbar.

834 Trotz weiterhin bestehenden Personenbezugs nach Art. 4 Nr. 1 DS-GVO bewirkt die interne Pseudonymisierung aber in jedem Fall, dass mehrere – wenn auch unter einer gemeinsamen Leitung stehende – Organisationseinheiten an der Datenverarbeitung mitwirken müssen und senkt durch dieses Vier-Augen-Prinzip die Wahrscheinlichkeit, dass Daten entgegen den Anforderungen der Verordnung verarbeitet werden. Auf dieser Annahme basiert auch die in ErwG 29 intendierte Privilegierungswirkung. Gemäß ErwG 29 S. 1 DS-GVO sollen Maßnahmen zu Pseudonymisierung bei demselben Verantwortlichen möglich sein, wenn die Umsetzung der Verordnung technisch und organisatorisch abgesichert und insbesondere das weitere Merkmal gesondert aufbewahrt wird. Dazu soll der Verantwortliche gemäß Satz 2 die bei ihm befugte natürliche Person angeben.

1092 In Art. 4 Abs. 5 DS-GVO ist inkonsequent von zusätzlichen „Informationen" die Rede.

1093 *Roßnagel*, ZD 2018, S. 243, 244 f.

Dass nur intern abgeschirmte weitere Merkmale den Personenbezug nicht aufheben, zeigt sich auch daran, dass die Verordnung gemäß ErwG 29 S. 1 DS-GVO weiterhin umgesetzt werden muss, also anwendbar bleibt. Es genügt darum nicht, das entscheidende Merkmal durch den Betriebsrat[1094] oder einen Auftragsdatenverarbeiter[1095] aufbewahren zu lassen. Aus dem Gebot der vertrauensvollen Zusammenarbeit nach § 2 BetrVG bzw. infolge des Vertrags über die Auftragsdatenverarbeitung nach Art. 28 Abs. 3 DS-GVO verfügt der verantwortliche Arbeitgeber über rechtliche Mittel, mit denen er die Bewahrer des Pseudonyms ggf. zwingen kann, ihm dieses Merkmal mitzuteilen. Dies lässt es wahrscheinlich werden, dass er dieses Mittel nutzt, um die betroffene Person zu identifizieren und stellt dadurch letztlich den Personenbezug der Daten her (siehe 3.3.1.4.1, S. 323). 835

3.3.4.5.2 Externe Pseudonymisierung

Bei einer externen Pseudonymisierung werden der Datensatz und das weitere Merkmal getrennt bei unabhängigen Verantwortlichen aufbewahrt. Aus der Sicht beider Verantwortlicher kann es sich bei den Daten und dem weiteren Merkmal darum für sich genommen um nicht personenbezogene Daten handeln,[1096] sodass sie lediglich für den Fall der Übermittlung an den jeweils anderen den Anforderungen der Datenschutz-Grundverordnung unterfielen. Hierfür ist abermals entscheidend, ob die Person aus der Sicht des Verantwortlichen nach den allgemeinen Maßstäben identifizierbar ist. 836

Eine den Personenbezug aufhebende Pseudonymisierung kommt nur in Betracht, wenn intern kein anderes Merkmal vorliegt, mit dem die Identifizierung der betroffenen Person gelingen würde. Das ist gerade dann fraglich, wenn der Arbeitgeber einen umfangreichen Datensatz behält und nur die Vergabe und die Aufbewahrung der Pseudonyme auslagert. So könnte wiederum der Dienstplan (siehe 3.3.4.1, S. 336) herangezogen werden, um einen Beschäftigten zu identifizieren. Auch kann die betroffene Person indirekt aus dem Inhalt der Daten erkennbar werden (etwa durch eine auto- 837

1094 Die Überlassung von personenbezogenen Daten durch den Arbeitgeber an den Betriebsrat ist keine Übermittlung, sondern eine Nutzung, BAG v. 7.2.2012 – 1 ABR 46/10, E 140, S. 350, Rn. 43 (=NZA 2012, S. 744); BAG v. 14.1.2014 – 1 ABR 54/12, NZA 2014, S. 738, Rn. 28; *Kort,* NZA 2015, S. 1345, 1347.

1095 *Roßnagel,* ZD 2018, S. 243, 245.

1096 *Roßnagel,* ZD 2018, S. 243, 245.

matisierte größenabhängige Einstellung einer Maschine, wenn eine bestimmte Körpergröße im Unternehmen nur einmal vorkommt). Eine solche Identifizierung dürfte unwahrscheinlicher sein, wenn der Arbeitgeber das Pseudonym verwaltet und ein externer Dienstleister die Daten verarbeitet. Im Gegenzug stiege für den Arbeitgeber aber das Risiko, dass Betriebs- und Geschäftsgeheimnisse abflössen. Wie er hier vorgeht, ob er also lieber das „Risiko" eines Personenbezugs oder das eines Geheimnisverlusts in Kauf nimmt, ist eine unternehmerische Entscheidung des Arbeitgebers.

838 Die Tatsache allein, dass kein anderes identifizierendes Merkmal verfügbar ist, genügt allerdings nicht, um einen Personenbezug sicher auszuschließen. Der Verantwortliche darf darüber hinaus kein rechtliches Mittel besitzen, das Merkmal von dem Dritten zu erlangen. Aufgrund des allgemeinen datenschutzrechtlichen Verarbeitungsverbots reicht hier aber u.U. schon ein vertragliches Verbot der Weitergabe aus (siehe 3.3.1.4.3.4, S. 330).

3.3.4.6 Selbstkontrolle des Beschäftigten

839 Eine weitere Möglichkeit, den Personenbezug als Risikomerkmal zu minimieren, besteht darin, auf die betroffenen Beschäftigten als Kontrollinstanzen in ähnlicher Weise wie auf unabhängige Dritte zurückzugreifen. Statt durch zentrale Stellen innerhalb des Unternehmens könnte die Datenverarbeitung von Endgeräten durchgeführt werden, die maßgeblich unter der Kontrolle desjenigen Beschäftigten stehen, über den Daten erhoben und verarbeitet werden sollen.[1097] Derartige Ansätze wurden bereits bei biometrischen Systemen diskutiert, bei denen die Erkennung etwa der Fingerabdrücke auf einer Karte stattfindet, die sich im Besitz des Beschäftigten befindet,[1098] die dieser also bei Bedarf auch selbst vernichten könnte. Ein anderes Beispiel sind Ortungssysteme, die in der Lage sind, sich innerhalb der Fabrik selbst zu orten, ohne dass dies eine zentrale Instanz auch nur bemerken könnte.[1099]

840 Diesen Gestaltungsansätzen ist gemein, dass sie die Kontrollmöglichkeiten des betroffenen Beschäftigten erweitern und gleichsam den Zugriff des Arbeitgebers auf die Informationen oder das identifizierende Merkmal er-

1097 Dazu bereits *Steidle* 2005, S. 267 ff.
1098 *Hornung/Steidle,* AuR 2005, S. 201, 203.
1099 *Lucke, et al.* 2008.

schweren. Der Arbeitgeber verfügt jedoch über die rechtlichen und meist auch tatsächlichen Mittel, um sich das benötigte Merkmal zu verschaffen. Der Arbeitnehmer ist gemäß § 855 BGB lediglich Besitzdiener,[1100] weshalb der Arbeitgeber ihm das fragliche Gerät wegnehmen kann, ohne damit verbotene Eigenmacht nach § 858 Abs. 1 BGB zu üben. Kann der Arbeitgeber das Gerät nicht selbst auslesen, weil es gegen einen anderen als den Zugriff durch den Beschäftigten gesichert ist, kann er den Beschäftigten anweisen, das Gerät zu entsperren.[1101]

Diese Methoden senken folglich zwar die Wahrscheinlichkeit, dass der Arbeitgeber den betreffenden Beschäftigten rechtswidrig identifiziert. Sie belassen dem Arbeitgeber aber einen substanziellen Rest an rechtmäßiger Datenverarbeitung, sodass sie den Personenbezug in den meisten Fällen nicht aufheben können. Etwas anderes gälte nur, wenn die betreffenden Informationen lediglich vorübergehend auf dem Gerät gespeichert würden, sodass der Arbeitgeber die Daten bei einem späteren Auslesen des Geräts nicht mehr vorfände. In dieser Konstellation wäre es sehr unwahrscheinlich, dass der Arbeitgeber die betreffende Information dem Beschäftigten zuordnet, weshalb hier keine personenbezogenen Daten verarbeitet würden. 841

3.3.4.7 Kamerabasierte Erfassung

Kamerabasierte Assistenzsysteme weisen einige Besonderheiten auf, welche die Frage nach der Anwendbarkeit des Datenschutzrechts zusätzlich verkomplizieren. Das hängt damit zusammen, dass einige dieser Systeme dazu eingesetzt werden, in einen zu überwachenden Bereich bestimmte Objekte zu erkennen, ohne dass die dazu verwendeten Aufnahmen notwendigerweise längerfristig gespeichert oder einem menschlichen Betrachter zur Verfügung gestellt würden. Der Zweck solcher Systeme liegt oft darin, bestimmte Objekte oder deren Bewegung zu erkennen, wobei es sich dabei auch um menschliche Körper oder Körperteile handeln kann. Die Identifizierung der betroffenen Person steht dagegen nicht im Fokus. 842

Ein Anwendungsbereich dieser Systeme ist die Arbeitssicherheit, speziell die Kollisionsvermeidung beim Einsatz von Leichtbaurobotern. Dazu 843

1100 BAG v. 17.9.1998 – 8 AZR 175/97, E 90, S. 9, Rn. 49 (=NZA 1999, S. 141); BGH v. 30.1.2015 – V ZR 63/13, NJW 2015, S. 1678, 1679.

1101 Zur Parallele der Entschlüsselung dienstlicher E-Mail, *Barton*, CR 2003, S. 839, 842.

filmt eine Kamera den zuvor definierten Schwenkbereich eines Roboters. Das System ist anhand der Aufnahmen in der Lage, Objekte zu erkennen und stoppt den Roboter, wenn es andernfalls zu einer Kollision kommen würde.[1102] Ein anderes Beispiel ist ein System, welches den Beschäftigten dabei hilft, bestimmte Handgriffe auszuführen. Hier ist eine Kamera über einem Montagearbeitsplatz angebracht. Der Tisch, die darauf befindlichen Einzelteile und Werkzeuge sowie die Hände des Monteurs werden gefilmt. Je nachdem, welchen Montageschritt der Arbeiter ausführt, wird die Anleitung angepasst oder ggf. eine Warnung ausgesprochen, wenn ein Schritt übersprungen wurde.[1103]

844 Wenn sich der Personenbezug der Aufnahmen nicht bereits anderweitig ergibt, etwa durch die Verknüpfung mit einem Nutzerkonto des Beschäftigten,[1104] kommt es darauf an, ob der Arbeitgeber den Aufnahmen selbst personenbezogene Informationen entnehmen kann. Dazu sind zwei Stufen zu unterscheiden: In der ersten Stufe muss der Videoausschnitt einen realen Zustand optisch erfassen, der überhaupt identifizierende Merkmale und ggf. weitere Informationen über die betroffene Person enthält. In der zweiten Stufe geht es darum, ob der Verantwortliche die betroffene Person anhand der Aufnahme mit hinreichender Wahrscheinlichkeit identifizieren kann.

3.3.4.7.1 Potenziell identifizierende Merkmale

845 In der ersten Stufe müssen Merkmale optisch erfasst werden, die einer Person zugeordnet sind. Das werden in erster Linie biometrisch auswertbare Merkmale wie das Gesicht[1105] sein. Gerade bei kleinen Vergleichsgruppen können aber auch an sich weniger aussagekräftige Merkmale des äußeren Erscheinungsbilds wie die Statur, die Körperhaltung oder der Gang relevant sein. Denkbar ist schließlich auch, dass eine Person anhand der von ihr typischerweise mitgeführten Gegenstände wie der Kleidung, ihres Mit-

1102 *Busch/Deuse* 2014, S. 62; dazu auch *Haustein* 2013, S. 94.
1103 Zu dem konkreten Beispiel *Bannat, et al.* 2008, S. 3 f.; zu vergleichbaren Systemen siehe 1.3.2, S. 71, Fn. 143.
1104 So z.B. bei *Bächler, et al.* 2015a, S. 59.
1105 Zu Verfahren und Anwendungsmöglichkeiten *Hornung/Schindler,* ZD 2017, S. 203, 204.

arbeiterausweises oder eines von ihr gesteuerten Fahrzeugs identifiziert werden kann.[1106]

Im Beispiel der Systeme zur Kollisionsvermeidung sind deren Kameras so ausgerichtet, dass sie diejenigen Körperteile erfassen, die sich in der Kollisionszone befinden. Hier liegt es nahe, dass auch Merkmale erfasst werden, die zur Identifizierung einer Person herangezogen werden können. Bei einem System, das wie im zweiten Beispiel lediglich die Hände filmt, ist dies hingegen äußerst fraglich. Hände werden typischerweise nur im Hinblick auf die Fingerabdrücke zur Identifikation einer Person herangezogen. Ob auch Videoaufnahmen der ganzen Hand, die überdies meist den Handrücken zeigen,[1107] in der maßgeblichen Vergleichsgruppe die Identifikation der betroffenen Person erlauben, hängt dagegen vom konkreten Einzelfall ab. Gerade bei einer kleinen Zahl von Anwendern ist dies aber durchaus denkbar. 846

3.3.4.7.2 Erkennungsleistung des Verantwortlichen

In der zweiten Stufe geht es darum, die abstrakte Identifizierbarkeit der Person im Hinblick auf die individuellen Fähigkeiten des Verantwortlichen einzuschränken. Dies setzt zum einen am sachlichen Anwendungsbereich der Datenschutz-Grundverordnung an, zum anderen an dem allgemeinen Maßstab der Identifizierbarkeit der Person. 847

3.3.4.7.2.1 Der sachliche Anwendungsbereich bei kamerabasierter Erfassung

Der Anwendungsbereich der Datenschutz-Grundverordnung ist auf die automatisierte oder dateisystembezogene Verarbeitung nach Art. 2 Abs. 1 DS-GVO begrenzt (siehe 3.3.2, S. 334). In Bezug auf die inhaltsgleiche Beschränkung des Anwendungsbereichs für nichtöffentliche Stellen in § 1 Abs. 2 Nr. 3 und § 3 Abs. 2 BDSG 2003 wurde die Auffassung vertreten, dass optische Aufnahmegeräte nur dann eine automatisierte Datenverarbeitungsanlage darstellen, wenn das verarbeitende System in der Lage sei, die Aufnahmen abhängig von dem in der Abbildung enthaltenden perso- 848

1106 Zur Identifizierung von Personen auf Bildern allgemein *Fuchs,* ZD 2015, S. 212, 213; *Scholz,* in: Simitis 2014, § 6b BDSG, Rn. 67.

1107 *Bannat, et al.* 2008, S. 4.

nenbezogenen Informationen zu behandeln. Dies sei erst dann der Fall, wenn das System die Bilder einer bestimmten Person zuordnen könne, entweder, indem es die Bilddaten mit anderweitig erhobenen Daten verknüpfe oder, indem es den Bildinhalt selbst auf Merkmale hin auswerte, die zur Identifizierung einer Person geeignet seien. Anlagen, die dies nicht können, wurden plakativ als „dumme Videoüberwachung" bezeichnet.[1108]

849 Für die erste Variante wurde das Beispiel eines Geldautomaten genannt, der den Videoaufnahmen die Kontodaten der verwendeten Karte zuordnet. Die zweite Variante sollte erfüllt sein, wenn das Bild einer biometrischen Gesichtserkennung oder einer Texterkennung unterzogen wurde.[1109] Demnach wäre ein System, dass die Aufnahmen dem Benutzerkonto des Mitarbeiters zuordnet, als automatisiert zu bezeichnen. Eine automatisierte Objekterkennung, die lediglich in der Lage ist, einen Menschen zu erkennen, ohne Merkmale zu erfassen, anhand derer einzelne Menschen voneinander unterschieden werden können, wäre dagegen nicht als automatisierte Datenverarbeitung nach Art. 2 Abs. 1 DS-GVO einzustufen.

850 Die Gegenauffassung lässt es für eine automatisierte Verarbeitung dagegen schon genügen, wenn die Aufzeichnung automatisiert erfolgt. So hat der Europäische Gerichtshof die Datenschutzrichtlinie in einem Fall privater Videoüberwachung schon allein deswegen angewendet, weil die Aufnahmen kontinuierlich auf einer Festplatte gespeichert wurden.[1110] In der Literatur wird teilweise sogar bereits die Zwischenspeicherung als ausreichend betrachtet. Zur Begründung wird darauf verwiesen, dass alles erfasst sei, „was man mit EDV-Anlagen mit personenbezogenen Daten machen kann."[1111] Geht man davon aus, dass stets Digitalkameras zum Einsatz kommen, läge damit in allen oben genannten Beispielen eine automatisierte Datenverarbeitung nach Art. 2 Abs. 1 DS-GVO vor.

851 Die im ersten Absatz genannte strenge Auslegung der automatisierten Datenverarbeitung weist den insgesamt stringenteren Begründungsansatz auf. Sie geht auf die Grundüberlegung des Datenschutzrechts zurück, den Umgang mit Informationen nur dann zu regulieren, wenn die Informationen in Form von Daten, also codiert verarbeitet werden (3.2.3.3.1, S. 290). Die automatisierte Datenverarbeitung nimmt darin eine hervorgehobene Stel-

---

1108 *Dammann*, in: Simitis 2014, § 3 BDSG, Rn. 79.
1109 *Dammann*, in: Simitis 2014, § 3 BDSG, Rn. 79.
1110 EuGH, ECLI:EU:C:2014:2428, Rn. 25 – *Ryneš*.
1111 BeckOK DSR/*Schild*, Art. 4 DS-GVO, Rn. 34; ähnlich *Ernst*, in: Paal/Pauly 2018, Art. 2 DS-GVO, Rn. 5; *Kühling/Raab*, in: Kühling/Buchner 2018, Art. 2 DS-GVO, Rn. 15.

lung ein, weil die gesuchten Informationen auch in großen Datenbeständen gefunden werden können. Dieses spezifische Risiko besteht aber nur, wenn das System die Informationen in ihrem semantischen Inhalt erfassen kann, die Daten also nicht nur menschen- sondern auch maschinenlesbar sind. Insofern spricht viel dafür, die automatisierte Verarbeitung im Falle der „dummen Videoüberwachung" zu verneinen.

Der weiten Gegenauffassung kann zugutegehalten werden, dass auch außerhalb der automatisierten Datenverarbeitung eine grundrechtliche Gefährdungslage bestehen kann, die eine datenschutzrechtliche Regulierung rechtfertigt. Dogmatisch kann dies allerdings nur im Merkmal der dateisystembezogenen Verarbeitung nach Art. 4 Nr. 6 DS-GVO verortet werden. Wie die Legaldefinition zeigt, muss die Sammlung nicht nach Personen geordnet werden; eine Ordnung nach funktionalen oder geografischen Gesichtspunkten genügt. Ein Dateisystem liegt demnach bereits dann vor, wenn das Aufzeichnungsdatum der jeweiligen Aufnahme vermerkt wird. Das bedeutet aber umgekehrt auch, dass die Bilddaten über eine gewisse Zeit gespeichert werden müssen.[1112] Nur dann besteht das spezifische Risiko einer Sammlung. Reine Kamera-Monitor-Systeme stellen darum keine dateisystembezogene Verarbeitung dar.[1113] 852

3.3.4.7.2.2 Eingeschränkte Bedeutung der Erkennungsleistung im Beschäftigungskontext

Die Begrenzung des Anwendungsbereichs der Datenschutz-Grundverordnung auf die automatisierte und dateisystembezogene Datenverarbeitung in Art. 2 Abs. 1 DS-GVO ist im Beschäftigungskontext nur eingeschränkt von Bedeutung. Für die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses wird der Anwendungsbereich in § 26 Abs. 7 BDSG 2018 auf sämtliche Formen der Datenverarbeitung erweitert (siehe 3.3.2, S. 334). Danach bliebe auch die „dumme Videoüberwachung" nach keiner Auffassung per se unreguliert. Der Streit ist darum vor allem 853

1112 *Scholz,* in: Simitis 2014, § 6b BDSG, Rn. 19.

1113 *Scholz,* in: Simitis 2014, § 6b BDSG, Rn. 19; a.A. wohl *Weichert,* in: Däubler et al. 2020, Art. 4 DS-GVO, Rn. 84. Falsch wäre es dagegen wie *Kühling/Raab,* in: Kühling/Buchner 2018, Art. 2 DS-GVO, Rn. 15 bei einem solchen Verfahren den Tatbestand der Verarbeitung zu verneinen. Es fehlt lediglich am Tatbestand des Speicherns in einem Dateisystem.

für die Frage relevant, welche Grundrechte in diesem Fall zur Anwendung kommen (siehe 3.1.3, S. 242).

854 Darüber hinaus zeigt die Diskussion aber auch, dass es Konstellationen gibt, in denen die dem Datenschutzrecht immanente Gefährdungslage fehlen kann, obwohl Daten verarbeitet werden, die abstrakt betrachtet Merkmale aufweisen, mit denen Personen identifiziert werden können. Aufgrund der Ausweitung des Anwendungsbereichs in § 26 Abs. 7 BDSG 2018 kann dies jedoch nur im Rahmen des Personenbezugs von Daten berücksichtigt werden.

3.3.4.7.2.3 Automatisierte Systeme und Systeme mit Schnittstellen nach außen

855 Wenn bestimmt wird, mit welcher Wahrscheinlichkeit der Verantwortliche die betroffene Person identifizieren kann, geht es neben der abstrakten Eignung der erfassten Merkmale (siehe 3.3.4.7.1, S. 346) maßgeblich um die Auswertungsmöglichkeiten des Verantwortlichen. Sie hängen von der technischen Gestaltung des Systems ab.

856 Können die Aufnahmen nicht oder nur mit unverhältnismäßigem Aufwand aus dem System ausgelesen werden, ist allein auf dessen eigene Erkennungsleistung abzustellen. Ist das System in der Lage, identifizierende Merkmale gezielt zu erfassen und anhand dessen voneinander zu unterscheiden, ist der Personenbezug solcher Aufnahmen dann zu bejahen, wenn die Daten von sich aus bereits zur Identifizierung genügen oder der Verantwortliche über personenbezogene Vergleichsdaten verfügt. Zu diesem Ergebnis käme selbst die strenge Ansicht zur automatisierten Datenverarbeitung. Ein Rückgriff auf § 26 Abs. 7 BDSG 2018 ist hier nicht notwendig.

857 Als problematisch erweisen sich solche Systeme, deren Erkennungsleistung nicht zu Identifizierung von Menschen ausreicht. Bezieht man die Identifizierbarkeit lediglich auf die Fähigkeiten des Systems, wäre hier ein Personenbezug abzulehnen.[1114] In diesen Fällen kommt es darauf an, inwiefern noch weitere Auswertungsmöglichkeiten zu berücksichtigen sind.

858 Verfügt das System über Schnittstellen nach außen, muss auch auf die Erkennungsleistung jener kompatiblen Systeme abgestellt werden, auf die

1114 So zum Beispiel eines Systems, dass lediglich Menschen und Tiere unterscheiden kann, *Schwenke,* NJW 2018, S. 823, 825.

der Verantwortliche realistischerweise zugreifen kann. Zu diesen weiteren „Systemen" können auch menschliche Betrachter zählen, vorausgesetzt, das erfassende System macht es möglich, die Aufnahmen in Augenschein zu nehmen. In diesem Fall wäre auch das Wissen der Betrachter über die identifizierenden Merkmale in die Prüfung einzubeziehen. Gerade bei der Beobachtung abgegrenzter Gruppen wie der Belegschaft dürfte das zur Identifizierung notwendige Wissen in jedem Fall vorliegen (siehe 3.2.3.5.3, S. 302). Werden identifizierende Merkmale wie das Gesicht oder kennzeichnende Objekte erfasst, ist darum bei gefilmten Beschäftigten stets von einem Personenbezug auszugehen.

Die Anwendbarkeit des Datenschutzrechts ist nicht zwingend davon abhängig, dass die Videoaufnahmen aufgezeichnet werden. Dies zeigt sich daran, dass in der Legaldefinition der Verarbeitung in Art. 4 Nr. 2 DS-GVO die Phasen des Erhebens und Erfassens gleichberechtigt neben denen des Speicherns stehen. Auch eine Videoüberwachung im Kamera-Monitor-Verfahren kann eine Verarbeitung im Sinne von Art. 4 Nr. 2 DS-GVO sein.[1115] Durch die Ausweitung des Anwendungsbereichs steht dem auch die fehlende Dateisystembezogenheit nicht im Weg. Folglich wären auch die Aufnahmen in einem System, die es dem Arbeitgeber nur erlauben „zuzusehen", ohne dass er die Bilder aufzeichnen kann, als personenbezogen einzustufen. 859

3.3.4.7.2.4 Systeme ohne automatisierte Erkennung oder Schnittstellen

Als letzte Kategorie bleiben Systeme, die weder über eine hinreichende Erkennungsleistung zur Identifizierung von Personen noch über Schnittstellen nach außen verfügen. Da nach § 26 Abs. 7 BDSG 2018 jede Form der Datenverarbeitung vom Anwendungsbereich des Datenschutzrechts erfasst ist, es also weder auf die automatisierte Erkennung noch die Speicherung der Daten ankommt, liegt es nahe, auch den Aufnahmen dieser Systeme einen Personenbezug zuzusprechen. Damit würde man den Anwendungsbereich des Datenschutzrechts jedoch u.U. auf Systeme ausdehnen, bei denen dies durch die grundrechtliche Gefährdungslage nicht gerechtfertigt wäre. 860

Die grundrechtliche Gefährdungslage beim Betrieb eines solchen Systems ist mit der Situation vergleichbar, die der Entscheidung des Bundesverfas- 861

1115 BeckOK DSR/*Schild*, Art. 4 DS-GVO, Rn. 37.

sungsgerichts zur automatisierten Kennzeichenerfassung[1116] zugrunde lag. Dort wurden Kfz-Kennzeichen automatisiert eingelesen und mit der Fahndungsdatenbank der Polizei abgeglichen. War das Kennzeichen dort hinterlegt, wurde eine Treffermeldung ausgegeben und nähere Informationen wie Ort und Zeit der Meldung gespeichert. Bei einem Nichttreffer, wenn das Kennzeichen nicht hinterlegt war, wurden die Daten umgehend gelöscht. Das Gericht verneinte in diesem und ähnlichen Fällen den Grundrechtseingriff, weil sich das behördliche Interesse an den betroffenen Daten noch nicht derart verdichtet habe, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen sei.[1117] Eine ähnliche Argumentation findet sich auch beim Europäischen Gerichtshof für Menschenrechte in Bezug auf Videoüberwachungssysteme, die lediglich im Kamera-Monitor-Verfahren arbeiten (siehe 3.2.3.5.3, S. 302).

862 Überträgt man die Argumentation ins einfache Datenschutzrecht, kann man in diesen Fällen den Personenbezug von Daten ablehnen, weil es unwahrscheinlich ist, dass die Behörde zu einem Nichttreffer den Kfz-Halter ermittelt. Die Polizei kann die Identifizierung nicht selbst durchführen, da in ihrer Datenbank nur Fahrzeuge enthalten sind, die zur Fahndung ausgeschrieben sind. Als Gefahrenabwehrbehörde verfügt sie aber grundsätzlich über die notwendigen rechtlichen Mittel, sich das fehlende identifizierende Merkmal zu verschaffen. Dies ist aber praktisch entweder sehr unwahrscheinlich oder sogar ganz ausgeschlossen, wenn die Daten über das Kennzeichen sogleich wieder gelöscht werden. Soweit die betroffene Person also nicht bereits bei Erhebung identifiziert ist, wird man auch die Identifizierbarkeit verneinen müssen.[1118]

863 An diesem Befund ändert auch die Ausweitung des Anwendungsbereichs in § 26 Abs. 7 BDSG 2018 nichts. Die Norm erweitert vor allem die nichtautomatisierte Datenverarbeitung und stellt sicher, dass im Kern manuelle Überwachungsmethoden wie Kamera-Monitor-Verfahren oder Torkontrollen ebenfalls in den Anwendungsbereich des einfachen Datenschutzrechts fallen. Der Begriff des Personenbezugs und insbesondere der allgemeine

---

1116 BVerfG v. 11.3.2008 – 1 BvR 2074/05, E 120, S. 378–433 – *Kfz-Kennzeichenerfassung I*.

1117 Eine Begründung findet sich nur in BVerfG v. 4.4.2006 – 1 BvR 518/02, E 115, S. 320, 343 – *Rasterfahndung II*. Zuvor in BVerfG v. 14.7.1999 – 1 BvR 2226/94, E 100, S. 313, 366 – *Telekommunikationsüberwachung I* sowie in später in BVerfG v. 11.3.2008 – 1 BvR 2074/05, E 120, S. 378, 399 – *Kfz-Kennzeichenerfassung I* wurde das Ergebnis nur festgestellt.

1118 *Hofmann*, ZD 2016, S. 12, 14; zustimmend *Varadinek, et al.* 2018, S. 22.

Maßstab der Identifizierbarkeit im Falle der automatisierten Datenverarbeitung soll dagegen nicht tangiert werden.

Die spätere Identifizierung einer Person könnte schließlich auch dadurch ausgeschlossen werden, dass die Aufnahmen stets im Gerät verbleiben, es also über keine Schnittstellen zu anderen Systemen verfügt. Die Schutzmaßnahme ist allerdings nicht so wirksam wie die Löschung der Daten. Im Falle der Aufzeichnung stehen dem Verantwortlichen wesentlich mehr Auswertungsmöglichkeiten zur Verfügung, da die Aufnahmen auch nachträglich und mehrfach verarbeitet werden können. Dies erhöht das Risiko, dass die Aufnahme – ggf. auch unter Überwindung technischer Schutzmaßnahmen – ausgelesen und die Person identifiziert wird. Die Systeme, welche die Aufnahmen nicht nur technisch bedingt zwischenspeichern, sind darum genauso zu behandeln, wie solche Systeme, die über Schnittstellen verfügen. 864

3.3.4.7.3 Fazit zur kamerabasierten Erfassung

Für kamerabasierte Assistenzsysteme lässt sich festhalten, dass die damit getätigten Aufnahmen einen Personenbezug aufweisen, wenn die abgebildeten Merkmale die Identifizierung der Person erlauben. Von diesem Grundsatz ist nur dann eine Ausnahme zu machen, wenn das System 865

- die Aufnahmen nicht mit anderen personenbezogenen Daten verknüpft,
- diese Merkmale nicht im Hinblick auf den Personenbezug auswerten kann,
- es über keine Schnittstellen zu anderen Systemen verfügt, über welche die Aufnahmen ausgelesen werden könnten und
- die Aufnahmen nach erfolgter Objekterkennung umgehend wieder löscht.

3.4 Grundlegende Vorgaben der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung enthält eine Reihe grundlegender materieller und verfahrensrechtlicher Anforderungen, die sowohl für alle Erlaubnistatbestände (siehe 3.6.1, S. 485) als auch alle Verarbeitungssituationen gelten (siehe 3.6.2, S. 525). Diese Vorgaben finden sich zunächst in den Grundsätzen der Verarbeitung personenbezogener Daten in Art. 5 DS-GVO. Von besonderer Bedeutung ist aber weiterhin auch das Prinzip 866

des Datenschutzes durch Technikgestaltung in Art. 25 DS-GVO, mit dem diese Grundsätze abgesichert werden.

3.4.1 Die Grundsätze des Datenschutzrechts

867 Die Erlaubnistatbestände im Bereich des Beschäftigtendatenschutzes sind – wie unter Gliederungspunkt 3.5 (S. 471) noch genauer erörtert wird – in einem hohen Maße unbestimmt. Zur genauen Bestimmung der Zulässigkeit der Datenverarbeitung ist es darum unerlässlich, auf die Grundsätze des Datenschutzrechts in Art. 5 DS-GVO zurückzugreifen. Dies sind die Grundsätze der Zweckbindung, der Datenminimierung, der Rechtmäßigkeit, von Treu und Glauben, der Transparenz, der Richtigkeit, der Speicherbegrenzung, der Integrität und Vertraulichkeit sowie als übergreifende, auf alle anderen bezogenen Pflichten die Rechenschaftspflicht.

868 Für den Einsatz von Assistenzsystemen sind die Zweckbindung und die Datenminimierung in Art. 5 Abs. 1 lit. b und c DS-GVO. Aus ihnen und ihrem gerade ihrem Zusammenspiel ergibt sich der zulässige Umfang der Datenverarbeitung und damit auch der personenbezogene Funktionsumfang des Assistenzsystems. Sie sollen darum hier vertieft erörtert werden. Die übrigen Grundsätze spielen nur eine untergeordnete Rolle und werden hier darum nur kursorisch dargestellt.

3.4.1.1 Die Funktion der Grundsätze

869 Die Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO gehören zu den wenigen Regelungen in der Datenschutz-Grundverordnung, die materielle Anforderungen an die Datenverarbeitung enthalten. Als solche stellen sie Ausprägungen der Schrankenregelungen nach Art. 8 Abs. 2 GRC dar, denen jene Maßnahmen unterliegen, die in das Grundrecht auf Schutz personenbezogener Daten nach Art. 8 Abs. 1 GRC eingreifen.

870 Aus dieser Funktion ergibt sich, dass die Grundsätze trotz ihres allgemein gehaltenen und hochgradig konkretisierungsbedürftigen Inhalts keine bloßen Programmsätze, sondern verbindliche Regelungen darstellen.[1119] Sie

1119 *Kramer*, in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 2 ff.; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 2.

dienen dabei jedenfalls als Maßstäbe zur Auslegung anderer Regelungen, vor allem der Erlaubnistatbestände in Art. 6 DS-GVO. Ob darüber hinaus ein Verstoß gegen die Grundsätze auch direkt zur Unzulässigkeit der Verarbeitung führen kann, ist unklar, aber im Ergebnis auch nicht relevant.[1120] Die Unzulässigkeit ergibt sich in diesen Fällen nämlich jedenfalls aus dem Umstand, dass die Verarbeitung nicht auf einen – entsprechend auszulegenden – Erlaubnistatbestand nach Art. 6 DS-GVO gestützt werden kann.

Die Grundsätze werden ihrerseits durch speziellere Vorschriften in der Datenschutz-Grundverordnung konkretisiert, z.B. durch die Vorschriften zu den Rechten der betroffenen Personen in Kapitel 3 der Verordnung.[1121] Diese detaillierten Regelungen wirken jedoch nicht abschließend.[1122] In Einzelfällen können aus den Grundsätzen auch weitergehende Anforderungen abgeleitet werden, die dann im Rahmen der Erlaubnistatbestände berücksichtigt werden müssen. 871

3.4.1.2 Zweckbindung

Gemäß Art. 5 Abs. 1 lit. b Hs. 1 DS-GVO müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. 872

Entsprechend der offiziellen Bezeichnung dieses Prinzips als „Zweckbindung“ geht es in dieser Regelung in erster Linie um die Bindung der Datenverarbeitung an den Erhebungszweck und weniger um die Begrenzung dieses Zwecks selbst.[1123] Es sollen nicht Daten, die für den einen Zweck erhoben wurden, ohne Weiteres für einen anderen Zweck weiterverarbeitet werden können. Hieraus ergeben sich letztlich aber auch Anforderungen an den Zweck selbst. 873

1120 So auch BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 2 unter Berufung auf EuGH, ECLI:EU:C:2014:317, Rn. 93 f. – *Google Spain*.
1121 *Herbst,* in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 2.
1122 *Frenzel,* in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 11.
1123 *Reimer,* in: Sydow 2018, Art. 5 DS-GVO, Rn. 18.

3.4.1.2.1 Anforderungen an die Zwecksetzung

874 Der Zweck ist von zentraler Bedeutung für die datenschutzrechtliche Prüfung. Er ist nicht nur für die Zweckbindung selbst relevant, sondern spielt nach deren Wortlaut auch in den Prinzipien der Datenminimierung, der Richtigkeit und der Speicherbegrenzung nach Art. 5 Abs. 1 lit. c bis e DS-GVO eine Rolle. Zudem ist er der erste Prüfungspunkt der Erforderlichkeitsprüfung, die ein Tatbestandsmerkmal der Erlaubnisnormen nach Art. 6 Abs. 1 UAbs. 1 lit. b bis f DS-GVO bildet.

875 Die Zwecksetzung hat darum bestimmenden Einfluss auf den Umfang der zulässigen Datenverarbeitung. Darum ist es entscheidend, welche Anforderungen die Verordnung an die Zwecksetzung stellt.

3.4.1.2.1.1 Festgelegt und eindeutig

876 Damit diese Prinzipien wirken und der Verantwortliche an den Erhebungszweck gebunden werden kann, muss er diesen zunächst erst einmal festlegen. Damit wird zugleich deutlich, dass auch nach der Datenschutz-Grundverordnung eine Datenverarbeitung auf Vorrat unzulässig ist.[1124] Die Festlegung des Zwecks hat spätestens mit dem Beginn der Datenverarbeitung zu erfolgen.[1125] Dies wird meist die Erhebung sein, teilweise – etwa im Fall der zweckändernden Weiterverarbeitung – aber auch ein späterer Prozessschritt. Die Zweckfestlegung bedarf keiner Form. Um die Rechenschaftspflichten nach Art. 5 Abs. 2 DS-GVO zu erfüllen, empfiehlt es sich für den Verantwortliche aber, die Schriftform[1126] oder eine andere dauerhafte Form der Dokumentation zu wählen.[1127]

877 Der Zweck muss eindeutig sein. Was hierunter genau zu verstehen ist, ist angesichts der in diesem Punkt voneinander abweichenden Sprachfassungen unklar. Dem deutschen „eindeutig" wird von einigen die materielle Anforderung entnommen, der Zweck dürfe nicht in Blankettformeln wie „zu kommerziellen Zwecken", „zur Verbesserung der Leistung" oder „zur

---

1124 Zu den Vorgaben des europäischen Primärrechts und des Verfassungsrechts, siehe 3.2.3.4.1, S. 293.

1125 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 14; zur Datenschutzrichtlinie *Art. 29-Grp.*, WP 203, S. 15.

1126 *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 27.

1127 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 14; zur Datenschutzrichtlinie *Art. 29-Grp.*, WP 203, S. 18.

Zwecken der IT-Sicherheit" gefasst sein.[1128] Die englische Sprachfassung „explicit", die sich auch mit „ausdrücklich" übersetzen ließe, wird dagegen eher als formelle Anforderung interpretiert, den Zweck der betroffenen Person mitzuteilen.[1129] Die Aufsichtsbehörden scheinen eine Kombination aus beiden Anforderungen zu bevorzugen.[1130]

Die Funktion der Zwecksetzung gebietet es, mit den Aufsichtsbehörden hohe Anforderungen an die Zwecksetzung zu stellen. Nur aufgrund einer präzisen Zwecksetzung kann die Datenverarbeitung auf einen Umfang begrenzt werden, in dem sie von der betroffenen Person sowohl im Vorhinein abgeschätzt als auch im Nachhinein überprüft werden kann.[1131] Hierzu müssen alle Beteiligten über ein gemeinsames Verständnis des Zwecks verfügen. Dies bedeutet allerdings nicht, dass keine unbestimmten Begriffe verwendet werden dürfen. Die genauen Konturen des so umschriebenen Zwecks müssen sich aber anhand anderer Merkmale, wie z.B. einem der Datenverarbeitung zugrundeliegenden Vertrag, oder durch den Rückgriff auf das Übliche und Erwartbare einer Datenverarbeitung bestimmen lassen.[1132] 878

3.4.1.2.1.2 Legitim

Schließlich muss der Zweck legitim sein. Das bedeutet nicht, dass der Zweck gesetzlich vorgesehen oder durch den Betroffenen durch Einwilligung anerkannt sein muss.[1133] Die Frage, inwiefern das Informationsinteresse des Verantwortlichen berechtigt ist, ist im Rahmen der Erlaubnistatbestände nach Art. 6 Abs. 1 UAbs. 1 DS-GVO zu ermitteln. Im Rahmen der Zweckbindung nach Art. 5 Abs. 1 lit. b DS-GVO bedeutet „legitim" nur, dass der Zweck mit der Rechtsordnung insgesamt vereinbar sein 879

1128 *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 27; *Kramer*, in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 27.
1129 *Monreal*, ZD 2016, S. 507, 509; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 16.
1130 Zur Datenschutzrichtlinie *Art. 29-Grp.*, WP 203, S. 17 f.
1131 So ähnlich auch *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 27; *Herbst*, in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 22; *Kramer*, in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 27.
1132 *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 27; *Kramer*, in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 27.
1133 *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 28.

muss.[1134] Dies dürfte allgemein vor allem im Hinblick auf die verpönten Kriterien des Antidiskriminierungsrechts[1135] relevant sein. Speziell im Kontext des Beschäftigtendatenschutzes bietet das Merkmal der Legitimität der Zwecksetzung aber auch einen Ansatzpunkt, um arbeitsrechtliche Vorgaben wie z.B. die Kontrolle des Weisungsrechts nach § 106 GewO in die datenschutzrechtliche Prüfung einzubinden (siehe 3.6.1.2.1.2, S. 493).[1136]

880 Das genaue Verhältnis der arbeitsrechtlichen zu den datenschutzrechtlichen Vorgaben ist mit dem Merkmal der Legitimität der Zwecksetzung aber noch nicht beschrieben. Klar ist nur, dass eine Zwecksetzung, die der Arbeitgeber unter Rückgriff auf sein Weisungsrecht vornimmt, die nach den Maßstäben des § 106 S. 1 GewO aber als unbillig zu werten ist, nicht nach Art. 5 Abs. 1 lit. b Hs. 1 DS-GVO legitim sein kann. Sie dürfte darum auch nicht als Rechtsgrund für die Verarbeitung von Beschäftigtendaten herangezogen werden. Bis zu welchem Punkt die auf das Weisungsrecht gestützte Zwecksetzungsbefugnis reicht oder umgekehrt, wie stark der Zweck konkretisiert werden muss, lässt sich dieser Konstruktion aber nicht entnehmen. Das Merkmal der Legitimität ist darum lediglich eine Generalklausel, mit der Vorgaben aus anderen Rechtsgebieten in die datenschutzrechtliche Prüfung integriert werden können. Aus sich selbst heraus formuliert es keine Anforderungen an die Zwecksetzung.

3.4.1.2.1.3 Gesamtbetrachtung

881 Insgesamt lassen sich aus den Regeln zur Zwecksetzung in Art. 5 Abs. 1 lit. b DS-GVO kaum konkrete Anforderungen ableiten. In dieser allgemeinen Form sind sie weniger als materielle Vorgaben und mehr als Verfah-

---

1134 S *Monreal*, ZD 2016, S. 507, 509; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 17; zur Datenschutzrichtlinie *Art. 29-Grp.*, WP 203, S. 19 f.; a.A. *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 28, demzufolge legitime Zwecke solche sind, die entweder per Einwilligung durch den Betroffenen oder durch ein Gesetz so festgelegt wurden. Dabei wird jedoch übersehen, dass der Verantwortliche den Verarbeitungszweck gemäß Art. 6 Abs. 1 S. 1 lit. f DS-GVO selbst setzen kann.

1135 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 17.; zur Datenschutzrichtlinie *Art. 29-Grp.*, WP 203, S. 12.

1136 So zur Datenschutzrichtlinie wohl auch *Art. 29-Grp.*, WP 203, S. 20. Dort werden die Regelungen des Arbeitsrechts als im Rahmen der Legitimität zu berücksichtigende Normen ausdrücklich genannt.

rensnormen gedacht, ohne deren Einhaltung keine ordnungsgemäße datenschutzrechtliche Prüfung durchgeführt werden kann.

Wie der Zweck aber festgelegt wird, ob unter Mitwirkung des Betroffenen oder einseitig durch den Verarbeiter, und welche Spielräume die Parteien bzw. der Verarbeiter hierbei hat, kann nicht beantwortet werden, ohne die genauen Rechtsverhältnisse der Beteiligten zueinander zu analysieren. Die Zwecksetzung hängt von den Rechtsbeziehungen ab, die das Datenschutzrecht „vorfindet" und variiert damit letztlich von Lebenssachverhalt zu Lebenssachverhalt. 882

3.4.1.2.2 Das Verhältnis der Vereinbarkeit zu anderen Prinzipien

Ihrem Wortlaut nach erfasst die Zweckbindung, der zufolge Daten nicht in einer mit dem Erhebungszweck nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen, sämtliche nach der Datenerhebung einsetzenden Verarbeitungsprozesse. Betrachtet man den Grundsatz der Zweckbindung isoliert, muss auch eine Datenverarbeitung, die zumindest vordergründig dem Erhebungszweck dient, daraufhin geprüft werden, ob sie mit diesem Zweck vereinbar ist.[1137] 883

Dieser Gewährleistungsgehalt der Zweckbindung wird aber für den Fall, dass der Zweck unverändert bestehen bleibt, bereits weitgehend[1138] durch die Prinzipien der Datenminimierung und der Speicherbegrenzung nach Art. 5 Abs. 1 lit. c bzw. e DS-GVO abgedeckt. Der Grundsatz der Datenminimierung (dazu sogleich 3.4.1.3, S. 373) besagt, dass die Verarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Dem Grundsatz der Speicherbegrenzung nach (dazu 3.4.1.6.4, S. 421) zufolge dürfen Daten nur so lange in einer Form gespeichert werden, welche die Identifizierung der betroffenen Personen ermöglicht, wie dies für die Zwecke, für die sie verarbeitet werden, erforderlich ist. 884

1137 Zur Datenschutzrichtlinie *Art. 29-Grp.*, WP 203, S. 21; *Roßnagel*, in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 92.

1138 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 20 sieht einen Anwendungsbereich dort, wo der Zweck zwar gleichgeblieben ist, der Kontext der Datenverarbeitung sich aber wesentlich geändert hat. Es ist aber fraglich, ob eine solche Konstellation nicht auch im Rahmen der Angemessenheitsprüfung der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO berücksichtigt werden kann.

885 Zusammen gewährleisten beide Grundsätze, dass sich die Datenverarbeitung sowohl was das Maß als auch was die zeitliche Dauer der Verarbeitung betrifft im Rahmen des ursprünglichen Erhebungszwecks bewegt. Im Hinblick auf die Datenverarbeitung, die dem Erhebungszweck folgt, wird dieser Gewährleistungsgehalt der Zweckbindung darum von jenen der insoweit spezielleren Grundsätze der Datenminimierung und Speicherbegrenzung verdrängt. Die Anforderung der Vereinbarkeit bezieht sich darum praktisch nur auf die Weiterverarbeitung zu anderen Zwecken.[1139] Diese Auslegung lässt sich auch mit ErwG 50 S. 2 stützen, in dem ausdrücklich von der Weiterverarbeitung zu anderen Zwecken als dem Erhebungszweck die Rede ist.

3.4.1.2.3 Zweckändernde Weiterverarbeitung

886 Gemäß Art. 5 Abs. 1 lit. b Hs. 1 DS-GVO dürfen personenbezogene Daten nicht in einer Weise verarbeitet werden, die mit dem Zweck der Erhebung nicht zu vereinbaren ist. Demzufolge kommt es beim Grundsatz der Zweckbindung nicht darauf an, dass sich die Datenverarbeitung im Rahmen des Erhebungszwecks bewegt. Es geht vielmehr darum, dass sie (nur) mit diesem vereinbar ist. Die Zweckbindung ist folglich nicht so streng ausgestaltet, dass sie gar keine zweckändernde Weiterverarbeitung personenbezogener Daten zu lassen würde.[1140] Das entscheidende Kriterium ist dasjenige der Vereinbarkeit.

3.4.1.2.3.1 Gegenstand der Vereinbarkeitsprüfung

887 Der Formulierung in Art. 5 Abs. 1 lit. b DS-GVO, wonach Daten nicht in einer mit dem Erhebungszweck (oder auch „Primärzweck") nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen, kann man entnehmen, dass es bei der Prüfung auf die zweckändernde Weiterverarbeitung insgesamt – und nicht etwa nur auf den geänderten Zweck (oder auch „Sekundärzweck") an sich[1141] – ankommt.

1139 I.E. *Herbst,* in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 38.

1140 So auch *Kramer,* in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 29.

1141 A.A. zur insofern gleichlautenden Datenschutzrichtlinie *Art. 29-Grp.*, WP 203, S. 21 f. Der Wortlaut ist hier aber eindeutig. Das zeigt auch der Vergleich mit Art. 6 Abs. 4 lit. a DS-GVO, der die Nähe der Zwecke anspricht. Dass bei Art. 5

Für Assistenzsysteme ist vor allem die Unterscheidung in Zwecke der Kontrolle und der Einsichtnahme (siehe 3.4.1.2.4.1, S. 368) relevant. Sollen Daten, die zum Zweck der Einsichtnahme – z.B. zur besseren Prozesssteuerung – erhoben wurden zu Kontrollzwecken – z.B., ob der Arbeitnehmer die Normleistung erbringt – verwendet werden, kommt es folglich nicht allein darauf an, ob sich die Zwecke der Einsichtnahme und der Kontrolle überhaupt und ganz grundsätzlich miteinander vertragen. Entsprechend des umfassenden Prüfungsmaßstabs der Zweckbindung kommt es vielmehr darauf an, ob die konkrete zu Kontrollzwecken durchgeführte Verarbeitung mit dem Erhebungszweck der Einsichtnahme vereinbar ist. Gleichwohl sich bereits anhand eines Zweckvergleichs bestimmte Tendenzen abzeichnen dürften darf eine Prüfung nicht schablonenhaft durchgeführt werden. 888

3.4.1.2.3.2 Funktion der Vereinbarkeitsprüfung

Nach welchen Kriterien diese Vereinbarkeit festzustellen ist, wird – nicht abschließend – in Art. 6 Abs. 4 lit. a bis e DS-GVO geregelt. Danach sind die Verbindung zwischen dem Primär- und dem Sekundärzweck (lit. a), der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden (lit. b), die Art der personenbezogenen Daten (lit. c), die Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (lit. d) sowie das Vorhandensein geeignete Garantien (lit. e) zu berücksichtigen. 889

Diese Kriterien zeigen, dass die Vereinbarkeitsprüfung letztlich eine besondere Form der Risikoabwägung ist. Das zeigt sich besonders an den Kriterien in den Buchstaben d und e, spielt aber auch bei Buchstabe a eine Rolle.[1142] Wo die typischen Risiken der zweckändernden Weiterverarbeitung liegen, lässt sich vor allem den Kriterien in Buchstaben a und b entnehmen. Ihnen liegt die Überlegung zugrunde, dass die Weiterverarbeitung den berechtigten Erwartungen der betroffenen Person zum Zeitpunkt der Datenerhebung entsprechen muss.[1143] 890

Obwohl die Datenschutz-Grundverordnung das Prinzip der Direkterhebung nicht kennt (siehe 3.4.1.5.2, S. 410), wird es dennoch nicht selten so 891

Abs. 1 lit. b Hs. 1 DS-GVO von der Vereinbarkeit der Datenverarbeitung die Rede ist, ist demnach keine ungenaue Formulierung, sondern augenscheinlich Absicht.

1142 Dazu *Roßnagel*, in: Simitis et al., Rn. 37.

1143 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 21.

sein, dass der Betroffene die Datenverarbeitung am besten dadurch kontrollieren kann, dass er bestimmte Angaben macht oder sie verwehrt.[1144] Diese Möglichkeit wird ihm im Fall der zweckändernden Weiterverarbeitung genommen. An die Stelle der Beteiligung treten hier die Informationspflichten nach Art. 13 Abs. 3 DS-GVO,[1145] auf Grundlage derer die Betroffenenrechte ausgeübt werden können.[1146] Dies erfordert aber ein erneutes aktives Tun. Die betroffene Person muss hinsichtlich der Datenverarbeitung intervenieren und kann sich nicht darauf verlassen, dass die Verarbeitung erst erfolgen kann, wenn sie die betreffenden Informationen preisgibt. Zur Aufrechterhaltung des Schutzniveaus für den Betroffenen muss die fehlende Neuerhebung bei der zweckändernden Weiterverarbeitung durch die Vereinbarkeitsprüfung kompensiert werden.[1147]

3.4.1.2.3.3 Die Prüfung der zweckändernden Weiterverarbeitung

892 Unklar ist, wie die Zulässigkeit der zweckändernden Weiterverarbeitung zu prüfen ist. Vorzugswürdig erscheint eine Prüfung, die sich sowohl am Gegenstand als auch an der Funktion der Zweckfestlegung orientiert.

893 Insbesondere *Roßnagel* scheint die Vereinbarkeitsprüfung als einen Vergleich der Zwecke zu verstehen.[1148] Wie aber bereits zum Gegenstand der Vereinbarkeitsprüfung erläutert (siehe 3.4.1.2.3.1. S. 360) ist dies aber ausweislich des Wortlauts der Art. 5 Abs. 1 lit. b und Art. 6 Abs. 4 DS-GVO nicht der Fall. Nicht nur der Sekundärzweck, sondern die gesamte zweckändernde Weiterverarbeitung muss mit dem Primärzweck vereinbar sein.

1144 So ähnlich auch *Buchner,* DuD 2016, S. 155, 156; *Frenzel,* in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 24; *Kramer,* in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 23.

1145 Zum Ganzen BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 19. Dort wird ebenfalls die Informationspflicht nach Art. 14 Abs. 4 DS-GVO erwähnt. Sie bezieht sich aber auf personenbezogene Daten, die ohne die Beteiligung der betroffenen Person erhoben wurden. Auch im Hinblick auf den Primärzweck muss hier lediglich informiert werden. Insofern stellt sich die Situation im Vergleich zur zweckändernden Weiterverarbeitung nicht wesentlich anders dar.

1146 Allgemein noch zur Datenschutzrichtlinie EuGH, ECLI:EU:C:2015:638, Rn. 33 – *Bara*.

1147 So i.E. auch *Albrecht,* in: Simitis et al. 2019, Einführung zu Art. 6 DS-GVO, Rn. 13.

1148 *Roßnagel*, in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 98 f.; *Roßnagel,* in: Simitis et al. 2019, Art. 6 Abs. 4 DS-GVO, Rn. 34.

Das wirkt sich auch auf den Aufbau der Prüfung aus. Es geht nicht darum, zu Anfang bei der Festlegung des Sekundärzwecks dessen Vereinbarkeit mit dem Primärzweck zu prüfen. Die Vereinbarkeitsprüfung findet vielmehr zum Ende der Prüfung statt. Hier wirkt sie als letztes korrektiv und lautet darauf, ob die – für den Sekundärzweck erforderliche und insofern als Neuerhebung prinzipiell zulässige – Datenverarbeitung insgesamt mit dem Primärzweck vereinbar ist. 894

3.4.1.2.3.3.1 Rechtsgrundlage

Zu Beginn steht die Frage, auf welche Rechtsgrundlage die Weiterverarbeitung gestützt werden kann. Gemäß ErwG 50 S. 2 DS-GVO bedarf es für die zweckändernde Weiterverarbeitung im Falle der Vereinbarkeit dieser Verarbeitung mit dem Primärzweck keiner anderen gesonderten Rechtsgrundlage als derjenigen für die Erhebung der personenbezogenen Daten. Ob der Verordnungsgeber mit dieser – lediglich als unverbindlicher[1149] Rechtsmeinung einzuordnenden – Aussage recht hat, ist lebhaft umstritten.[1150] Wie sich im Folgenden zeigen wird, spricht viel dafür, dass der Verordnungsgeber falsch liegt und es sehr wohl stets einer neuen Rechtsgrundlage für die Weiterverarbeitung bedarf. 895

Die praktischen Auswirkungen dieses Streits dürften sich aber ohnehin in engen Grenzen halten. Das zeigt ein Blick auf die Generalklausel, die für den hier relevanten Bereich[1151] in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO geregelt ist. Zumindest sie kann zum Tragen kommen, wenn die Weiterverarbeitung an sich nicht mehr auf die ursprüngliche Rechtsgrundlage gestützt 896

1149 *SJ* 2015, S. 31.

1150 Befürwortend *Kühling/Martini*, EuZW 2016, S. 448, 451; *Monreal*, ZD 2016, S. 507, 510; *Roßnagel*, in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 98; *Ziegenhorn/Heckel*, NVwZ 2016, S. 1585, 1589 f.; ablehnend *Albrecht*, in: Simitis et al. 2019, Einführung zu Art. 6 DS-GVO, Rn. 12 ff.; *Herbst*, in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 48 f.; *Schantz*, NJW 2016, S. 1841, 1844; zur Datenschutzrichtlinie *Art. 29-Grp.*, WP 203, S. 36.

1151 Der Vollständigkeit und Konsistenz halber sei darauf hingewiesen, dass sich die öffentliche Verwaltung auf „ihre" Generalklausel in Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO, wonach eine Verarbeitung zulässig ist, welche für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Die öffentliche Verwaltung ist für ihr Handeln ohnehin an eine Aufgabeneröffnung gebunden, weshalb ein Handeln, dass sich nicht mindestens auf diesen Erlaubnistatbestand stützen kann, rechtswidrig wäre.

werden kann. Gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO ist eine Verarbeitung zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Es ist schwer vorstellbar, dass eine Datenverarbeitung, die mit dem Primärzweck vereinbar ist, sich nicht auch auf diese Rechtsgrundlage stützen ließe. Denn wo ein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO fehlt, kann auch die Vereinbarkeitsprüfung nicht bestanden werden.

897 Gegen die in ErwG 50 S. 2 ErwG vertretene Meinung spricht zudem, dass ihre konsequente Fortsetzung zu problematischen Effekten führt. Denn wenn im Fall der Vereinbarkeit keine neue Rechtsgrundlage von Nöten ist, ließe sich daraus auch der Umkehrschluss ziehen, dass es keiner Vereinbarkeitsprüfung bedürfe, wenn ohnehin eine neue Rechtsgrundlage zur Verfügung stände.[1152]

898 Gegen[1153] diese Auslegung spricht aber, dass die Konstellationen, in denen eine neue Rechtsgrundlage die Vereinbarkeitsprüfung nach Art. 5 Abs. 1 lit. b DS-GVO überflüssig macht, in Art. 6 Abs. 4 DS-GVO eigens geregelt sind.[1154] Dort genügt nicht irgendeine Erlaubnisnorm, sondern eine „Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt". Diese Anforderung dürfen nicht unterlaufen werden. Hierfür spricht auch die Entstehungsgeschichte dieser Ausnahmetatbestände.[1155]

899 Darüber hinaus verkennt diese Meinung die Funktion der Vereinbarkeitsprüfung. Sie soll den Verantwortlichen nur über die aufwändige oder u.U.

1152 *Kramer*, in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 29. Diese bereits in der fünften Auflage (*Kramer*, in: Auernhammer 2017, Art. 5 DS-GVO, Rn. 16) vertretene Meinung war in der sechsten Auflage (*Kramer*, in: Auernhammer 2018, Art. 5 DS-GVO, Rn. 22 f.) zwischenzeitlich aufgegeben worden.

1153 Ablehnend auch *Art. 29-Grp.*, WP 203, S. 36.

1154 Das übersieht *Kramer*, in: Auernhammer 2017, Art. 5 DS-GVO, Rn. 16, wenn er sich in Fn. 32 auf *Plath*, in: Plath 2016, Art. 6 DSGVO, Rn. 31 beruft. Dort wird die spezielle Situation der Art. 6 Abs. 4 DS-GVO thematisiert, nicht die allgemeine Situation in Art. 5 Abs. 1 lit. b Hs. 1 DS-GVO. Die Meinung wurde aber wohl mittlerweile aufgegeben, siehe Fn. 1152.

1155 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 23; zur Entstehungsgeschichte auch *Albrecht*, CR 2016, S. 88, 92.

sogar (nunmehr) unmögliche Neuerhebung der Daten[1156] hinweghelfen. Eine weitergehende Besserstellung ist nicht intendiert (siehe 3.4.1.2.3.2, S. 361). Da die Neuerhebung aber auch dann wegfällt, wenn die zweckändernde Weiterverarbeitung auf eine neue Rechtsgrundlage gestützt werden kann, kann auf die Vereinbarkeitsprüfung nicht verzichtet werden.

3.4.1.2.3.3.2 Zwecksetzung

Die Zwecksetzung ist im Hinblick auf den geänderten Zweck nicht anders vorzunehmen als für den ursprünglichen Erhebungszweck. Sowohl der Primärzweck als auch der Sekundärzweck unterliegen den oben dargelegten Anforderungen an die Zwecksetzung. Eine Prüfung, ob der Sekundärzweck mit dem Primärzweck vereinbar ist, findet hier nicht statt. Insofern ist zunächst prinzipiell jeder geänderte Zweck zu akzeptieren. 900

3.4.1.2.3.3.3 Prüfung anhand der übrigen Grundsätze

Egal welcher Meinung man folgt, steht fest, dass auch eine mit dem Verarbeitungszweck vereinbare Weiterverarbeitung nicht von dem Erfordernis befreit ist, allen übrigen Grundsätzen der Datenverarbeitung zu genügen. Das gilt insbesondere für den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO (dazu sogleich 3.4.1.3, S. 373), demzufolge die (Weiter-) Verarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Ebenso verhält es sich für den Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DS-GVO, demzufolge Daten nur so lange in einer Form gespeichert werden dürfen, die die Identifizierung der betroffenen Personen ermöglicht, wie es für die Zwecke, für die sie (weiter-) verarbeitet werden, erforderlich ist. 901

Die genannten Grundsätze beziehen sich logisch auf den geänderten Zweck, den Sekundärzweck. Denn blieben sie auf den Primärzweck bezogen, wäre die Prüfung hier vorbei. Wäre die fragliche Datenverarbeitung und -speicherung nämlich bereits auf das zum Primärzweck notwendige 902

1156 So i.E. auch *Albrecht*, in: Simitis et al. 2019, Einführung zu Art. 6 DS-GVO, Rn. 13, der aber selbst davon ausgeht, dass die zweckändernde Weiterverarbeitung einer neuen Rechtsgrundlage bedarf und ErwG 50 S. 2 auf diesen Effekt beschränkt wissen will.

Maß bzw. die erforderliche Dauer beschränkt, bedürfte es überhaupt keiner Zweckänderung. Die Verarbeitung könnte dann problemlos im Rahmen des Zwecks durchgeführt werden, für den sie erhoben wurde.

903 Der Maßstab für die Prüfung der Weiterverarbeitung muss sich ebenfalls am Sekundärzweck orientieren. Selbst wenn man die Auffassung vertritt, dass es keiner neuen Rechtsgrundlage bedürfe, muss doch klar sein, dass man z.B. die Verarbeitung zu vertragsfremden Zwecken nicht danach prüfen kann, ob sie nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO für die Vertragserfüllung – für die sie ursprünglich erhoben wurde – erforderlich ist. Ebenso fernliegend wäre es, eine Weiterverarbeitung zu einem anderen Zweck als demjenigen, zu dem der Betroffene eingewilligt hat anhand eben dieser Einwilligung zu prüfen. Diese Einwilligung bildet zwar gemäß Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO die Rechtsgrundlage für die ursprüngliche Datenerhebung. Der darin festgelegte Umfang der Datenverarbeitung ist aber im Hinblick auf den Erhebungszweck formuliert worden und hat darum für den Sekundärzweck keine Bewandtnis mehr.

904 Daran zeigt sich, dass der Streit über die Notwendigkeit einer neuen Rechtsgrundlage fruchtlos ist. Wenn man die alte Rechtsgrundlage heranziehen dürfte, müsste man sie jedenfalls im Hinblick auf den Primärzweck entkernen und anschließend bezogen auf den Sekundärzweck mit neuem Inhalt befüllen. Dabei bliebe einem nichts anderes übrig, als die Rechtsgrundlage heranzuziehen, die der Verantwortliche im Falle einer Neuerhebung genutzt hätte. Ob man aber nun anhand der entkernten alten oder gleich einer neuen Rechtsgrundlage prüft, macht keinen Unterschied.

3.4.1.2.3.3.4 Die eigentliche Vereinbarkeitsprüfung als letztes Korrektiv

905 Steht der Umfang der – wäre sie als Neuerhebung durchgeführt worden zulässigen – Weiterverarbeitung fest, setzt die eigentliche Vereinbarkeitsprüfung ein. Hier sind die Kriterien nach Art. 6 Abs. 4 lit. a bis e DS-GVO zu berücksichtigen. So spielt z.B. eine Rolle, ob der Primär- und der Sekundärzweck eng beieinander liegen (zu lit. a)[1157] oder ob der Betroffene die Daten in Erwartung eines gesteigerten Maßes an Vertrauen preisgege-

1157 *Roßnagel*, in: Simitis et al. 2019, Art. 6 Abs. 4 DS-GVO, Rn. 36.

ben hat (zu lit. b).[1158] Das ist umso eher der Fall, je stärker der Primärzweck konkretisiert worden war.[1159]

Die Vereinbarkeitsprüfung ist dabei im Grunde wie eine Angemessenheitsprüfung zu gestalten.[1160] Dabei sind die Interessenlagen der Beteiligten zu vergleichen, wie sie bei der Verarbeitung und der zweckändernden Weiterverarbeitung bestanden. War die ursprüngliche Verarbeitung z.B. nur zulässig, weil seitens des Verantwortlichen bestimmte Verarbeitungseinschränkungen zugesagt wurden, dürfen diese nun nicht umgangen werden. Bei Assistenzsystemen ist dies gerade bei einer umfangreichen Datenverarbeitung zur Einsichtnahme, also zur Steuerung der Arbeitsprozesse, der Fall. 906

3.4.1.2.3.4 Konsequenzen für die Konkretisierung des Zwecks

Das Konzept des Verordnungsgebers, die Weiterverarbeitung personenbezogener Daten nicht eng an den Zweck, sondern eher weit an die Vereinbarkeit mit dem Zweck zu binden, wirkt auf die Anforderungen an die Zwecksetzung zurück. Die Grenze der Vereinbarkeit mit dem Erhebungszweck ist gleichsam die Grenze der zulässigen Weiterverarbeitung. 907

Soll das Merkmal der Vereinbarkeit mit dem Erhebungszweck seine Eigenständigkeit behalten, darf die Zwecksetzung nicht allzu abstrakt erfolgen. Ließen sich unter einen sehr abstrakten Zweck nämlich ohnehin schon all jene Verarbeitungen subsumieren, die mit diesem Zweck vereinbar wären, blieben keine Konstellationen mehr übrig, in denen eine Zweckänderung zulässig wäre. Denn unter diesen Umständen wäre eine Weiterverarbeitung entweder noch zweckidentisch und daher zulässig oder schon zweckfremd und gleichsam nicht mehr mit dem Erhebungszweck vereinbar und folglich unzulässig. Damit das Merkmal der Vereinbarkeit mit dem Erhebungszweck eine Bedeutung zukommt, muss es also eine „Lücke" geben, zwischen der zweckidentischen und damit ohne weiteres zulässigen Verarbeitung und der unzulässigen – weil mit dem Primärzweck unvereinbaren – zweckändernden Weiterverarbeitung. 908

1158 *Roßnagel,* in: Simitis et al. 2019, Art. 6 Abs. 4 DS-GVO, Rn. 45.
1159 *Richter,* DuD 2015, S. 735, 739; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 69.
1160 *Reimer,* in: Sydow 2018, Art. 5 DS-GVO, Rn. 26.

3.4.1.2.4 Das Verhältnis von Zweck und Rechtsgrundlage

909 Eng verbunden mit dem soeben behandelten Verhältnis der Zwecksetzung zur Vereinbarkeit ist die Frage, wie sich die Zwecksetzung zur Rechtsgrundlage der Verarbeitung verhält. Nach einer Meinung liegt es im Belieben des Verantwortlichen, wie weit er den Zweck konkretisieren will. Für die Rechtmäßigkeit sei nur maßgeblich, ob der vom Verantwortlichen verfolgte Zweck denjenigen Zwecken entspreche, die den Gegenstand der jeweiligen Rechtsgrundlage bildeten.[1161] Das lässt sich so verstehen, dass die Zwecke lediglich auf die Rechtsgrundlage hin konkretisiert werden müssen.[1162] Im Falle des Erlaubnistatbestands nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO würde dies bedeuten, dass es genügt, als Zweck die Erfüllung des Vertrags festzulegen.

910 Die Gegenauffassung verlangt, den Zweck enger als die jeweilige Rechtsgrundlage festzulegen.[1163] Im Beispiel des Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO müsste der Verantwortliche folglich die verschiedenen Aspekte der Vertragsabwicklung – etwa die Erbringung der Leistung und die Entgegennahme der Gegenleistung – identifizieren und als über die Erfüllung des Vertrags hinaus konkretisierten Zweck festlegen.[1164]

3.4.1.2.4.1 Verschärfte Problematik im Arbeitsverhältnis

911 Relevanz erlangt dieser Streit vor allem im Arbeitsverhältnis, dem zwar ein Arbeitsvertrag zugrunde liegt, das aber so komplex ist, dass es aus einem ganzen Bündel von Pflichten und Interessenlagen besteht, die zu verschiedenen Anforderungen an eine Datenverarbeitung führen. So lassen sich die Interessen des Arbeitgebers grob in die Einsichtnahme – also die Datenverarbeitung zur Organisation der Arbeit und allgemein des Betriebs – einerseits und die in letzter Konsequenz auf arbeitsrechtliche Maßnahmen gerichtete Kontrolle der Leistung und des Verhaltens der Beschäftigten andererseits einteilen (dazu näher 3.6.1.2.3.1, S. 508).

912 Die Zulässigkeit der Verarbeitung von Beschäftigtendaten richtet sich grundsätzlich[1165] nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO, also danach,

---

1161 Noch zur alten Rechtslage *Härting,* NJW 2015, S. 3284, 3286 f.
1162 So die Interpretation durch BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 15.
1163 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 15.
1164 In die Richtung zur Datenschutzrichtlinie *Art. 29-Grp.,* WP 203, S. 16.
1165 Zum Verhältnis der Erlaubnistatbestände siehe 3.6.1.1 (S. 485).

ob sie zur Erfüllung des Arbeitsvertrags erforderlich ist. Beide Maßnahmen, die Kontrolle und die Einsichtnahme, lassen sich prinzipiell dieser Vertragserfüllung, also demselben Erlaubnistatbestand zuordnen.[1166] Verlangte man keine Zweckkonkretisierung über die Rechtsgrundlage hinaus, könnten Daten, die zur Einsichtnahme erhoben wurden, ohne weiteres zur Kontrolle der Beschäftigten herangezogen werden. Wäre dagegen eine Konkretisierung notwendig, müssten die Daten entweder von vornherein für beide Zwecke erhoben werden oder – falls der Zweck rückwirkend geändert werden soll – eine Vereinbarkeitsprüfung vorgenommen werden. Gerade weil die Datenverarbeitung zur Einsichtnahme aber deutlich niedrigeren Anforderungen als jene zur Kontrolle begegnet (siehe 3.6.2, S. 525), dürfte eine Zweckänderung in Richtung einer Kontrollmaßnahme nicht selten unzulässig sein.[1167] Die Weiterverarbeitung für eine (andere) Einsichtsmaßnahme wird dagegen in der Regel zulässig sein.[1168]

3.4.1.2.4.2 Konkretisierung nur bei vielen Erlaubnistatbeständen zwingend bzw. nicht notwendig

Es ist zweifelhaft, ob diese Frage für alle Rechtsgrundlagen gleich beant- 913
wortet werden kann. Zumindest im Hinblick auf die Generalklausel in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO ist es unmittelbar einsichtig, dass der Verantwortliche seine oder die berechtigten Interessen eines Dritten klar definieren muss, wenn die Datenverarbeitung zur Wahrung dieser Interessen zulässig sein soll. Der Erlaubnistatbestand ist schlicht so weit gefasst, dass darüber jedwede Zweckbindung ausgehebelt werden könnte. Entsprechend verpflichten Art. 13 Abs. 1 lit. d und Art. 14 Abs. 2 lit. b DS-GVO dazu, der betroffenen Person die konkreten berechtigten Interessen mitzuteilen.

1166 ErfK/*Franzen*, § 26 BDSG, Rn. 22; BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 118. Zur Überwachung zu Beschäftigungszwecken *Forst,* in: Auernhammer 2020, § 26 BDSG, Rn. 18; *Seifert,* in: Simitis et al. 2019, Art. 88 DS-GVO, Rn. 156. Zum vergleichbaren Problem, ob § 28 Abs. 1 S. 2 BDSG 2003 bei der Datenverarbeitung im Beschäftigungsverhältnis nach § 32 Abs. 1 S. 1 BDSG 2003 Anwendung finden sollte *Däubler,* in: Däubler et al. 2016, § 32 BDSG, Rn. 9; *Schmitz* 2016, S. 187; *Stamer/Kuhnke,* in: Plath 2016, § 32 BDSG, S. 10; *Thüsing,* NZA 2009, S. 865, 869.

1167 *Däubler* 2019, Rn. 391c; ausführlicher noch zur alten Rechtslage *Däubler* 2015, Rn. 418 ff.

1168 *Varadinek, et al.* 2018, S. 17 f.

914 Ähnliches gilt für die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO. Anders als bei den übrigen Erlaubnistatbeständen wird der Einwilligung keine Richtung vorgegeben; es geht nicht um einen bestimmten Vertrag, eine bestimmte rechtliche Verpflichtung oder eine bestimmte gesetzliche Aufgabe. Hier auf eine Konkretisierung des Zwecks zu verzichten, würde bedeuten, den Zweck komplett offen zu lassen. Aus diesem Grund ist eine Einwilligung nach Art. 4 Nr. 11 DS-GVO schon definitorisch auf einen „bestimmten Fall" und in Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO auf „einen oder mehrere bestimmte Zwecke" beschränkt.

915 Bei den Erlaubnistatbeständen in Art. 6 Abs. 1 UAbs. 1 lit. c, d und e wird der Zweck durch eine übergeordnete Instanz festgesetzt, entweder unmittelbar durch den Verordnungsgeber selbst (lit. d) oder durch den Gesetzgeber, der eine gesetzliche Verpflichtung oder eine öffentliche Aufgabe definiert (lit. c und e). Ähnliches gilt für die Verarbeitung auf der Grundlage einer Kollektivvereinbarung nach Art. 88 Abs. 1 DS-GVO, § 26 Abs. 4 S. 1 BDSG 2018. Hier wird der Zweck in dem betreffenden Tarifvertrag oder der betreffenden Betriebsvereinbarung definiert; er ist also nicht gleichzusetzen, mit der Kollektivvereinbarung.

916 Aufgrund der großen Unterschiede zwischen den einzelnen Erlaubnistatbeständen in Art. 6 Abs. 1 UAbs. 1 DS-GVO und den genannten weiteren Bestimmungen ist es aber problematisch, aus den Erwägungen zu Tatbeständen in den Buchstaben a und c bis f Schlüsse für das Verhältnis der Zweckkonkretisierung in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO zu ziehen. Zwar sprechen auch die Überlegungen zur Eigenständigkeit des Vereinbarkeitskriteriums für eine Konkretisierung des Zwecks über die Rechtsgrundlage hinaus. Daraus allein lässt sich aber kein zwingender Schluss ziehen.

3.4.1.2.4.3 Einbeziehung weiterer Grundrechte

917 Eine gewisse Richtungsentscheidung lässt sich aber deutlich erkennen. Selbst wenn eine starke Zweckkonkretisierung nicht zwingend vorgeschrieben sein mag, eine nur abstrakte Zwecksetzung also nicht bereits von selbst zur Unzulässigkeit der Datenverarbeitung führt, muss doch klar sein, dass ein sehr weit gefasster Zweck die Erforderlichkeitsprüfung zuun-

gunsten des Verantwortlichen beeinflusst.[1169] In die hier stets auch vorzunehmende Interessenabwägung[1170] sind nicht nur jene Zwecke einzustellen, die der Verantwortliche vordergründig verfolgt, sondern auch diejenigen, die infolge der mangelnden Konkretisierung des Erhebungszwecks ermöglicht werden.[1171] Eine Datenerhebung, die zwar eigentlich nur der Einsichtnahme dienen soll, die aber dem Wortlaut der Zwecksetzung nach auch Daten für eine Kontrollmaßnahme liefern könnte, muss entsprechend auch an dieser möglichen Kontrollmaßnahme gemessen werden. Dies gilt insbesondere für die Angemessenheit der Maßnahme, die nach der oben verfolgten Konzeption in der Vereinbarkeit der Maßnahme mit dem Erhebungszweck zu prüfen wäre. In der Folge muss die Vereinbarkeit gewissermaßen schon zu Anfang geprüft werden.

Folgt man dieser Überlegung, lassen sich bereits bei der Frage der Zweckkonkretisierung (siehe 3.2.2.5.2, S. 281) die Grundrechte der betroffenen Person umfassend berücksichtigen.[1172] Die Anforderung, eindeutige Zwecke festzusetzen ist eng verbunden mit der Transparenz und Nachprüfbarkeit der Datenverarbeitung (siehe 3.4.1.2.1.1, S. 356). In der Vereinbarkeitsprüfung nach Art. 6 Abs. 4 DS-GVO spiegelt sich dies in Buchstabe b wieder, wonach u.a. der Zusammenhang berücksichtigt werden muss, in dem die personenbezogenen Daten erhoben wurden. Wie sich auch aus ErwG 50 ergibt, wird hierfür maßgeblich auf die vernünftigen Erwartungen der betroffenen Person abgestellt.[1173] Ebenso wie aus dem Merkmal der Eindeutigkeit können hieraus jedoch keine besonderen Anforderungen an die Konkretisierung des Zwecks abgeleitet werden. So ließe sich argumentieren, dass auch bei eher abstrakten, gleichwohl aber nicht ungenauen Zwecken wie „Marketing“ oder „Weitergabe an Dritte“ die betroffene Person im Grunde genommen weiß, was auf sie zukommt.[1174] 918

Die Formulierung der vernünftigen Erwartungen geht auf das Konzept der vernünftigen Vertraulichkeitserwartungen („reasonable expectation of pri- 919

1169 So ähnlich auch *Wagner* 2015, S. 87 f., demzufolge die Anforderungen an die Bestimmtheit des Zwecks steigen, je umfangreicher die Datenverarbeitung ausfällt.

1170 A.A. in Bezug auf die Datenverarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 Uabs. 1 lit. b DS-GVO *Ziegenhorn/Heckel*, NVwZ 2016, S. 1585, 1588.

1171 So noch zu § 28 BDSG 2003 *Simitis*, in: Simitis 2014, § 28 BDSG, Rn. 40 ff.

1172 Dazu ausführlich *Grafenstein*, DuD 2015, S. 789, 794 f.

1173 *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 27; *Herbst*, in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 44.

1174 *Grafenstein*, DuD 2015, S. 789, 793.

vacy“) zurück und ist stark mit dem Recht auf Privatsphäre nach Art. 8 EMRK und Art. 7 GRC verknüpft.[1175] Das Recht auf Schutz personenbezogener Daten nach Art. 8 GRC ist hiervon zu unterscheiden und schützt nicht nur die Privatsphäre, sondern als Vorfeldschutz sämtliche Grundrechte der betroffenen Person. Entsprechend ist die Vereinbarkeitsprüfung und – über diese vermittelt – die Zwecksetzung unter Berücksichtigung sämtlicher Grundrechte vorzunehmen. In der Datenschutz-Grundverordnung lässt sich dies in Art. 6 Abs. 4 lit. d DS-GVO verankern, wonach bei der Prüfung der Vereinbarkeit u.a. die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffene Person berücksichtigt werden. Im Übrigen entspricht es auch der Zielsetzung der Datenschutz-Grundverordnung in Art. 1 Abs. 2 DS-GVO, die – also sämtliche – Grundrechte und Grundfreiheiten natürlicher Personen zu schützen. Unter den Folgen nach Art. 6 Abs. 4 lit. d DS-GVO sind hier also die Folgen für sämtliche grundrechtlich geschützte Positionen zu verstehen.

920 Im Beispiel des Arbeitsverhältnisses ist demnach auch die Berufsfreiheit des betroffenen Beschäftigten zu berücksichtigen. Sie ist bei Kontrollmaßnahmen, die auf arbeitsrechtliche Maßnahmen hinauslaufen, stärker berührt als bei einer Einsichtnahme zur Organisation der Arbeit und des Betriebs (siehe 3.2.3.5.6, S. 306). Soll die Datenverarbeitung zur Einsichtnahme zulässig sein, sollte der Zweck also darauf konkretisiert werden.

921 Im Ergebnis ist es aber nicht unter allen Umständen zwingend, den Zweck stark zu konkretisieren. Der Verantwortliche kann sich auch für die Angabe eines eher abstrakten Zwecks entscheiden; er zieht daraus aber keinerlei Vorteil. Ein solches Vorgehen dürfte im Gegenteil sogar insofern nachteilig sein, als er nur in seltenen Fällen tatsächlich vorhat, sämtliche sich ihm durch die weite Zwecksetzung bietenden Möglichkeiten zu nutzen. Der Verantwortliche läuft dadurch Gefahr, auch solche Maßnahmen nicht durchführen zu dürfen, die bei einer gestaffelten Vorgehensweise mit zweckändernder Weiterverarbeitung zulässig gewesen wären.[1176] Es ist also in seinem eigenen Interesse, den Zweck möglichst konkret festzulegen.

1175 EGMR v. 25.9.2001 – 44787/98, Rn. 57 – *P.G. und J.H./Vereinigtes Königreich*.

1176 Dieser Zusammenhang wird oft übersehen, wenn eine Zweckkonkretisierung mit dem Argument bejaht wird, dass andernfalls Schutzlücken entstehen würden, so z.B. bei *Däubler,* in: Däubler et al. 2016, § 32 BDSG, Rn. 9; *Joussen*, NZA 2010, S. 254, 257; *Stamer/Kuhnke,* in: Plath 2016, § 32 BDSG, S. 10; *Thüsing,* NZA 2009, S. 865, 869.

3.4.1.2.5 Zwischenfazit

Die Regelungen zur Zweckfestlegung und -bindung lassen zwar eine gewisse Tendenz zur möglichst weitgehenden Konkretisierung des Zwecks erkennen; zwingende Schlüsse erlauben sie aber nicht. Das ist u.a. dem Umstand geschuldet, dass die Zweckbindung in einem engen Verhältnis zum Prinzip der Datenminimierung steht, sodass sich belastbare Aussagen erst aus dem Zusammenspiel dieser Grundsätze ergeben. Die Zweckkonkretisierung soll darum unter diesem Gliederungspunkt 3.4.1.4 (S. 389) wiederaufgegriffen werden. 922

3.4.1.3 Datenminimierung

Gemäß Art. 5 Abs. 1 lit. c DS-GVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dieses Prinzip der Datenminimierung fordert vom Verantwortlichen nichts anderes als eine Verhältnismäßigkeitsprüfung vorzunehmen. Die hierfür verwendeten europarechtlich geprägten Begriffe weichen zwar von der aus dem deutschen Verfassungsrecht bekannten Terminologie ab, können aber ohne Bedeutungsverschiebung in die gewohnten Begriffe übersetzt werden:[1177] 923

- Die Erheblichkeit ist gleichzusetzen mit der Frage, ob die Datenverarbeitung überhaupt geeignet ist, ihren Zweck zu erreichen.[1178]
- Die Beschränkung auf das notwendige Maß entspricht dem Gebot der Erforderlichkeit, nur das mildeste zur Zweckerreichung geeignete Mittel einzusetzen. Dieses Erfordernis ist zudem – mit Ausnahme der Einwilligung nach Buchstabe a – als Tatbestandsmerkmal in sämtlichen Erlaubnistatbeständen in Art. 6 Abs. 1 UAbs. 1 DS-GVO enthalten.
- Das Erfordernis der Angemessenheit ist mit dem wortgleichen Prüfungspunkt gleichzusetzen, der auch als Verhältnismäßigkeit im engeren Sinn bezeichnet wird.

Für den Maßstab der Erforderlichkeit sind verschieden strenge Ansätze denkbar, die von der bloßen Nützlichkeit bis zur Unverzichtbarkeit der Datenverarbeitung reichen. Dies betrifft letztlich die Frage, an welcher 924

1177 Zum Ganzen *Kramer,* in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 35; *Pötters,* in: Gola 2018, Art. 5 DS-GVO, Rn. 15; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 24 ff.

1178 A.A. *Roßnagel,* in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 120.

Stelle im Prüfungsaufbau die datenschutzrechtlichen Anforderungen genau zu bestimmen sind, und kann am besten im Zusammenspiel mit der Zwecksetzung unter 3.4.1.4.5 (S. 399) erläutert werden. Hier sollen zunächst die grundlegenden Mechanismen der Erforderlichkeitsprüfung dargestellt werden.

3.4.1.3.1 Gegenstand der Datenminimierung

925 Auffällig ist, dass nach dem Wortlaut der Norm auf die Daten selbst und nicht ihre Verarbeitung abgestellt wird. Nähme man diese Formulierung ernst, würde Art. 5 Abs. 1 DS-GVO zwar die Datenerhebung im Hinblick auf die Zahl und die Güte – im Sinne der Aussagekraft – der Daten beschränken. Auch die Frage, wie lange die Daten gespeichert werden dürften, wäre in Art. 5 Abs. 1 lit. e DS-GVO auf das für die Zweckerreichung erforderliche Maß beschränkt. Die übrigen Vorgänge, die gemäß Art. 4 Nr. 2 DS-GVO unter den Begriff der Verarbeitung gefasst werden, etwa die Verwendung, das Übermitteln und die Verbreitung sowie der Abgleich und die Verknüpfung von Daten, würden jedoch nicht dem Gebot der Datenminimierung unterfallen.

926 Diese Beschränkung hätte konkrete Folgen für den Prüfungsumfang der Datenminimierung. Bei wörtlicher Auslegung der Norm spielte es nur eine Rolle, welche Daten verarbeitet werden, nicht aber wie intensiv dies geschieht. Der Verantwortliche wäre durch Art. 5 Abs. 1 lit. c DS-GVO nicht daran gehindert, die Daten z.B. mehr Mitarbeitern zugänglich zu machen oder die Daten stärker mit anderen Daten zu verknüpfen, als dies notwendig ist oder sie gar zu übermitteln, obwohl er den Zweck auch durch eine interne Datenverarbeitung erreichen könnte.

927 Als praktisches Problem stellt sich dies nur bei der Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO dar. Bei allen anderen Erlaubnistatbeständen bezieht sich das Erforderlichkeitsgebot ausweislich der Formulierung im Eingangssatz in Art. 6 Abs. 1 DS-GVO auf die Verarbeitung von Daten. Nun ließe sich argumentieren, dass der Umfang der Datenverarbeitung durch die Einwilligung genau bestimmt wird, es also des Erforderlichkeitsgebots hier nicht bedarf. Dagegen spricht aber, dass kaum eine Einwilligung alle Datenverarbeitungsvorgänge im Detail abbilden kann; das Prinzip der Datenminimierung muss hier wenigstens als Auslegungsmaßstab angelegt werden. Dann gibt es aber keinen Grund, die Verarbeitung aufgrund einer Einwilligung nicht ebenso wie die aufgrund der restlichen Erlaubnistatbestände an das Erforderlichkeitsprinzip zu binden.

Die Formulierung in Art. 5 Abs. 1 lit. c DS-GVO ist darum unglücklich gewählt und letztlich wohl nur der Form der Aufzählung in Art. 5 Abs. 1 DS-GVO geschuldet. Sie ist entgegen des Wortlauts nicht nur auf die Daten – also ihre Erhebung –, sondern auch auf deren Verarbeitung in der ganzen Breite dieses Begriffs nach Art. 4 Nr. 2 DS-GVO zu beziehen.[1179] 928

3.4.1.3.2 Die Erheblichkeit oder die Eignung eines Mittels

Der Begriff der Erheblichkeit in Art. 5 Abs. 1 lit. c DS-GVO ist nicht anders zu verstehen als jener der Geeignetheit im Rahmen der Eingriffsprüfung nach Art. 52 Abs. 1 S. 2 GRC. Geeignet im dortigen Sinne ist ein Mittel, mit dem sich das verfolgte Ziel erreichen lässt.[1180] Die Erheblichkeit einer Datenverarbeitung beurteilt sich also danach, ob mit ihr der festgelegte Zweck erreicht werden kann. Dabei ist es unschädlich, wenn die Datenverarbeitung den Erfolg nicht selbst herbeiführen kann; geeignet und damit auch erheblich ist bereits jeder Beitrag, der die Zweckerreichung fördert.[1181] 929

Diesem an der klassischen Verhältnismäßigkeitsprüfung orientierte Begriffsverständnis wird in der einschlägigen Literatur – wenn es überhaupt thematisiert wird – kaum angezweifelt. Eine Ausnahme bildet *Roßnagel*, demzufolge für den Zweck erheblich ist, was für seine Erfüllung einen Unterschied bewirkt. Anders als bei der Geeignetheit genüge nicht jeder, sondern nur ein entscheidender Beitrag zur Zweckerreichung. Dazu bringt er das Beispiel der Verarbeitung der Kontonummer. Diese sei für die Zahlung zur Vertragserfüllung zwar geeignet, wenn Barzahlung vereinbart worden sei aber nicht erheblich, weil für die konkrete Vertragsabwicklung bedeutungslos.[1182] Das ist zwar im Ergebnis richtig, lässt sich aber konsistenter mit der Zweckkonkretisierung begründen (siehe 3.4.1.4.8.1,S. 404). Dafür muss die Systematik der Verhältnismäßigkeitsprüfung nicht verändert werden. 930

1179 So auch *Pötters*, in: Gola 2018, Art. 5 DS-GVO, Rn. 22.
1180 EuGH, ECLI:EU:C:2014:238, Rn. 46 – *Digital Rights Ireland*.
1181 GA Cruz Villalón, ECLI:EU:C:2013:781, Rn. 99.
1182 A.A. *Roßnagel*, in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 120.

3.4.1.3.3 Das notwendige Maß der Datenverarbeitung

931 Der Begriff der Erforderlichkeit oder – wie im Prinzip der Datenminimierung in Art. 5 Abs. 1 lit. c DS-GVO formuliert – des notwendigen Maßes wird negativ definiert, als das Fehlen eines milderen, zur Zweckerreichung gleich geeigneten Mittels.[1183] Mild bedeutet im diesem Sinne möglichst wenig in die Rechte der betroffenen Person einzugreifen; sowohl in ihr Recht auf Schutz personenbezogener Daten als auch – dem Ziel der Datenschutz-Grundverordnung in Art. 1 Abs. 2 DS-GVO folgend – in ihre übrigen Grundrechte und Grundfreiheiten.

932 Die Eignung bezieht sich auf den Zweck und die zur Zweckerreichung notwendigen Kosten, in dem Sinne, dass die geplanten Funktionen mit möglichst wenig Aufwand realisiert werden können. Im Zusammenspiel ergeben die beiden Merkmale den Maßstab der Erforderlichkeit.

3.4.1.3.3.1 Eingriffsintensität

933 Um innerhalb der Erforderlichkeitsprüfung beurteilen zu können, ob eine andere, gleich geeignete Maßnahme weniger tief in Grundrechte eingreift, ist die Intensität der beiden Eingriffe festzustellen und miteinander zu vergleichen. Die Eingriffsintensität ist in erster Linie anhand der Art und des Umfangs der Datenverarbeitung festzustellen. Eine Datenverarbeitung ist umso intensiver, je mehr Daten der betroffenen Person sie erfasst, je mehr Verarbeitungsschritte sie beinhaltet und je mehr Personen auf Seiten des Verarbeiters daran beteiligt sind.

934 Bei diesem eher quantitativen Ansatz erfüllt der Datenschutz seine Wirkung als Vorfeldschutz anderer Grundrechte, weil mit der Intensität der Verarbeitung auch die Wahrscheinlichkeit sinkt oder steigt, dass die übrigen Grundrechte und Grundfreiheiten der betroffenen Person verletzt werden.[1184] Trotz dieses mittelbaren Zusammenhangs ist auf einer zweiten Ebene zu prüfen, ob aus der Gestaltung der Datenverarbeitung bereits unmittelbar ablesbar ist, ob und wie intensiv in übrige Grundrechte und Grundfreiheiten eingegriffen wird. Dies ist insbesondere dann relevant,

---

1183 Statt Vieler *Roßnagel*, in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 121.

1184 Dieser Automatismus funktioniert nur bei solchen Verarbeitungsschritten nicht, die gerade dazu gedacht sind, die Verarbeitungsmöglichkeiten zu begrenzen. Daten zu pseudonymisieren vermindert bspw. die Eingriffsintensität und erhöht sie nicht noch.

wenn der Zweck vergleichsweise abstrakt gehalten ist (siehe 3.4.1.2.4.3). Bei stärker konkretisierten Zwecken sind die Auswirkungen auf andere Grundrechte der betroffenen Personen dagegen meist ohnehin aus der Natur dieser Zwecke zwingend vorgegeben.

Auf die Eingriffsintensität wirkt sich schließlich auch die Sensibilität der verarbeiteten Daten aus (siehe 3.2.3.5.1, S. 300). Insofern könnte man von einem eher qualitativen Ansatz sprechen. Dabei gilt zwar grundsätzlich, dass sich die Sensibilität nicht abstrakt aus der Datenkategorie, sondern aus dem Kontext der Verarbeitung ergibt (siehe 3.2.3.5, S. 299). Dennoch hat der Verordnungsgeber – wie auch schon in der Datenschutzrichtlinie, Art. 8 DSRL – in Art. 9 DS-GVO mit den besonderen Kategorien personenbezogener Daten eine Gruppe per se sensibler Daten definiert. Wie die Aufzählung in Art. 9 Abs. 1 DS-GVO zeigt, geht es dabei im Kern um absehbare, weil typischerweise eintretende Auswirkungen auf andere Grundrechte und Grundfreiheiten. Die Voraussetzungen für die Verarbeitung solch sensibler Daten werden vorrangig in Art. 9 Abs. 2 bis 4 DS-GVO behandelt; allgemein kann aber festgehalten werden, dass die Eingriffsintensität einer Datenverarbeitung umso höher ist, je mehr personenbezogene Daten besonderer Kategorien nach Art. 9 Abs. 1 DS-GVO verarbeitet werden. 935

3.4.1.3.3.2 Maßstab für die gleiche Eignung des Mittels

In die Erforderlichkeitsprüfung werden nur gleich geeignete Mittel einbezogen. Dabei muss der Verantwortliche zumindest in diesem Punkt (anders als ggf. im Rahmen der Angemessenheit) keine Abstriche hinsichtlich der Wirksamkeit der Datenverarbeitung machen. Mittel, mit denen der Zweck nicht optimal erfüllt werden kann, sind nicht in gleichem Maße geeignet und kommen darum als mildere Alternative nicht in Betracht.[1185] 936

An die Frage der Wirksamkeit schließt sich die nach der Wirtschaftlichkeit eines Mittels an, also nach den mit seinem Einsatz verbundenen Kosten. Hier kann prinzipiell nach demselben formalisierten Ansatz vorgegangen werden, mit dem auch die Eingriffsintensität ermittelt wird. Ebenso wie 937

1185 *Deutsch/Diller,* DB 2009, S. 1462, 1463; ähnlich *Zöll,* in: Taeger/Gabel 2019, § 26 BDSG, Rn. 25, demzufolge keine Abstriche in der Qualität der Zweckerfüllung hingenommen werden müssten. Zum Prinzip der Gleichwertigkeit der Alternativen allgemein BVerfG v. 14.11.1989 – 1 BvL 14/85, E 81, S. 70, 91 – *Rückkehrgebot für Mietwagen*.

sich die Verarbeitungsintensität mit jedem erhobenen Datum und jedem Verarbeitungsschritt erhöht, vermindert sich die Eignung eines Mittels mit jedem Cent mehr, den es kostet. Hier gilt derselbe rigorose Ansatz wie bei der Wirksamkeit des Mittels: Aufwändigere und in der Folge weniger wirtschaftliche Maßnahmen müssen vom Verantwortlichen bei der Suche nach milderen Maßnahmen nicht berücksichtigt werden.[1186]

938 Gegen diese enge Auslegung könnte die Formulierung in ErwG 39 S. 9 sprechen, der zufolge Daten nur verarbeitet werden sollten, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.[1187] Diese Passage muss aber nicht zwingend auf die Erforderlichkeit im engeren Sinne bezogen sein. Sie könnte auch vielmehr die Ansicht stützen, dass es im Rahmen der Datenminimierung einer umfangreichen Angemessenheitsprüfung bedarf (siehe 3.4.1.3.4.2, S. 380). Dies hat den Vorzug, dass die Prüfungsebenen nicht miteinander vermischt werden. Eine Datenverarbeitung ist folglich nicht erst dann erforderlich, wenn ihr Zweck andernfalls überhaupt nicht, d.h. auch nicht durch den Einsatz aufwändigerer Methoden, erreicht werden könnte.

939 Die Erforderlichkeit einer konkreten Datenverarbeitung ist vielmehr in der Kombination der beiden Merkmale zu ermitteln. Es kommt also nicht nur darauf an, welche Daten für eine bestimmte Arbeitsaufgabe gebraucht werden, d.h. ob sie überhaupt verarbeitet werden müssen. Es geht auch darum wie, d.h. mit welchem Datenverarbeitungssystem dies geschieht. So zählte bspw. in Fällen der elektronischen Datenverarbeitung auch, dass dadurch im Vergleich zur herkömmlichen „analogen" Methode Verwaltungsvereinfachungen realisiert werden konnten. Der Verantwortliche kann darum nicht allein mit dem Argument der mangelnden Erforderlichkeit auf die mildere „analoge" Alternative verwiesen werden.[1188] Ob er aber dennoch Einbußen hinsichtlich der Wirksamkeit oder Wirtschaftlichkeit der Datenverarbeitung hinnehmen muss, ist eine Frage der Angemessenheit.

1186 *Gola/Jaspers*, RDV 2009, S. 212–214; *Wybitul*, BB 2010, S. 1085. Zur Berücksichtigung des Aufwands des für die Maßnahme Verantwortlichen (in diesem Fall des Staates) allgemein BVerfG v. 16.3.1971 – 1 BvR 52/66, E 30, S. 292, 319 – *Erdölbevorratung*; BVerfG v. 6.10.1987 – 1 BvR 1086/82, E 77, S. 84, 110 – *Arbeitnehmerüberlassung*.

1187 So auch *Roßnagel*, in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 121.

1188 BAG v. 11.3.1986 – 1 ABR 12/84, E 51, S. 217, Rn. 37 (=NZA 1986, S. 526); BAG v. 22.10.1986 – 5 AZR 660/85, E 53, S. 226, Rn. 37 (=NZA 1987, S. 415).

3.4.1.3.4 Der Begriff der Angemessenheit

Den Abschluss der Prüfung der Datenminimierung bildet die Prüfung der Angemessenheit. Stärker noch als bei den anderen Merkmalen der Datenminimierung finden sich in der Kommentarliteratur bereits unterschiedliche Auffassungen über den Anwendungsbereich und den Inhalt der Angemessenheitsprüfung. Darüber hinaus steht auch hier die Frage des Maßstabs im Fokus des Interesses. 940

3.4.1.3.4.1 Inhalt der Angemessenheitsprüfung

Eine Meinung verortet die Angemessenheit – oder wie es Art. 5 Abs. 1 lit. c DS-GVO formuliert: die Anforderung, dass Daten dem Zweck angemessen sein müssen – als einen zweiten Vorfilter neben der Erheblichkeit bzw. Geeignetheit. So sollen Daten angemessen sein, wenn sie überhaupt einen Bezug zum Verarbeitungszweck haben.[1189] Wie der Vergleich mit dem Begriff in der englischen Sprachfassung „adequate" zeige, ginge es um die Zuordnung der Daten zu einem Zweck.[1190] 941

Demgegenüber steht das Verständnis der Zweckangemessenheit als Verhältnismäßigkeit im engeren Sinne. Es geht über die Zuordnung der Daten hinaus, indem es eine umfassende wertende Betrachtung verlangt, die sich auch auf den gesamten Umfang der Datenverarbeitung bezieht.[1191] Entsprechend des allgemeinen Begriffsverständnisses müsste hier der Grundsatz gelten, demzufolge die mit einer Maßnahme verbundenen Nachteile, nicht außer Verhältnis zu den Vorteilen stehen dürfen, welche die Maßnahme bewirkt. 942

Mit Blick auf den Gegenstand der Datenminimierung ist der umfassenden Auslegung der Vorzug zu geben. Die Meinung, wonach die Daten lediglich einen Bezug zum Verarbeitungszweck haben müssten, wäre nur dann konsequent, wenn es bei der Datenminimierung nur um die Beschränkung der Datenerhebung ginge. Weitet man aber den Gegenstand der Da- 943

1189 *Frenzel,* in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 35; *Herbst,* in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 57; *Kramer,* in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 39.

1190 *Reimer,* in: Sydow 2018, Art. 5 DS-GVO, Rn. 30.

1191 *Pötters,* in: Gola 2018, Art. 5 DS-GVO, Rn. 15; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 26; zu § 26 Abs. 1 BDSG 2018 *Kort,* ZD 2017, S. 319, 320; *Varadinek, et al.* 2018, S. 30 f.

tenminimierung auf alle Verarbeitungsphasen des Art. 4 Nr. 2 DS-GVO aus, muss auch die Angemessenheit entsprechend mit ausgeweitet werden. Sie kann also nicht auf die Datenerhebung beschränkt bleiben, sondern muss als umfassende Prüfung sicherstellen, dass die Nachteile, die mit der Verarbeitung für die betroffene Person verbunden sind, nicht außer Verhältnis zu den Vorteilen stehen, die der Verantwortliche aus der Verarbeitung zieht.

3.4.1.3.4.2 Das Verhältnis zu den Erlaubnistatbeständen

944 Folgt man der umfassenden Auslegung des Merkmals der Angemessenheit in Art. 5 Abs. 1 lit. c DS-GVO, so ergibt sich bereits aus dem Grundsatz der Datenminimierung selbst, dass jede Datenverarbeitung einer Angemessenheitsprüfung zu unterziehen ist. Die Grundsätze des Datenschutzrechts stellen eigenständige Rechtssätze mit einem eigenständigen Regelungsgehalt dar, der im Datenschutz durchgehend zu befolgen ist. Der Begriff der Grundsätze impliziert aber auch, dass durch speziellere Regelungen Ausnahmen formuliert werden können. Diese Ausnahmen könnten sich den einzelnen Erlaubnistatbeständen finden, die nicht durchgehend selbst eine Angemessenheitsprüfung vorsehen.

945 Eine Umschreibung der Angemessenheitsprüfung ist lediglich im Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO enthalten. Die Datenverarbeitung muss nicht nur erforderlich sein, um die berechtigten Interessen des Verantwortlichen oder eines Dritten zu wahren, die schützenswerten Interessen der betroffenen Person dürfen auch nicht überwiegen. Den anderen Erlaubnistatbeständen fehlt diese Umschreibung einer Angemessenheitsprüfung; die Datenverarbeitung muss dort lediglich zur Erreichung des jeweiligen Zwecks erforderlich sein. Insbesondere im Falle der für diese Untersuchung relevanten Verarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO wird darum die Meinung vertreten, dass es keiner Angemessenheitsprüfung bedürfe.[1192]

1192 *Assion et al.*, in: Gierschmann et al. 2018, Art. 6 DS-GVO, Rn. 88; *Ziegenhorn/Heckel*, NVwZ 2016, S. 1585, 1588; zur Parallelen Problematik in § 26 Abs. 1 S. 1 BDSG 2018 *Düwell/Brink*, NZA 2017, S. 1081, 1084; a.A. (d.h. für eine Angemessenheitsprüfung in § 26 Abs. 1 S. 1) *Kort*, RdA 2018, S. 24, 25; *Martini/Botta*, NZA 2018, S. 625, 629 f.; *Maschmann*, in: Kühling/Buchner 2018, § 26 BDSG, S. 18 f.; *Pötters*, in: Gola 2018, Art. 88 DS-GVO, Rn. 50.

3.4.1.3.4.2.1 Die Angemessenheitsprüfung in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO

Die Schlussfolgerung, es sei nur dann eine Angemessenheitsprüfung durchzuführen, wenn sich die Datenverarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO stützt, wird der Struktur der Erlaubnistatbestände in Art. 6 Abs. 1 DS-GVO sowie speziell der Eigenart des Tatbestands in UAbs. 1 lit. b nicht gerecht. 946

3.4.1.3.4.2.1.1 Die Struktur der Erlaubnistatbestände

Die Erlaubnistatbestände der Art. 6 Abs. 1 UAbs. 1 lit. b bis e DS-GVO regeln spezielle Konstellationen, aus deren Natur sich bereits die Berechtigung des Interesses des Verantwortlichen ergibt. Bei der Verarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO sind dies die einzelnen vertraglichen Pflichten, die von den Parteien im Einvernehmen begründet wurden. Dabei spielt es keine Rolle, ob es sich um Hauptleistungspflichten, Nebenleistungspflichten nach § 242 BGB oder Rücksichtnahmepflichten nach § 241 Abs. 2 BGB handelt.[1193] Die Erfüllung dieser Pflichten ist a priori ein berechtigtes Interesse des Verantwortlichen.[1194] 947

Dies allein rechtfertigt jedoch nicht, auf eine abschließende Angemessenheitsprüfung zu verzichten. Schließlich wird auch in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO beides verlangt: ein berechtigtes Interesse und eine aus Sicht des Verantwortlichen positive Interessenabwägung. Allein der Umstand, dass ein Vertrag vorliegt, hilft dem Rechtsanwender lediglich über die Prüfung hinweg, ob ein berechtigtes Interesse des Verantwortlichen besteht. Die positive Interessenabwägung, die im Fall des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO gesondert vorzunehmen ist, ist im Fall des Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO in der Vertragsauslegung enthalten. Sie gliedert sich in zwei Kontrollinstrumente, die in ihrem Zusammenspiel erst die Gewähr dafür bieten, dass die Grundrechte der betroffenen Person und insbesondere ihr 948

1193 BeckOK DSR/*Albers/Veit*, Art. 6 DS-GVO, Rn. 31; *Assion et al.*, in: Gierschmann et al. 2018, Art. 6 DS-GVO, Rn. 91; *Buchner/Petri*, in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 33; zur Abgrenzung dieser Pflichten, siehe 2.3.4, S. 163.

1194 BeckOK DSR/*Albers/Veit*, Art. 6 DS-GVO, Rn. 31; *Buchner/Petri,* in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 33.

Recht auf Schutz ihrer personenbezogenen Daten hinreichend berücksichtigt.

3.4.1.3.4.2.1.2 Die angemessene Ausgestaltung der vertraglichen Pflichten

949 Das erste Instrument betrifft die nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO zu erfüllenden vertraglichen Pflichten. Sind sie angemessen ausgestaltet, also so, dass den Vorteilen der einen Vertragspartei keine unverhältnismäßigen Nachteile der anderen Vertragspartei gegenüberstehen, führt dies mit einiger Wahrscheinlichkeit dazu, dass auch die zur Erfüllung dieser Pflichten notwendige Datenverarbeitung selbst angemessen ist.

950 Die angemessene Gestaltung der vertraglichen Pflichten nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO ist in erster Linie die Sache der Parteien. Wo dies, wie im Beschäftigungsverhältnis, aufgrund bestehender Machtungleichgewichte nicht angenommen werden kann, greifen Schutzinstrumente wie die AGB-Kontrolle oder die Billigkeitskontrolle nach § 106 S. 1 GewO oder § 315 Abs. 3 BGB (zu den genauen Auswirkungen dieser Instrumente auf den Prüfungsaufbau, siehe 3.6.1.2.1.2, S. 493).

951 Wo vertragliche Pflichten nicht von vornherein so bestimmt sind, dass sie zu angemessenen Ergebnissen führen, ist dies im Wege der Vertragsauslegung sicherzustellen. Hier gilt der Grundsatz, dass sich die vertraglichen Pflichten dort, wo weder zwingende gesetzliche Vorgaben noch sich auf diese Pflicht beziehende Absprachen zwischen den Parteien bestehen, nach der konkreten Situation unter Abwägung der beiderseitigen Interessen bestimmen.[1195]

952 Diese Schutzinstrumente stehen nicht im Konflikt mit der einheitlichen Geltung der Datenschutz-Grundverordnung. Sie betreffen den jeweils der Datenverarbeitung zugrundeliegenden Lebenssachverhalt, der selbst nicht von der Datenschutz-Grundverordnung geregelt wird. Das Datenschutzrecht enthält keine genauen Anforderungen an die Legitimität der konkreten Zweckfestlegung und akzeptiert stattdessen die hierauf gerichteten Schutzinstrumente aus den Regelungen über den jeweiligen Lebenssachverhalt als vorbestehend. Die Schutzinstrumente, die speziell das Arbeitsrecht betreffen, liegen außerhalb der Geltung der EU-Grundrechte (siehe 3.2.2.4, S. 278), weshalb insofern kein Konflikt besteht.

1195 BGH v. 30.9.2009 – VIII ZR 238/08, NJW 2010, S. 1135, 1136 f.

Das Schutzinstrument der AGB-Kontrolle steht der einheitlichen Geltung des Europarechts schließlich auch deswegen nicht entgegen, weil es selbst auf europarechtlichen Vorgaben beruht (dazu auch 3.4.1.4.4.1, S. 397). Die Bindung an Treu und Glauben ist in Art. 3 der Klausel-RL 93/13/EWG geregelt. 953

3.4.1.3.4.2.1.3 Allgemeine Rücksichtnahmepflichten

Das zweite, die Prüfung abschließende Instrument betrifft die Datenverarbeitung selbst. Die verarbeitende Vertragspartei unterliegt hierbei der Rücksichtnahmepflicht, die im deutschen Recht in § 241 Abs. 2 BGB verankert ist, und u.a. darin besteht, die informationelle Selbstbestimmung der anderen Partei zu wahren.[1196] Die Datenverarbeitung selbst muss also rücksichtsvoll und damit im Ergebnis auch angemessen sein. 954

Dieser Weg dürfte allerdings durch den Anwendungsvorrang des europäischen Rechts versperrt sein. Für eine solche Sperrwirkung genügt es aber nicht, dass diese Pflicht den Bereich des europäisch geregelten Datenschutzrechts betrifft. Ob es auf der Ebene des europäischen Primär- und Sekundärrechts allgemeine Grundsätze wie Treu und Glauben oder Rücksichtnahmepflichten gibt, ist angesichts der mangelnden europäischen Kodierung des Privatrechts zweifelhaft.[1197] Insofern können zumindest diese allgemeinen Grundsätze nicht durch europäisches Recht verdrängt werden.[1198] 955

Es spricht aber viel dafür, dass die Regelungen der Datenschutz-Grundverordnung das punktuelle Gebot nach Treu und Glauben zu handeln in Art. 8 Abs. 2 S. 1 GRC[1199], nämlich personenbezogene Daten nach Treu und Glauben zu verarbeiten, konkretisieren. Die Datenschutz-Grundverordnung nimmt sich zugunsten des mitgliedstaatlichen Vertragsrechts nur dort zurück, wo sie wie in der gerade diskutierten Zwecksetzung anhand vertraglicher Pflichten (siehe 3.4.1.3.4.2.1.2, S. 382) an dieses Vertragsrecht anknüpft. Bei der Datenverarbeitung selbst ist dies jedoch nicht der Fall. Dadurch werden die allgemeinen Regeln zumindest im Hinblick auf das 956

1196 MHdB ArbR/*Reichold*, § 96, Rn. 5.
1197 Zu Treu und Glauben BeckOGK/*Kähler*, § 242 BGB, Rn. 280 m.w.N.; a.A. *Metzger* 2012, S. 349.
1198 Zu Treu und Glauben BeckOGK/*Kähler*, § 242 BGB, Rn. 307.
1199 So auch BeckOGK/*Kähler*, § 242 BGB, Rn. 280.

Datenschutzrecht entsprechend des Anwendungsvorrangs europäischen Rechts verdrängt.

957 Dennoch gilt es zu beachten, dass Rücksichtnahmepflichten nicht nur dem deutschen Schuldrecht immanent sind, sondern sich in vielen nationalen Rechtstraditionen der Mitgliedstaaten der Europäischen Union wiederfinden.[1200] Ein solches Vertragsverständnis liegt darum auch Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO zugrunde. Dies muss bei der Auslegung dieses Erlaubnistatbestands berücksichtigt werden.

958 Es wurde oben (siehe 3.4.1.3.4.2.1.2, S. 382) bereits erläutert, dass die angemessene Vertragsauslegung der mit der Datenverarbeitung zu erfüllenden Pflicht an die Stelle der berechtigten Interessen in der Generalklausel nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO tritt. Die Rücksichtnahmepflichten erklären die zweite „Lücke", die Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO im Vergleich zu der Generalklausel aufweist: die abschließende Interessenabwägung. Legt man dem Erlaubnistatbestand in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO das Verständnis eines vertraglichen Schuldverhältnisses zugrunde, das auch Elemente einer Interessenabwägung kennt, wird deutlich, dass die Nichterwähnung dieses Aspekts im Wortlaut der Norm nicht dazu führen soll, dass die Interessenabwägung in Art. 5 Abs. 1 lit. c DS-GVO entfällt.

959 Entsprechend der horizontalen Abgrenzung der Grundrechtsebenen (siehe 3.2.2.5.2, S. 281) ist die Interessenabwägung im Rahmen der Datenverarbeitung zur Vertragserfüllung anhand der europäischen Grundrechte vorzunehmen.

3.4.1.3.4.2.1.4 Ergebnis

960 Im Ergebnis zeigt sich, dass aus der fehlenden Erwähnung einer abschließenden Interessenabwägung in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO nicht der Schluss gezogen werden kann, dass es keiner Angemessenheitsprüfung bedürfe.[1201] Vertragliche Pflichten können sowohl bei ihrer Gestaltung als auch bei ihrer Auslegung einer Interessenabwägung unterliegen, weshalb auch die im Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c

1200 *Bar/Zimmermann* 2002, S. 112 ff.

1201 In die Richtung auch BeckOK DSR/*Albers/Veit*, Art. 6 DS-GVO, Rn. 32; für den Beschäftigtendatenschutz *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 63; *Gola*, BB 2017, S. 1462, 1464. Davon geht auch der deutsche Gesetzgeber in Bezug auf § 26 Abs. 1 S. 1 BDSG 2018 aus, BT-Drucks. 18/11325, S. 97.

DS-GVO enthaltene Angemessenheitsprüfung für die Datenverarbeitung zur Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO kein Fremdkörper ist.

3.4.1.3.4.2.2 Die Angemessenheitsprüfung in den übrigen Erlaubnistatbeständen

961 Die anderen Erlaubnistatbestände der Art. 6 Abs. 1 UAbs. 1 lit. a und c bis e DS-GVO stehen nicht im Fokus dieser Untersuchung. Dass bei ihnen ebenfalls keine abschließende Interessenabwägung eigens angeordnet ist, lässt sich aber auf ähnliche Weise wie bei der Verarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO erklären:

- In den meisten Fällen der Einwilligung werden zwischen dem Verantwortlichen und der betroffenen Person bereits vertragliche Beziehungen bestehen. Wo dies keine Leistungsbeziehungen sind, wird man doch jedenfalls ein Schuldverhältnis nach § 311 Abs. 2 BGB annehmen können.
- Als Verpflichtungen nach Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO kommen nur solche in Betracht, die dem Verantwortlichen von einer staatlichen Stelle aufgegeben werden.[1202] Eine rechtliche Verpflichtung des Verantwortlichen, die im Ergebnis zu einer unangemessenen Datenverarbeitung führt, ist selbst unangemessen und damit verfassungswidrig.[1203]
- Soweit lebenswichtige Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. d DS-GVO betroffen sind, ist nur schwer vorstellbar, dass eine erforderliche Datenverarbeitung unangemessen sein könnte. Hier wurde die typische Interessenabwägung vorweggenommen.
- Der öffentliche Aufgabenträger nach Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO ist grundrechtsgebunden, weshalb er ohnehin eine Angemessenheitsprüfung vornehmen muss.

1202 BeckOK DSR/*Albers/Veit*, Art. 6 DS-GVO, Rn. 34; *Assion et al.*, in: Gierschmann et al. 2018, Art. 6 DS-GVO, Rn. 92 ff.; *Buchner/Petri,* in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 77.

1203 Ähnlich *Assion et al.,* in: Gierschmann et al. 2018, Art. 6 DS-GVO, Rn. 98.

3.4.1.3.4.3 Der Maßstab der Angemessenheitsprüfung

962 Der Maßstab der Angemessenheitsprüfung wird im Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO nicht definiert. Der Datenschutz-Grundverordnung lässt sich lediglich entnehmen, welche Kriterien der Interessenabwägung zugrunde zu legen sind. In der Sache geht es um eine risikoorientierte Betrachtung, was sich u.a. an der Regelung zum technischen Datenschutz in Art. 25 Abs. 1 DS-GVO (siehe 3.4.2.2.4, S. 439) zeigt, in der ausdrücklich auf dieses Prinzip zurückgegriffen wird. Unklar ist aber, wie und nach wessen Vorstellungen diese Kriterien zu gewichten sind.

3.4.1.3.4.3.1 Unterscheidung nach Erlaubnistatbeständen

963 Dies dürfte dem Umstand geschuldet sein, dass der Grundsatz auf sämtliche Erlaubnistatbestände Anwendung findet, die jeweils unterschiedliche Konstellationen erfassen. Es liegt darum nahe, den Angemessenheitsmaßstab für jeden Erlaubnistatbestand einzeln festzulegen. Dieser Ansatz wird dadurch bekräftigt, dass die Vorgaben der Datenschutz-Grundverordnung, zumindest soweit sie den Abwägungsmaßstab betreffen, dispositiv sind. Das zeigt sich allein schon daran, dass die betroffene Person die Datenverarbeitung auch durch ihre Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO legitimieren kann.

964 Bei der hier besonders relevanten Interessenabwägung im Rahmen der Verarbeitung zur Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO ist zu berücksichtigen, dass die beteiligten mit dem Vertragsschluss die maßgebliche Verarbeitungsgrundlage einvernehmlich geschaffen haben. Daraus lässt sich ableiten, dass auch die Interessenabwägung nach ihren gemeinsamen Vorstellungen vorzunehmen ist. Bei der Interessenabwägung in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO gilt darum kein objektiver[1204], sondern ein übereinstimmend subjektiver Maßstab.

1204 Für einen objektiven Maßstab in Art. 5 Abs. 1 lit. c DS-GVO ohne eine Differenzierung nach Erlaubnistatbeständen, *Roßnagel*, in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 119; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 26.

3.4.1.3.4.3.2 Orientierung an Verkehrssitten

Der beschriebene übereinstimmend subjektive Maßstab der Angemessenheitsprüfung wirkt auch in dem Fall, dass sich der tatsächliche Wille der Parteien nicht ermittelt lässt. Soweit dem keine tatsächlichen Anhaltspunkte entgegenstehen, ist davon auszugehen, dass die Parteien ihren vertraglichen Beziehungen denjenigen Abwägungsmaßstab zugrunde gelegt haben, den sie auf dem Markt, in dem sie agieren, vorgefunden haben.[1205] Im Zweifel ist der Angemessenheitsprüfung darum die herrschende Verkehrssitte zugrunde zu legen. *965*

Die Verkehrssitte zu ermitteln ist zwar keine Frage des Einzelfalls, wohl aber der jeweiligen Branche und der typischen Verarbeitungssituation. Ihre Entstehung hängt von vielen Faktoren ab und lässt sich – wie Fehleinschätzungen der Vergangenheit zeigen[1206] – kaum abstrakt beschreiben. Neben dem typischerweise in der jeweiligen Branche bestehenden Risiko spielen hier Aspekte wie die Kommerzialisierbarkeit des Produkts, die Erwartungen der betroffenen Personen und speziell deren Zahlungsbereitschaft eine Rolle. Denkbar ist auch, dass staatliche Regulierung die Mindeststandards einer Branche hebt. Allgemeingültige Aussagen können hier jedenfalls kaum getroffen werden. Zumindest hinsichtlich des Aufwands, der dem Verantwortlichen typischerweise zugemutet werden kann, um die Verarbeitung personenbezogener Daten möglichst zu vermeiden oder wenigstens einzuschränken, lässt sich aber eine Richtung erkennen. *966*

Augenfällig ist, dass sich in Bereichen, in denen ein professionelles Interesse an der Datenverarbeitung besteht und in denen der Kontext der Verarbeitung ohne Weiteres als besonders sensibel erkennbar ist, etwa im Bereich der Lohnbuchhaltung, sehr strenge Verkehrssitten herausgebildet haben. Umgekehrt zeigt die Entwicklung im Bereich sozialer Netzwerke, dass sich im privaten Bereich und wenn sich die Gefahren der Datenverarbeitung nicht auf den ersten Blick erschließen, auch vergleichsweise niedrige Standards etablieren können. Beim letztgenannten Beispiel könnte man aber auch mit guten Argumenten daran zweifeln, ob hier die gängi- *967*

1205 Zur Situation im deutschen Recht MüKo BGB/*Bachmann*, § 241 BGB, Rn. 55.

1206 So wurde auf Grundlage von Umfragen prognostiziert, dass das Fehlen datenschutzfreundlicher Bezahlsysteme ein Wachstumshindernis für den Online-Handel darstellen werde, *Grimm et al.*, DuD 1999, S. 272.

gen Marktmechanismen funktionieren, also ob dies wirklich die Vorstellungen des Verkehrs oder nicht vielmehr die eines Monopolisten sind.[1207]

968 In jedem Fall entspricht es aber dem Wesen einer Verkehrssitte, dass sie das Verhalten abbildet, wie es unter den am Rechtsverkehr Beteiligten üblich ist. Sie dürfte also in der Regel daraus bestehen, übliche weithin anerkannte und erprobte Methoden anzuwenden. Das Datenschutzrecht knüpft über das Regelungsinstrument des Erforderlichkeitsprinzips hieran an. Unter gewissen Bedingungen muss davon aber nach den Regeln zum technischen Datenschutz nach Art. 25 Abs. 1 DS-GVO abgewichen werden (siehe 3.4.2.2.5, S. 444).

3.4.1.3.5 Fazit: In der Regel kein Optimierungsgebot

969 Das Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO erstreckt sich auf sämtliche Verarbeitungsvorgänge und unterwirft diese einer Verhältnismäßigkeitsprüfung. Teil dieser Prüfung ist auch eine Angemessenheitsprüfung, die im Rahmen aller Erlaubnistatbestände vorzunehmen ist. Dies gilt auch für Erlaubnistatbestände wie denjenigen für die Verarbeitung zur Vertragserfüllung in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO, deren Wortlaut keine Interessenabwägung erwähnt.

970 Der Interessenabwägung im Rahmen der Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO ist der übereinstimmend subjektive Maßstab der Vertragsparteien zugrunde zu legen. Dies hat zur Folge, dass im Zweifel auf die Verkehrssitte in der jeweiligen Branche abzuheben ist. Im Zusammenspiel mit der Erforderlichkeitsprüfung, bei der jeder Mehraufwand die gleiche Eignung eines Mittels beseitigt, bedeutet dies, dass der Verantwortliche keinen über das übliche Maß hinausgehenden Aufwand in Kauf nehmen muss, um die Verarbeitung personenbezogener Daten zu vermeiden oder zu beschränken.

971 Dem Prinzip der Datenminimierung kann folglich kein Optimierungsgebot entnommen werden. Der Verantwortliche muss nicht besonders sorgfältig oder besonders innovativ sein oder in sonst einer Kategorie aus der Masse der anderen Verantwortlichen in seiner Branche herausragen. Er darf sich darauf beschränken, das zu tun, was hier üblich ist – in der Regel

1207 Siehe das Kartellverfahren gegen Facebook, *BKartA* 2017; BGH v. 23.6.2020 – KVR 69/19, Z 226, S. 67–116 – *Facebook I*; BGH, ECLI:DE:BGH:2020:151220BKVZ90.20.0.

wird das darauf hinauslaufen, gängige und erprobte Methoden anzuwenden.

3.4.1.4 Das Zusammenspiel von Zweckbindung und Datenminimierung

Die Prinzipien der Zweckbindung in Art. 5 Abs. 1 lit. b und der Datenminimierung in Art. 5 Abs. 1 lit. c DS-GVO stehen in einem derart engen Verhältnis zueinander,[1208] dass sie sich in ihrer genauen Ausgestaltung gegenseitig beeinflussen. Sie lassen sich darum am besten in diesem Zusammenwirken erläutern. Das gilt insbesondere für die Fragen, wie stark ein Zweck zu konkretisieren und wie streng der Maßstab der Datenminimierung zu handhaben ist. Die Auslegung der beiden Merkmale bestimmt maßgeblich darüber, wieviel Spielraum dem Verantwortlichen bei der Entscheidung über Art und Umfang der Datenverarbeitung zu gewähren ist. 972

Diese Fragen sind vor allem im Hinblick auf die Datenverarbeitung im Beschäftigungsverhältnis umstritten und werden im weiteren Verlauf der Untersuchung eine wichtige Rolle spielen. Sie sollen darum hier zunächst in ihrer allgemeinen Bedeutung vertieft untersucht werden. 973

3.4.1.4.1 Die Problemstellung

Die Wechselwirkung, in der die Zweckbindung und die Datenminimierung zueinanderstehen, liegt darin begründet, dass der gemäß Art. 5 Abs. 1 lit. b DS-GVO festzulegende Zweck den Bezugspunkt der nach Art. 5 Abs. 1 lit. c DS-GVO vorzunehmenden Erforderlichkeitsprüfung bildet. Je strenger also der Maßstab der Erforderlichkeitsprüfung ausfällt, desto stärker wird die Verarbeitung an ihren Erhebungszweck gebunden. Und umgekehrt gilt, dass der Ergebniskorridor der Erforderlichkeitsprüfung umso schmaler wird, je konkreter der Zweck festgelegt ist. 974

1208 So auch *Herbst,* in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 56.

3.4.1.4.1.1 Unklarer Ausgangspunkt für die Prüfung der Datenverarbeitung zur Vertragserfüllung

975 Dieser Zusammenhang ist im Grunde trivial und wäre nicht weiter erwähnenswert. Bei der Datenverarbeitung zur Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO sieht man sich aber dem Problem gegenüber, dass hier – anders als bei den übrigen Erlaubnistatbeständen (siehe 3.4.1.2.4.2, S. 369) – nicht klar ist, inwieweit der Zweck konkretisiert werden muss. Wenn man aber lediglich auf den Vertrag an sich als Zweck und Bezugspunkt der datenschutzrechtlichen Prüfung abstellt, gelangt man kaum zu belastbaren Aussagen. Eine datenschutzrechtliche Prüfung ist kein mechanisch ablaufender Vorgang, sondern eine umfassende Interessenabwägung, die ebenso komplex ausfällt, wie der Lebenssachverhalt, der dadurch geregelt werden soll.

976 Bei einem simplen Kaufvertrag mag es noch auf der Hand liegen, welche Datenverarbeitung zu seiner Erfüllung notwendig und also gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO zulässig ist. Aber schon bei komplexeren Situationen, wie sie vor allem in Dauerschuldverhältnissen auftreten, ist dies nicht mehr der Fall. Was zur Erfüllung eines Arbeitsvertrags erforderlich ist oder welche Qualifikationen für eine ausgeschriebene Stelle relevant sind,[1209] lässt sich im Detail nicht ohne weiteres objektiv feststellen.[1210]

3.4.1.4.1.2 Problem bei Assistenzsystemen

977 Zu welchen Problemen die Bestimmung der zur Vertragserfüllung erforderlichen Datenverarbeitung führt, soll in Anlehnung an die verschiedenen Arten von Assistenzsystemen (siehe 1.3.2, S. 71) anhand von drei Beispielen verdeutlicht werden, die im späteren Verlauf dieser Arbeit wieder aufgegriffen werden (siehe 3.6.1.2.1.4.2, S. 502).

– Bei einem System, das Arbeitnehmern kontextsensitiv die relevanten Informationen zur Produktion einblenden soll, kommt es maßgeblich darauf an, anhand welcher Merkmale der Kontext bestimmt wird. Frag-

---

1209 Zur vorratsweisen Erhebung von Daten über die Qualifikation von Bewerbern BAG v. 22.10.1986 – 5 AZR 660/85, E 53, S. 226, Rn. 38 f. (=NZA 1987, S. 415).

1210 *Däubler,* in: Däubler et al. 2016, § 32 BDSG, Rn. 9; *Schmitz* 2016, S. 187; *Stamer/Kuhnke,* in: Plath 2016, § 32 BDSG, Rn. 10; *Thüsing,* NZA 2009, S. 865, 869; allgemein *Buchner/Petri,* in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 39 f.

lich ist nun, ob es erforderlich ist, zu diesen Merkmalen auch Informationen über den Beschäftigten mit hinzuzunehmen – etwa seine räumliche Position in der Fabrik, sein bisheriger Erfahrungs- und Wissensstand, seine Nutzungspräferenzen oder die Aufträge, die er als nächstes zu erledigen hat.

- Bei einem System, welches automatisch Arbeitsaufträge (z.B. die Reparatur eines Defekts einer Maschine) ermittelt und sie unter den Beschäftigten in der Fabrik verteilt, ist es durchaus denkbar, Informationen über die einzelnen Mitarbeiter in die Entscheidung einzubeziehen, wem von ihnen der Auftrag erteilt wird. Dies können z.B. seine zeitliche Verfügbarkeit oder die zurückzulegende Wegstrecke zum Einsatzort sein oder die Güte und Schnelligkeit, mit der er bisher vergleichbare Aufgaben erfüllt hat. Die Aufgabe könnte aber auch schlicht an den nächsten freien Mitarbeiter vergeben werden – unabhängig davon, wo er sich befindet und als wie kompetent er sich in der Vergangenheit erwiesen hat.
- Bei einem Leichtbauroboter, der direkt mit dem Beschäftigten interagiert und ihm schwere Lasten abnimmt oder diese besser positioniert, kann es darauf ankommen, Daten über den mit dem Roboter interagierenden Beschäftigten zu verarbeiten, etwa seine Körpergröße oder seine Position zur Maschine im Raum. Statt der Roboter könnten aber auch z.B. manuell bediente Hebebühnen die Lasten tragen oder am Körper getragene „passive" Exoskelette, die statt sensorgesteuerter Motorik nur Federmechanismen einsetzen,[1211] den Mitarbeiter in unbequemen Körperhaltungen unterstützen.

In diesen Fällen liegt das Ergebnis der Prüfung angesichts der Komplexität des der Datenverarbeitung zugrundeliegenden Lebenssachverhalts nicht auf der Hand. Für die Konkretisierung der datenschutzrechtlichen Anforderungen ist es darum umso wichtiger, wie die hierzu verwendete Prüfung gestaltet wird. Dabei geht es vor allem um die Frage, in welchem Prüfungspunkt für die Konkretisierung maßgeblich anzusetzen ist. 978

3.4.1.4.1.3 Berücksichtigung eines ggf. bestehenden Entscheidungsspielraums

Bei der Klärung des Verhältnisses von Zwecksetzung und Erforderlichkeitsprüfung gilt es zusätzlich zu beachten, dass dem Verantwortlichen bei 979

1211 *Martini/Botta,* NZA 2018, S. 625, 626.

den Entscheidungen über die Datenverarbeitung ggf. ein gewisser Spielraum zugebilligt werden muss. Ob und in welchen Umfang dies zu geschehen hat, wird maßgeblich von den Wertungen desjenigen Rechtsgebiets beeinflusst, das den Lebenssachverhalt regelt, welcher der Datenverarbeitung zugrunde liegt. Allein auf der Grundlage des Datenschutzrechts, ohne Kenntnisse etwa des Arbeitsrechts, können hier keine werthaltigen Aussagen getroffen werden.

980 Zur Reichweite des Spielraums des Arbeitgebers soll unter dem Punkt 3.6.1.2.1 (S. 491) umfassend Stellung genommen werden. Zunächst stellt sich aber die Frage, mit welcher Vorgehensweise die spezifisch datenschutzrechtlichen Anforderungen konkretisiert werden können und wo dabei ein ggf. bestehender Spielraum des Verantwortlichen zu verorten ist.

3.4.1.4.2 Ansatzpunkte für die Konkretisierung der Anforderungen aus Zweckbindung und Datenminimierung

981 Die Anforderungen der Grundsätze der Zweckbindung und Datenminimierung nach Art. 5 Abs. 1 lit. b und c DS-GVO erklären sich nur aus ihrem Zusammenspiel. Will man diese Anforderungen an die Datenverarbeitung konkretisieren, bieten sich drei Ansatzpunkte: die Konkretisierung des Zwecks, die Konkretisierung des Erforderlichkeitsmaßstabs oder die Berücksichtigung des Problems ausschließlich in der Angemessenheitsprüfung.

3.4.1.4.2.1 Festlegen konkreter Zwecke

982 Der erste Ansatzpunkt betrifft die Zwecksetzung. Im Rahmen der dortigen Erforderlichkeitsprüfung werden nur jene Mittel miteinander verglichen, die zur Zweckerreichung gleich geeignet, also insbesondere gleich wirksam sind (siehe 3.4.1.3.3.2, S. 377). Je genauer der Zweck vorgegeben ist, desto deutlicher können Mittel in ihrer Wirksamkeit voneinander unterschieden werden. Entsprechend schrumpft die Palette der gleich geeigneten und darum überhaupt erst auf ihre Eingriffsintensität zu prüfenden Mittel. Die Konkretisierung des Zwecks kann vorentscheidend sein für die Frage, welche Vorgaben sich aus dem Grundsatz der Datenminimierung ableiten lassen.

983 In den oben genannten Beispielen (siehe 3.4.1.4.1.2, S. 390) könnte der Zweck also darin liegen, ein personalisiertes System zur Entscheidungsfin-

dung bzw. ein standortbasiertes System zur Verteilung von Wartungsaufträgen zu betreiben.

Wer die Befugnis hat, den Zweck zu setzen, steuert hierdurch zu einem gewissen Maß, welche Anforderungen für Datenverarbeitung aus dem Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO folgen. Die Frage nach der Zweckkonkretisierung beinhaltet darum immer auch die Frage, nach welchen Maßstäben und nach wessen Vorstellungen die Anforderungen des Prinzips der Datenminimierung an die Datenverarbeitung zu konkretisieren sind. In diesem Rahmen wäre auch ein eventueller Spielraum des Verantwortlichen zu diskutieren. Die gerichtliche Kontrolle beschränkte sich dann auf die Grenzen dieses Spielraums, den aufgrund der Zwecksetzung weiteren oder schmaleren Ergebniskorridor der Erforderlichkeitsprüfung sowie die Angemessenheitsprüfung. 984

3.4.1.4.2.2 Konkretisierung des Erforderlichkeitsmaßstabs

Die Konkretisierung der Anforderungen des Grundsatzes der Datenminimierung könnte aber auch im Rahmen der Erforderlichkeitsprüfung vorgenommen werden. Für den Verantwortlichen ist es nämlich keinesfalls zwingend, den Zweck zu konkretisieren, er könnte ihn stattdessen auch nur sehr abstrakt festsetzen (siehe 3.4.1.2.4, S. 368). Im Fall des Arbeitnehmerdatenschutzes würde dies bedeuten, den Zweck schlicht mit der Durchführung des Arbeitsverhältnisses an sich festzulegen. 985

Die Konkretisierung der Anforderungen der Datenminimierung müsste dann im Rahmen der Erforderlichkeitsprüfung erfolgen. Dabei wird man aber nicht selten Schwierigkeiten haben, zu bestimmen, welche Handlungen zur Erreichung des arbeitstechnischen Zwecks überhaupt vorgenommen werden müssen. Bei einem strengen Erforderlichkeitsmaßstab käme man jedenfalls zu dem Ergebnis, dass in den oben genannten Beispielen (siehe 3.4.1.4.1.2, S. 390) eine Personalisierung bzw. die Verarbeitung der Standortdaten nicht erforderlich wäre, weil sich Anweisungen schließlich auch so – im Zweifel wie bisher auch – erteilen ließen. Man könnte hier lediglich argumentieren, dass die Anweisungen weniger gut sind, weil sie nicht den kompletten Kontext erfassen bzw. denjenigen betreffen, der die zu verteilende Aufgabe am schnellsten erledigen könnte. Der konkrete Nutzen „verbesserter“ Anweisungen müsste aber womöglich vom Arbeitgeber belegt werden. 986

Will man dort dem Verantwortlichen dagegen einen gewissen Spielraum zubilligen, könnte dazu der Maßstab der Erforderlichkeit gelockert wer- 987

den. Statt von ihrer Unabdingbarkeit zur Zweckerreichung, die den Spielraum des Verantwortlichen einengen würde, könnte man sich stattdessen mit der bloßen Nützlichkeit der Datenverarbeitung begnügen. Denkbar wäre auch die Erforderlichkeit des Mitteleinsatzes nicht objektiv, sondern subjektiv nach den Vorstellungen des Verantwortlichen zu prüfen. Die Prüfung wäre dann weniger streng und würde sich in wesentlichen Punkten damit zufriedengeben, dass der Verantwortliche etwas für erforderlich hält.

3.4.1.4.2.3 Verlagerung in die Angemessenheitsprüfung

988 Die Konkretisierung der Anforderungen könnte schließlich auch in die abschließende Angemessenheitsprüfung verlagert werden. Problematisch ist hier aber schon, dass keinem Beteiligten einseitig Zugriff auf den Maßstab der Angemessenheitsprüfung gestattet werden kann. Einen gewissen Spielraum für den Verantwortlichen, wie er sich u.U. bei der Zwecksetzung oder der Erforderlichkeitsprüfung berücksichtigen ließe, kann es hier nicht geben.

989 Die Angemessenheitsprüfung ist auch aus einem anderen Grund untauglich. Sie soll verhindern, dass die konsequente Anwendung der vorgeschalteten Prüfungsschritte zu untragbaren Ergebnissen führt. Das bedeutet aber nicht, dass man dann auf eine genauere Zweckfestlegung oder eine Prüfung der Erforderlichkeit anhand eines bestimmten Maßstabs verzichten könnte. Dies birgt die Gefahr, dass im Grunde jede Datenverarbeitung als zur Zweckerreichung erforderlich angesehen würde, und die eigentliche Prüfung des Grundsatzes der Datenminimierung allein im Rahmen der Angemessenheit stattfände. Dadurch würde das Kriterium der Angemessenheit überfrachtet und in seiner Leistungsfähigkeit überschätzt. Es steht auch zu befürchten, dass letztlich Datenverarbeitungen die Zulässigkeit attestiert wird, die auch ohne relevanten Mehraufwand seitens des Verantwortlichen grundrechtsschonender hätten gestaltet werden können.

3.4.1.4.3 Inhärente Grenzen der Konkretisierung

990 In jedem Fall muss klar sein, dass dem jeweils anderen Prüfungspunkt noch ein sinnvoller Anwendungsbereich verbleibt. Dies beschränkt den Verantwortlichen in zwei Richtungen bei der Zwecksetzung.

Der Zweck darf zum einen nicht so konkret und kleinteilig festgelegt werden, dass die Erforderlichkeitsprüfung lediglich das Ergebnis zu Tage fördern kann, dass jene Daten erhoben werden müssen, die auch erhoben werden sollen. Das wäre etwa der Fall, wenn man den Zweck darauf konkretisiert, ein bestimmtes Ziel mithilfe eines konkreten und in jedem Detail feststehenden Datenverarbeitungssystems zu erreichen. Die Daten würden dann nicht deswegen verarbeitet, weil dies zur Zielerreichung objektiv notwendig wäre, sondern schlicht, weil es in der Konzeption des Datenverarbeitungssystems so vorgesehen ist. Die Erforderlichkeitsprüfung würde dadurch inhaltlich entleert. 991

Umgekehrt darf der Zweck zum anderen nicht auf abstrakte Begriffe beschränkt werden. Dies gilt schon allein deswegen, weil die Zweckbindung sonst nicht gewährleistet werden könnte. Hier kann auf die Argumente verwiesen werden, die bereits zu der Frage diskutiert wurden, welche Anforderungen an die Zwecksetzung aus den Regelungen zur Zweckbindung erwachsen (3.4.1.2.3.4, S. 367). Daraus ergibt sich zumindest die praktische Anforderung, den Zweck über die Rechtsgrundlage hinaus zu konkretisieren. 992

3.4.1.4.4 Zwecksetzung bei der Verarbeitung zur Vertragserfüllung

Die Literatur ist hinsichtlich der weiteren Konkretisierung der Verarbeitungsgrundlage unentschieden. Eine Meinung geht davon aus, dass jedem Vertragstyp ein Kern charakteristischer Leistungen zugeordnet werden müsse, der möglichst eng zu fassen sei. Der Vertrag als Verarbeitungsgrundlage soll demnach durchaus konkretisiert werden.[1212] Hierzu soll aber offenbar nicht der Wille der Parteien herangezogen werden, sondern ein objektiv zu ermittelnder idealtypischer Vertragsinhalt.[1213] An die so zu ermittelnden vertraglichen Leistungen knüpfe dann die Erforderlichkeits- 993

1212 *Buchner/Petri,* in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 39 gehen vom konkreten Zweck des rechtsgeschäftlichen Schuldverhältnisses aus. Irreführen wäre es darum, diese Auffassung als „abstrakten Vertragsbegriff" zu bezeichnen, so aber *Engeler,* ZD 2018, S. 55, 57; *Wagner,* ZD-Aktuell 2018, 06103.

1213 Dafür *Buchner/Petri,* in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 40; ähnlich *Golland,* MMR 2018, S. 130, 132 Für das Beschäftigungsverhältnis, aber noch zu § 32 Abs. 1 S. 1 BDSG 2003 *Erfurth,* NJOZ 2009, S. 2914, 2918 f.

prüfung an. Dies soll verhindern, dass das Erforderlichkeitsprinzip mit einer stark spezifizierten Zwecksetzung umgangen wird.[1214]

994 Dieser Ansatz scheitert spätestens dort, wo er auf sehr komplexe Vertragsbeziehungen stößt. Aber selbst bei weniger komplexen, dafür aber neuartigen Dienstleistungen dürfte es regelmäßig einige Zeit dauern, bis nach der Verkehrsauffassung feststeht, was zu deren charakteristischen Leistungen zählt und was nicht.[1215] Das Datenschutzrecht droht hier in eine allgemeine Vertragskontrolle auszuufern, was zum einen wegen der Kompetenzverteilung zwischen der Union und der Mitgliedstaaten äußerst problematisch wäre, zum anderen aber auch übermäßig in die Privatautonomie der Beteiligten[1216] eingriffe.

995 Die vorzugswürdige Gegenauffassung will die Konkretisierung des Zwecks den Vertragsparteien überlassen.[1217] Dazu sind die konkreten vertraglichen Pflichten unter Zuhilfenahme sämtlicher Auslegungsmethoden zu ermitteln. Danach wäre der Vertrag erst dann nach objektiven Maßstäben zu interpretieren, wenn ein anderweitiger Parteiwille nicht ermittelt werden könnte.

996 Dieses an der gängigen Vertragsauslegung orientierte Vorgehen hat den Vorteil, dass es die dahinterstehenden Wertungen offenbart. Ebenso wie im Rahmen der späteren Angemessenheitsprüfung gilt nämlich im Rahmen des Vertragsrechts – und damit auch im darauf aufsetzenden Datenschutzrecht – kein objektiver, sondern ein übereinstimmend subjektiver Ansatz (siehe 3.4.1.3.4.2.1, S. 381). Die Parteien können grundsätzlich vereinbaren, was sie wollen und diesen Vertrag auch mit einer beliebigen Bezeichnung versehen. Da sie im Vertragsrecht nicht an einen typischen Vertragsinhalt gebunden sind, kann dieses Instrument auch nicht ohne Weiteres in die datenschutzrechtliche Beurteilung eingeführt werden.

1214 *Buchner/Petri,* in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 26, in Bezug auf diese Gefahr auch *Wendehorst/Graf von Westphalen,* NJW 2016, S. 3745, 3746 f.

1215 *Engeler,* ZD 2018, S. 55, 57; *Wagner,* ZD-Aktuell 2018, 06103.

1216 *Gola,* in: Gola 2018, Art. 6 DS-GVO, Rn. 37.

1217 *Engeler,* ZD 2018, S. 55, 57 f.; *Gola,* in: Gola 2018, Art. 6 DS-GVO, Rn. 37; *Schantz,* in: Simitis et al. 2019, Art. 6 Abs. 1 DS-GVO, Rn. 25; *Wagner,* ZD-Aktuell 2018, 06103; wohl auch *Assion et al.,* in: Gierschmann et al. 2018, Art. 6 DS-GVO, Rn. 90 Zur Konkretisierung der Zwecke im Beschäftigungsverhältnis.

3.4.1.4.4.1 Die AGB-Kontrolle als Umgehungsschutz

Zum Offenlegen der Wertungen gehört auch, dass sich die Grenzen der Zweckkonkretisierung bei der Verarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO in erster Linie aus dem Vertragsrecht ergeben. Insbesondere wenn das Machtverhältnis zwischen den Vertragsparteien zu ungleichgewichtig ist, als dass man dadurch auf ausgewogene Vertragsinhalte schließen könnte, kommen die Kontrollinstrumente der §§ 138, 242 BGB und der AGB-Kontrolle zur Anwendung. 997

Gerade das AGB-Recht findet hier die deutlich passenderen Ansätze.[1218] Statt für alle Verträge einen typischen Vertragsinhalt vorzugeben, wirken die Beschränkungen gemäß § 305 Abs. 1 BGB nur für vorformulierte Vertragsbedingungen. Die Parteien müssen also nicht den Weg über eine Einwilligung beschreiten. Dieser Weg wäre vor dem Hintergrund des Kopplungsverbots nach Art. 7 Abs. 4 DS-GVO, demzufolge die Wirksamkeit einer Einwilligung kritisch zu hinterfragen ist, wenn die Erfüllung des Vertrags von dieser Einwilligung abhängig gemacht wird, ohnehin zweifelhaft. Liegen aber AGB vor, greift die Einbeziehungskontrolle, die in Bezug auf die Transparenz mit § 305 Abs. 2 und § 305c BGB ähnliche Anforderungen wie Art. 7 Abs. 2 DS-GVO zur Einwilligung stellen. 998

Auf der Ebene, auf der die eingangs erwähnte objektive Vertragsauslegung ansetzt (siehe 3.4.1.4.4, S. 395), steht im AGB-Recht die allgemeine Inhaltskontrolle nach § 307 BGB. Die Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO sowie der Erlaubnistatbestand selbst in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO könnte hier als gesetzliche Regelung nach § 307 Abs. 2 Nr. 1 BGB begriffen werden, mit deren Grundgedanken – dem Erforderlichkeitsprinzip – die vertragliche Bestimmung vereinbar sein muss. Damit wäre letztlich über den Umweg des AGB-Rechts und mit der Einschränkung der Individualabreden nach § 305b BGB das gleiche Ergebnis wie nach einer objektiven Vertragsauslegung erreicht.[1219] 999

Gegen den Ansatz über die AGB-Kontrolle kann nicht eingewendet werden, er führe dazu, dass nationales Recht dem europäischen Recht Vorgaben mache, obwohl letzteres doch Anwendungsvorrang genieße. Es ist nämlich zum einen so, dass für die Bestimmung der vertraglichen Pflich- 1000

1218 Für ein Vorgehen über die AGB-Kontrolle auch *Hoffmann et al.*, MMR 2014, S. 89, 92 f. und wohl auch *Schantz*, in: Simitis et al. 2019, Art. 6 Abs. 1 DS-GVO, Rn. 27 f. Zu § 13 Abs. 6 TMG bereits *Schnabel/Freund*, CR 2010, S. 718, 720.

1219 So i.E. auch *Hornung*, DuD 2015, S. 359, 364 f.

ten, die den Verarbeitungszweck nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO bilden, prinzipiell mitgliedstaatliches Recht zur Anwendung kommt (siehe 3.2.2.5.2, S. 281). Zum anderen ist zu beachten, dass die Transparenz- und Inhaltskontrolle selbst europäische Vorgaben in Art. 4 und 5 der Klausel-RL 93/13/EWG umsetzen. Der Ansatz über die AGB-Kontrolle kann folglich in allen Mitgliedstaaten verfolgt werden.

1001 Ein Vorgehen über die Inhaltskontrolle nach § 307 BGB setzt allerdings voraus, dass das Erforderlichkeitsprinzip bestimmte Anforderungen an die Zwecksetzung enthält, die mit einer sehr spezifischen Vertragsgestaltung umgangen würden. Dies wäre gemäß § 307 Abs. 3 S. 1 BGB auch die Voraussetzung dafür, dass die Klauselverbote der §§ 308 f. BGB Anwendung finden. Angesichts dessen, dass das Erforderlichkeitsprinzip gerade an der Zwecksetzung ansetzt, ist hier Vorsicht geboten. Die einzige sichere Anforderung besteht hier darin, diesen Prüfungspunkt nicht leerlaufen zu lassen (siehe 3.4.1.4.2.3, S. 394). Darüberhinausgehende Anforderungen ließen sich dagegen nur schwer mit dieser Grundannahme vereinbaren. Insbesondere die Vereinbarungen zur Funktionalität eines Dienstes bleiben damit von der Inhaltskontrolle nach § 307 BGB unberührt.[1220]

3.4.1.4.4.2 Der Konkretisierungsspielraum des Verantwortlichen

1002 Die rechtfertigende Wirkung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO basiert auf den Gedanken der Privatautonomie. Beide Parteien begegnen sich beim Vertragsschluss grundsätzlich auf Augenhöhe, ohne dass sich einer dem Bestimmungsrecht eines anderen unterwirft. Ein Konkretisierungsspielraum für den Verantwortlichen kann darum auch in dieser Konstellation nicht ohne Weiteres angenommen werden. Die Konkretisierung des Zwecks erfolgt hier ausschließlich so weit, wie beide Parteien Einfluss auf die Gestalt der Einwilligung bzw. den Vertragsgegenstand genommen haben.

1220 *Wendehorst/Graf von Westphalen*, NJW 2016, S. 3745, 3748 f. wollen diese Ausnahme auf den „Kern der Leistungsbeschreibung" reduzieren. Die umgekehrte Situation, wenn nicht die Funktionalität des Dienstes, sondern die (im Zuge der Erforderlichkeitsprüfung erst zu ermittelnde) Verarbeitung personenbezogener Daten als Hauptleistung deklariert wird, soll dagegen auf jeden Fall der Inhaltskontrolle nach §§ 307 ff. BGB unterliegen. Die Funktionalität darf demnach nicht allein in der Verarbeitung personenbezogener Daten bestehen.

Nach diesem Ansatz ist der Konkretisierungsspielraum im Vertragsrecht zu suchen.[1221] Wenn und soweit eine Partei befugt ist, die vertraglichen Pflichten einseitig näher zu bestimmen, ist ihr auch auf der Ebene des Datenschutzrechts ein Spielraum bei der Konkretisierung des Zwecks zuzubilligen. Ein solches Leistungsbestimmungsrecht kann sich – konkludent oder ausdrücklich – aus einer vertraglichen Vereinbarung, in Spezialfällen aber auch aus dem Gesetz ergeben.[1222] Für das im Rahmen dieser Darstellung allein relevante Weisungsrecht des Arbeitgebers trifft sogar beides zu. Es ist zum einen in § 106 S. 1 GewO gesetzlich verankert, zum anderen als Wesensmerkmal des Arbeitsverhältnisses aber auch Teil jedes Arbeitsvertrags (siehe 2.4, S. 189). 1003

Seine äußeren Grenzen findet das Leistungsbestimmungsrecht – und damit die Zwecksetzungsbefugnis – im Vertragsrecht. Unter der Maßgabe des § 310 Abs. 4 S. 2 und 3 BGB unterliegt der vertragliche Rahmen des Weisungsrechts dabei auch der AGB-Kontrolle. Innerhalb dieser Grenzen unterliegt das Weisungsrecht der Ausübungskontrolle nach § 315 BGB und § 106 GewO (siehe 2.4.2, S. 190). 1004

Im Zusammenwirken dieser Kontrollinstrumente ist zumindest die spezifisch datenschutzrechtliche Grenze der Zweckkonkretisierung sicherzustellen, nach der die Erforderlichkeitsprüfung nicht entleert werden darf (siehe 3.4.1.4.2.3, S. 394). Der Zweck kann also insbesondere nicht auf die Verwendung eines bestimmten, im Detail vorgegebenen Datenverarbeitungssystems vorgegeben werden. Auf das Ineinandergreifen dieser Kontrollinstrumente wird vor dem Hintergrund der Spezifika des Beschäftigungsverhältnisses unter Gliederungspunkt 3.6.1.2.1.2 (S. 493) näher eingegangen. 1005

3.4.1.4.5 Erforderlichkeitsprüfung

Wie oben (siehe 3.4.1.4.2, S. 392) bereits angedeutet, bestehen durchaus unterschiedliche Vorstellungen über den Maßstab der Erforderlichkeit. So 1006

1221 So auch *Thüsing/Traut,* in: Thüsing 2014, § 14, Rn. 43, die allerdings noch das Verhältnis nach der alten Rechtslage, also zwischen § 106 S. 1 GewO und § 32 Abs. 1 S. 1 BDSG 2003 behandeln.

1222 BeckOK BGB/*Gehrlein*, § 315 BGB, Rn. 3. Ein Beispiel für ein ausschließlich gesetzlich verankertes Leistungsbestimmungsrecht betrifft die Vergütung von Arbeitnehmererfindungen, die unter gewissen Umständen vom Arbeitgeber festgelegt werden kann, § 12 Abs. 3 S. 1 ArbNErfG.

will z.B. eine Meinung die Erforderlichkeit nicht so verstanden wissen, dass die Datenverarbeitung absolut unverzichtbar für die Erreichung des Zwecks sein müsse.[1223] Dies biete die notwendige Flexibilität, um die Vorstellung der Beteiligten und ggf. auch einen Spielraum des Verantwortlichen zu berücksichtigen.[1224] Hierfür ergeben sich verschiedene Ansatzpunkte, die im Folgenden diskutiert werden sollen.

3.4.1.4.5.1 Eingriffsintensität

1007 Jede Erforderlichkeitsprüfung basiert darauf, dass zunächst die Eingriffsintensität der in Frage kommenden Maßnahmen bewertet wird. So wird beurteilt, welches Mittel milder und darum bei gleicher Eignung vorzuziehen ist. Die Eingriffsintensität bestimmt sich danach, wie stark das Mittel die Grundrechte und Grundfreiheiten des Betroffenen gefährdet (siehe 3.4.1.3.3.1, S. 376). Dies ist eine reine Rechtsfrage, bei deren Beurteilung kein Spielraum in Betracht kommt.

3.4.1.4.5.2 Eignung des Mittels

1008 Die Eignung des Mittels bestimmt sich nach dessen Wirksamkeit – ob und mit welcher Qualität der Zweck erreicht werden kann – und der Wirtschaftlichkeit – welcher Aufwand damit für den Verantwortlichen verbunden ist. Zumindest im ersten Teil, der Wirksamkeit eines Mittels zur Zweckerreichung, könnten ohne Weiteres die Vorstellungen der Beteiligten und ggf. ein Spielraum des Verantwortlichen berücksichtigt werden.[1225] Dies wäre z.B. dann relevant, wenn die Beteiligten eine bestimmte Vorstellung über die Gestaltung eines Dienstes haben oder der Verantwortliche ein bestimmtes unternehmerisches Konzept verfolgt und die

---

1223 BAG v. 22.10.1986 – 5 AZR 660/85, E 53, S. 226, Rn. 33 (=NZA 1987, S. 415); BeckOK DSR/*Albers/Veit*, Art. 6 DS-GVO, Rn. 32; *Buchner/Petri*, in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 45; *Frenzel*, in: Paal/Pauly 2018, Art. 6 DS-GVO, Rn. 14.

1224 Zu § 32 Abs. 1 S. 1 BDSG 2003 *Deutsch/Diller*, DB 2009, S. 1462, 1463; *Gola/Jaspers*, RDV 2009, S. 212, 213; *Thüsing*, NZA 2009, S. 865, 866 f. *Zöll*, in: Taeger/Gabel 2019, § 26 BDSG, Rn. 25 plädiert darum für einen subjektiven Prüfungsmaßstab bei der Erforderlichkeitsprüfung.

1225 *Erfurth*, NJOZ 2009, S. 2914, 2918 f.

Frage aufgeworfen wird, ob dies zur Durchführung des jeweiligen Vertrags erforderlich ist.

Für die Frage der Erforderlichkeit ist entscheidend, ob mit dem Einsatz des Mittels ein relevanter Mehrwert erzeugt wird, ob ein weniger einschneidendes Mittel, das diesen Mehrwert nicht bietet, also gleich geeignet ist. Bei der Beurteilung der Wirksamkeit eines Mittels könnte man stärker auf die gemeinsamen subjektiven Vorstellungen der Beteiligten bzw. bei Bestehen eines Spielraums einseitig auf die subjektiven Vorstellungen des Verantwortlichen abstellen und weniger auf die objektive Eignung, zumal letztere im Regelfall angesichts der Komplexität von Assistenzsystemen und der Beurteilung der durch ihren Einsatz erzielten Effekte (siehe 3.4.1.4.1.2, S. 390) ohnehin nur schwer zu ermitteln ist. 1009

Der Vergleich mit der Zwecksetzung zeigt hier eine gewisse Austauschbarkeit der Ansätze.[1226] Die Vorstellungen der Beteiligten oder das Konzept des Verantwortlichen ließe sich ebenso dergestalt berücksichtigen, dass der Zweck anhand dieser Kriterien auf bestimmte Funktionalitäten konkretisiert wird. Lehnt man die Verortung in der Zwecksetzung aber ab, so wäre es immerhin konsequent, die Konkretisierung in der Wirksamkeit des Mittels zu prüfen. 1010

Auf der Ebene der Wirtschaftlichkeit scheint es dagegen nicht notwendig, weitere Konkretisierungen zuzulassen. Der Maßstab der gleichen Eignung ist hier bereits derart streng, dass sich kein Ansatzpunkt bietet, über den dieses Kriterium flexibilisiert werden könnte. Wenn grundsätzlich jeder Mehraufwand die gleiche Eignung eines Mittels entfallen lässt, kann die Vergleichsgruppe von vornherein so gestaltet werden, dass die wirtschaftlichen Interessen des Verantwortlichen gewahrt bleiben.[1227] Eine Flexibilisierung würde hier darauf hinauslaufen, den Verantwortlichen von der Last zu befreien, den Aufwand, der in seine Erforderlichkeitsprüfung einfließt, im Einzelnen darzulegen. 1011

3.4.1.4.6 Stärkung der Zweckbindung

Insgesamt kann festgehalten werden, dass die Konkretisierung der genauen datenschutzrechtlichen Anforderungen konstruktiv sowohl im Rahmen der Zwecksetzung als auch im Rahmen der gleichen Eignung berücksich- 1012

1226 So auch *Schmitz* 2016, S. 197 f.
1227 So ähnlich auch *Schmitz* 2016, S. 198 f.

tigt werden kann. Der entscheidende Nachteil einer Lösung in der Erforderlichkeitsprüfung besteht allerdings darin, dass der Zweck dann notwendigerweise abstrakter ausfallen muss. Genau dies läuft aber dem Gebot der Zweckbindung nach Art. 5 Abs. 1 lit. b DS-GVO zuwider. Denn je abstrakter der Zweck gefasst ist, desto unterschiedlichere Ziele (im Sinne von Teilzwecken) kann der Verantwortliche mit der Datenverarbeitung verfolgen, ohne sie als zweckändernde Weiterverarbeitung behandeln zu müssen (siehe 3.4.1.2.4.1, S. 368).

1013 Gegen die Verletzung der Zweckbindung ließe sich zwar argumentieren, dass die Vereinbarkeitsprüfung nach Art. 5 Abs. 1 lit. b DS-GVO, die hierdurch entfiele, letztlich auch nur eine Form der Angemessenheitsprüfung ist (siehe 3.4.1.2.3.3, S. 362), die im Falle eines nur abstrakten Zwecks bereits zu Anfang, also vorweggenommen zu prüfen ist. Je unkonkreter der Zweck aber definiert wird, je mehr potenzielle Verarbeitungskonstellationen also abgedeckt sind, desto vielfältiger werden auch die Anforderungen, denen sich ein Verantwortlicher im Rahmen der Angemessenheitsprüfung stellen muss (siehe 3.4.1.2.4.3, S. 370).

1014 Dies änderte aber nichts daran, dass die nach Art. 13 Abs. 3 DS-GVO notwendige Information der betroffenen Person unterbliebe. Diese Information ist bei einer Zweckänderung zwingend zu erteilen. Auf eine Änderung des Teilzwecks ist die Norm nicht anwendbar. Dem Betroffenen ginge bei einer weiten Zweckfestlegung im Vergleich zu einer engen Zweckfestlegung also ein Kontrollinstrument verloren.

1015 Unter dem Eindruck der Zweckbindung spricht darum viel dafür, die Zwecksetzung als das eigentlich variable Element zu begreifen, in das die Vorstellungen der Parteien einfließen und in dem auch – wenn und soweit dieser besteht – ein Spielraum des Verantwortlichen zu verorten wäre.[1228] Dies erscheint zunächst paradox, schließlich steht und fällt eine enge Zweckbindung mit der möglichst weitgehenden Konkretisierung des Zwecks. Variabilität zu gewähren, bedeutet in diesem Fall aber auch, dass der- oder diejenigen, die den Zweck festlegen, diese Variabilität auch nut-

1228 Mit diesem Argument wurde auch die Anwendung des § 28 Abs. 1 S. 2 BDSG 2003 im Rahmen der Datenverarbeitung zu Beschäftigungszwecken nach § 32 Abs. 1 S. 1 BDSG 2003 (jetzt § 26 Abs. 1 S. 1 BDSG 2018) bejaht. Gemäß § 28 Abs. 1 S. 2 BDSG 2003 hatte der Verantwortliche die Zwecke, für die die Daten verarbeitet oder genutzt werden sollten, bei der Verarbeitung konkret festzulegen. Dafür *Däubler*, in: Däubler et al. 2016, § 32 BDSG, Rn. 9; *Schmitz* 2016, S. 187. Gegen die Anwendung *Erfurth*, NJOZ 2009, S. 2914, 2923.

zen müssen, um den Zweck zu konkretisieren. Dies stärkt die Zweckbindung, betont das Merkmal der Vereinbarkeit und verhindert, dass die Betroffenenrechte nach Art. 13 Abs. 3 DS-GVO durch eine allzu weite Zwecksetzung ausgehebelt werden.

3.4.1.4.7 Zwischenfazit: Konsequenzen für die Konkretisierung der Anforderungen

Im für diese Untersuchung relevanten Bereich der Datenverarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO wird der Zweck auf Basis einer durch die Parteien einvernehmlich geschaffenen Grundlage festgelegt. Etwaige Machtungleichgewichte müssen hier durch die AGB-Kontrolle ausgeglichen werden (siehe 3.4.1.4.4.1, S. 397). Der Zweck ist dabei nicht die Erfüllung des Vertrags als Ganzes und insbesondere nicht das abstrakte Leitbild eines typischen Vertrags, sondern die Erfüllung der einzelnen vertraglichen Pflichten. Sie sind unter Auslegung des Parteiwillens möglichst weit zu konkretisieren. Soweit dem Verantwortlichen ein Leistungsbestimmungsrecht, etwa nach § 106 GewO oder § 315 BGB zusteht, kann er den Zweck in den Grenzen dieses Rechts auch einseitig konkretisieren. 1016

Die Herangehensweise hat besonders in komplexen Vertragssituationen wie dem eingangs geschilderten Arbeitsvertrag (siehe 3.4.1.4.1, S. 389) besondere Bedeutung. Hier ist folglich nicht davon auszugehen, dass der Zweck in der Erfüllung des Arbeitsvertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO bzw. der Durchführung des Beschäftigungsverhältnisses nach § 26 Abs. 1 S. 1 BDSG 2018 oder daraus objektiv ableitbarer Vertragspflichten besteht. Der Zweck ist vielmehr anhand der vom Arbeitgeber verfolgten Ziele konkret festzulegen.[1229] Die Reichweite seiner Zwecksetzungsbefugnis ist dabei anhand seines Weisungsrechts nach § 106 GewO zu bestimmen. 1017

An diesem konkreten Zweck setzt eine strenge Erforderlichkeitsprüfung an, die objektiv zu bestimmen ist. Insofern ist auch die verbreitete Formulierung kritisch zu betrachten, wonach die Datenverarbeitung zwar nicht nur nützlich, gleichsam aber auch nicht unverzichtbar sein müsse. Hinsichtlich der Ablehnung der Nützlichkeit ist ihr zuzustimmen; hinsicht- 1018

1229 Zu § 32 Abs. 1 S. 1 BDSG 2003 *Däubler* 2015, Rn. 255; *Schmitz* 2016, S. 197 f.; a.A. *Erfurth,* NJOZ 2009, S. 2914, 2918.

lich der Ablehnung der Unverzichtbarkeit jedoch nur, wenn damit gemeint ist, dass auch die Kosten einer Maßnahme ins Gewicht fallen. Dieser Umstand ist aber bereits ein anerkanntes Merkmal des hergebrachten Begriffs der Erforderlichkeit und bedarf insofern keiner hervorgehobenen Erwähnung.

3.4.1.4.8 Beispiel eines einfachen Lebenssachverhalts

1019 Das Zusammenspiel aus Zweckbindung und Datenminimierung lässt sich abschließend am Beispiel eines einfachen Kaufvertrags des alltäglichen Lebens erläutern. Wie sich zeigen wird, besteht hier u.U. ein geringer Entscheidungsspielraum, der aber letztlich von der konkreten Vertragsauslegung abhängt.

1020 Die einschlägige Rechtsgrundlage für die Datenverarbeitung bildet in diesem Fall Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO. Danach muss die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich sein. Ein Kaufvertrag begründet gemäß § 433 Abs. 1 S. 1 BGB die Pflicht des Verkäufers, dem Käufer die Sache zu übergeben und das Eigentum an der Sache zu verschaffen sowie gemäß § 433 Abs. 2 BGB die Pflicht des Käufers, dem Verkäufer dem vereinbarten Kaufpreis zu zahlen und – in diesem Beispiel nicht relevant – die gekaufte Sache abzunehmen.

3.4.1.4.8.1 Zahlungspflicht des Käufers

1021 An dieser Stelle könnte der Frage nachgegangen werden, welche Datenverarbeitung erforderlich ist, um die Zahlung des Käufers abzuwickeln. Das mildeste, weil die Erhebung von Zahlungsdaten völlig vermeidende, Mittel bestünde hier darin, die Zahlung mit Bargeld zu ermöglichen. Alternativ könnten auch Gutscheinkarten akzeptiert werden, die durch eine Barzahlung aufgeladen werden können. Dabei wäre aber gleichzeitig der Aufwand zu berücksichtigen, der mit einer solchen datenvermeidenden Zahlungsmethode einhergeht. Zumindest im stationären Handel wäre der Mehraufwand aber wohl so gering, dass er die datenschutzrechtliche Pflicht, die datenschutzfreundliche Barzahlung zuzulassen, nicht aufheben könnte. Denkbar wäre dies allenfalls im Online-Handel, weil sich dort zumindest bei der Bargeldannahme praktische Probleme stellen.

Eine solche Vorgehensweise wäre aber verfehlt. Statt zu fragen, welches die datenschutzrechtlich erforderliche Zahlungsmethode ist, muss der Kaufvertrag weiter ausgelegt werden. Ohne eine – u.U. auch konkludent getroffene – abweichende Regelung sind Geldschulden „in bar, d.h. durch Übereignung einer entsprechenden Anzahl von gesetzlichen Zahlungsmitteln zu erfüllen."[1230] Der Zweck wurde also weiter konkretisiert, von der „Abwicklung der Zahlung" zu der „Abwicklung der Zahlung *in bar*". Welcher Aufwand hiermit verbunden ist und, ob der Verkäufer unter Verweis hierauf eine Zahlungsmethode wählen und bspw. die Kreditkartendaten der betroffenen Person verarbeiten dürfte, spielt keine Rolle mehr. Der Zweck wurde bereits auf diese Zahlungsmittel konkretisiert. 1022

Entsprechend verhält es sich, wenn die Parteien eine andere Zahlungsmethode vereinbart haben. Hierzu gibt der Verkäufer in der Regel die Zahlungsmethoden an, die er akzeptieren will. Wählt der Käufer eine von ihnen, ist seine Zahlungspflicht nach § 433 Abs. 2 BGB entsprechend auf diese Methode konkretisiert. Wird die Zahlung in Buchgeld vereinbart, etwa per Kreditkarte lautet der Zweck also „Abwicklung der Zahlung *per Kreditkarte*". Ob es eine mildere, weil datensparsamere Zahlungsmethode gegeben hätte, spielt dann ebenfalls keine Rolle mehr. Der Zweck wurde – wenn auch wenig datenschutzfreundlich – konkretisiert. Die Kreditkartendaten dürften folglich unproblematisch erhoben werden. 1023

3.4.1.4.8.2 Eigentumsverschaffungspflicht des Verkäufers

Auch was die Pflicht des Verkäufers angeht, dem Käufer das Eigentum an der Ware zu verschaffen, könnte nun thematisiert werden, welche Datenerhebung hierfür erforderlich wäre. Auch hier wäre diese Frage allerdings teilweise verfehlt. 1024

3.4.1.4.8.2.1 Zulässigkeit der Datenübermittlung an einen Frachtführer

Theoretisch könnte der Verkäufer im Online-Handel die Ware dem Käufer auch selbst bringen – verbunden allerdings mit einem hohen Aufwand. Erneut könnte der Frage nachgegangen werden, ob es erforderlich ist, die 1025

1230 BGH v. 25.3.1983 – V ZR 168/81, Z 87, S. 156, Rn. 21 (=NJW 1983, S. 1605); MüKo BGB/*Fetzer*, § 362 BGB, Rn. 19; BeckOGK/*Looschelders*, § 362 BGB, Rn. 136.

Adressdaten zu erheben *und* an einen Frachtführer zu übermitteln oder, ob es nicht vielmehr genügt, die Daten nur intern zu verarbeiten und die Ware selbst zu bringen. Die Antwort stünde hier fest, schließlich wäre das Bringen so aufwändig, dass es kaum als gleich geeignet gelten könnte.

1026 Wie bei der Zahlungspflicht sollte aber zunächst geprüft werden, inwiefern sich die Pflicht des Verkäufers bereits konkretisiert hat. So wird im Online-Handel in der Regel ein Versendungskauf nach § 447 BGB vorliegen. Der Inhalt der Eigentumsverschaffungspflicht ist also u.a. bereits auf die Zuhilfenahme eines Dritten konkretisiert. Die Frage, ob die Übermittlung der Daten das mildeste Mittel ist, ist darum fehl am Platz; sie ist das einzige, das zur Zweckerreichung geeignet ist.

3.4.1.4.8.2.2 Wahl des Empfängers der Datenübermittlung

1027 Was die Wahl des konkreten Frachtführers angeht, so hängt diese wiederum von der Vertragsauslegung ab. Gibt der Versandhändler im Vorfeld an, mit welchen Frachtführern er versendet oder lässt er den Käufer unter mehreren wählen, so ist seine Pflicht, dem Käufer das Eigentum zu verschaffen, hierauf konkretisiert. Entsprechend vordefiniert wäre hier wieder die Erforderlichkeitsprüfung. Wollte er den Frachtführer wechseln, wäre das – neben der Frage der vertraglichen Zulässigkeit – eine Frage der Zweckbindung. Solange der andere Frachtführer aber hinsichtlich der Wahrung des Postgeheimnisses ebenso zuverlässig ist wie der bisherige, bestehen gegen die Vereinbarkeit mit dem Erhebungszweck nach Art. 5 Abs. 1 lit. b DS-GVO keine Bedenken. Allein die Informationspflichten nach Art. 13 Abs. 3 DS-GVO wären einzuhalten.

1028 Wurde kein bestimmter Frachtführer vereinbart, hat sich die Eigentumsverschaffungspflicht des Verkäufers auch nicht konkretisiert. Auf vertraglicher Ebene darf er den Frachtführer dann grundsätzlich frei auswählen.[1231] Erst an dieser Stelle setzt die datenschutzrechtliche Erforderlichkeitsprüfung an. In diese Prüfung sind auch besonders datenschutzfreundliche Methoden einzubeziehen. So wurde in den Anfangszeiten des Online-Handels ein System mit Treuhändern entwickelt, das verhindert, dass der Verkäufer die Adresse des Käufers erfährt und der Frachtführer erfährt, von welchem Händler das Paket stammt. Ein Online-Einkauf wäre damit beinahe so an-

1231 Vgl. zum Dienstvertrag *Tillmanns* 2007, S. 130.

onym abgelaufen wie ein Geschäft des täglichen Lebens im stationären Handel.[1232]

3.4.1.4.8.2.2.1 Erheblicher Mehraufwand für datensparsame Lösung

Geht man davon aus, dass mit diesem System ein erheblicher Mehraufwand verbunden ist, scheidet es im Vergleich zum herkömmlichen Frachtsystem bereits beim Merkmal der gleichen Eignung aus. In der abschließenden Angemessenheitsprüfung ist das Risiko für die Grundrechte der betroffenen Person mit den Vorteilen des Verantwortlichen abzuwägen. Dabei sind u.a. die Zuverlässigkeit des gewählten Frachtführers in datenschutzrechtlichen Fragen und der Mehraufwand einer datenschutzfreundlicheren Lösung zu berücksichtigen. Der Bewertungsmaßstab ergibt sich im Zweifel aus der Verkehrssitte, die wohl darauf lautet, die Adressdaten selbst zu erheben und sie zusammen mit den Absenderdaten an anerkannte Frachtführer zu übermitteln. Der Maßstab wäre hier nur ein anderer, wenn eine abweichende Vereinbarung zwischen den Parteien bestünde oder sich aus den Umständen des Vertrags ein besonderes Risiko für die betroffene Person ergäbe. 1029

Der Einsatz von Datentreuhändern liegt deutlich über dem, was nach der Verkehrssitte als risikoadäquate Maßnahme gefordert werden kann. Das Prinzip der Datenminimierung begründet im Grundsatz kein Verbesserungsverbot in der Gestalt, dass der Verantwortliche verpflichtet wäre, über die Masse der anderen Marktteilnehmer, die das weithin Übliche und allgemein Akzeptierte praktizieren, hinauszuragen. Da hier kein erhöhtes Risiko für die Grundrechte des Käufers zu erkennen ist, bleibt es auch bei diesem Grundsatz (zur Ausnahme bei hohem Risiko siehe 3.4.2.2.5.4, S. 450). 1030

Der Versandhändler kann sich bei seiner Auswahl also auf übliche und marktgängige Methoden des Versendens beschränken. Soweit sich keine wesentlichen Unterschiede in Bezug auf die Einhaltung datenschutzrechtlicher Regelungen durch die Frachtführer zeigen, ist der Verkäufer darum frei, diese nach eigenem Belieben zu wählen. Die Grenze wäre hier die Unzuverlässigkeit im Hinblick auf die Wahrung des Postgeheimnisses. Insofern gilt nichts Anderes als bei der Vereinbarkeitsprüfung; nur die Infor- 1031

1232 *Roßnagel/Scholz*, MMR 2000, S. 721, 725; zu dem damaligen Projekt allgemein *Grimm et al.*, DuD 1999, S. 272–276.

mationspflicht nach Art. 13 Abs. 3 DS-GVO entfällt, wenn der Zweck nicht konkretisiert wurde.

3.4.1.4.8.2.2.2 Vergleichbarer Aufwand für datensparsame Lösung

1032 Diese Beschränkung auf marktübliche Methoden gilt jedoch nur, solange mit dem Einsatz datensparsame Alternativen tatsächlich ein relevanter Mehraufwand verbunden ist. In dem Maße, wie die Systemkosten innovativer Lösungen sinken, steigt auch die Verpflichtung der Verantwortlichen, sie einzusetzen. Dies folgt den allgemeinen Regeln:

1033 Liegen die Wirksamkeit und die Kosten einer datensparsamen, aber unüblichen Lösung auf dem Niveau einer etablierten Methode, so sind beide als gleich geeignet einzustufen. Die übliche, aber eingriffsintensivere Maßnahme ist dann nicht mehr als das mildeste Mittel einzustufen und folglich unzulässig. Der Verantwortliche muss in jedem Fall die neue Lösung wählen. Die Verkehrssitte spielt im Rahmen der Erforderlichkeitsprüfung i.e.S. keine Rolle.

1034 Nähern sich die Kosten einer datensparsamen Lösung denen der gängigen Methoden an, wirkt sich dies immerhin auf die Angemessenheitsprüfung aus. Dem gesunkenen Mehraufwand seitens des Verantwortlichen steht das unverminderte Risiko für die betroffene Person gegenüber. Gerade in Fällen, in denen das Risiko als hoch einzustufen ist, kann dies die Abwägung zuungunsten des Verantwortlichen beeinflussen. Ihm ist dann eher zuzumuten, den Mehraufwand zu stemmen. Unbeirrt an etablierten Methoden festzuhalten, könnte die Datenverarbeitung hier unzulässig machen.

3.4.1.5 Transparenz

1035 Das Transparenzgebot wurde in der Datenschutzrichtlinie, in der es in Art. 6 Abs. 1 lit. a DSRL nicht enthalten war, der Formel Treu und Glauben entnommen.[1233] Entsprechend werden der bisher unter Treu und Glauben subsumierte Ausschluss der heimlichen Verarbeitung und die Informationspflichten nun diesem ausgegliederten Grundsatz nach Art. 5

1233 EuGH, ECLI:EU:C:2015:638, Rn. 34 – *Bara*.

Abs. 1 lit. a DS-GVO zugeordnet.[1234] Dabei legt die in der deutschen Sprachfassung gewählte Umschreibung des Begriffs Transparenz als Datenverarbeitung in einer für die betroffene Person nachvollziehbaren Weise nahe, dass sie sich nur auf bereits abgeschlossene Datenverarbeitung bezieht. Sowohl ErwG 39 S. 2 DS-GVO als auch der Vergleich mit anderen Sprachfassungen, die den Begriff nicht umschreiben, stellen aber klar, dass es auch um die vorherige Information geht.[1235]

3.4.1.5.1 Allgemeine Anforderungen

Die Transparenz der Datenverarbeitung ist eine Vorbedingung der informationellen Selbstbestimmung des Einzelnen, weil nur so gesichert ist, dass die betroffene Person eine Datenverarbeitung – sei es durch ihre Einwilligung oder einen Vertragsschluss – wirksam legitimieren und allgemein ihre Rechte ausüben kann.[1236] Der Grundsatz steht darum in enger Verbindung mit den Betroffenenrechten der Art. 12 ff. DS-GVO und wird durch die Informationspflichten des Verantwortlichen nach Art. 13 und 14 DS-GVO und die Auskunftsrechte der betroffenen Person nach Art. 15 DS-GVO spezifiziert.[1237] 1036

Es ist allerdings unklar, ob dem allgemeinen Transparenzgebot auch Informationspflichten und Auskunftsechte entnommen werden können, die über die Kataloge der Art. 13 ff. DS-GVO hinausgehen. *Schantz*[1238], der dies befürwortet, verweist hierzu auf ErwG 39 S. 4 DS-GVO, demzufolge der Grundsatz der Transparenz neben der Identität des Verantwortlichen und den Zwecken der Verarbeitung auch sonstige Informationen betrifft, die eine faire und transparente Verarbeitung gewährleisten. Damit dürfte aber lediglich die zusätzliche Informationspflicht nach Art. 13 Abs. 2 DS-GVO gemeint sein, die unter der nahezu wortgleichen Voraussetzung steht. 1037

1234 *Herbst*, in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 18.
1235 *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 21; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 11.
1236 *Herbst*, in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 18; *Pötters*, in: Gola 2018, Art. 5 DS-GVO, Rn. 11.
1237 *Herbst*, in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 19; *Kramer*, in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 19.
1238 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 11.

3.4.1.5.2 Direkterhebungsgrundsatz

1038 Das Gebot der Transparenz und der Verarbeitung nach Treu und Glauben wird auch herangezogen, um einen – in § 4 Abs. 2 BDSG 2003 noch ausdrücklich geregelten – Direkterhebungsgrundsatz zu statuieren.[1239] Es ist allerdings fraglich, ob man dieses Prinzip derart bruchlos in die Datenschutz-Grundverordnung übertragen kann. In der Datenschutzrichtlinie wurde Treu und Glauben lediglich dahingehend ausgelegt, dass sie einer heimlichen Datenverarbeitung grundsätzlich entgegensteht, aber nur dergestalt, dass die betroffene Person umfassend informiert werden muss.[1240] Wie die sehr ähnliche Ausgestaltung der Informationspflichten nach Art. 13 und 14 DS-GVO zeigt, ist dies sowohl unter Mitwirkung als auch ohne Mitwirkung der betroffenen Person prinzipiell möglich.[1241]

1039 Aus Treu und Glauben allein lässt sich demnach kein Vorrang der Direkterhebung ableiten. Das ändert aber nichts daran, dass die betroffene Person im Falle der Direkterhebung zumindest eine bessere Kontrolle über den Umfang der erhobenen Daten hat. Dies muss zumindest bei der Zweckbindung (siehe 3.4.1.2.3.2, S. 361) und in der Angemessenheitsprüfung berücksichtigt werden.[1242] Einen eigenständigen Prüfungspunkt wie in § 4 Abs. 2 BDSG 2003 bildet es allerdings nicht.

3.4.1.5.3 Verdeckte Datenerhebung

1040 Vom Direkterhebungsgrundsatz ist der Problemkreis der verdeckten Datenerhebung zu unterscheiden. Bei ersterem geht es um die Frage, ob die Daten prinzipiell nur unter Mitwirkung des Betroffenen erhoben werden dürfen und welche Ausnahmen hiervon ggf. zuzulassen sind. Bei der letzterem geht es darum, wann – also zu welchem Zeitpunkt – der Verantwortliche seine Informationspflichten nach Art. 13 f. DS-GVO nachkommen muss. Ob diese Informationspflichten einer – zunächst – verdeckten Datenerhebung entgegenstehen, ist umstritten.

1239 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 9.

1240 EuGH, ECLI:EU:C:2015:638, Rn. 34 – *Bara*; *Herbst,* in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 15 ff.; so wohl auch *Kramer,* in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 18.

1241 *Ziegenhorn/Heckel*, NVwZ 2016, S. 1585, 1588 f.

1242 So auch *Bäcker,* in: Kühling/Buchner 2018, Art. 13 DS-GVO, Rn. 3; *Buchner*, DuD 2016, S. 155, 156; *Däubler*, in: Däubler et al. 2020, Art. 13 DS-GVO, Rn. 2.

3.4.1.5.3.1 Ansätze zu Abgrenzung von Art. 13 und 14 DS-GVO

Gemäß Art. 13 Abs. 1 DS-GVO ist dem Betroffenen zum Zeitpunkt der Erhebung u.a. der Zweck der Verarbeitung mitzuteilen, vorausgesetzt die Daten werden „bei der betroffenen Person erhoben". Werden die Daten dagegen „nicht bei der betroffenen Person erhoben" bestimmen sich die Informationspflichten nach Art. 14 DS-GVO, der keine derart strengen Anforderungen an den Zeitpunkt macht. Die Informationen können entweder im Vorhinein und dann naturgemäß für eine Vielzahl von Fällen erfolgen – gemäß Art. 14 Abs. 5 lit. a DS-GVO entfällt dann die einzelfallbezogene Informationspflicht – oder im Nachhinein, gemäß Art. 14 Abs. 3 lit. a DS-GVO innerhalb einer angemessenen Frist von bis zu einem Monat. 1041

Eine Meinung stellt für die Abgrenzung von Art. 13 und 14 DS-GVO entweder nur auf die Mitwirkung[1243] der Person ab oder lässt zusätzlich auch deren Kenntnis[1244] genügen. Mitwirkung bedeutet, dass die Person aktiv werden, die Erhebung selbst also von ihrer Handlung abhängen muss.[1245] Die Kenntnis wäre aus der Sicht der betroffenen Person zu bestimmen. Beide Male wäre eine verdeckte Datenerhebung nicht „bei der betroffenen Person" und folglich im Anwendungsbereich von Art. 14 DS-GVO. 1042

Dagegen will eine strenge Meinung Art. 13 und Art. 14 DS-GVO danach voneinander abgrenzen, ob die betroffene Person dem Verantwortlichen als unmittelbare Datenquelle dient, er ihr Verhalten also synchron wahrnimmt. Ob dies offen oder verdeckt erfolgt, soll keine Rolle spielen.[1246] Verdeckte Maßnahmen wäre nur unter strengen Voraussetzungen der Beschränkung der Betroffenenrechte nach Art. 23 DS-GVO möglich. 1043

Eine eher vermittelnde Meinung will die Frage aus der Sicht des Verantwortlichen beurteilen und stellt darauf ab, ob die Person für ihn erkennbar körperlich oder mental aktiv oder passiv an der Datenverarbeitung be- 1044

1243 *Ingold*, in: Sydow 2018, Art. 13 DS-GVO, Rn. 8 Ähnlich *Däubler*, in: Däubler et al. 2020, Art. 13 DS-GVO, Rn. 2, demzufolge ein bewusster Kontakt notwendig ist, um Art. 13 DS-GVO anzuwenden.

1244 „Mit Kenntnis oder unter Mitwirkung der betroffenen Person", *Franck*, in: Gola 2018, Art. 13 DS-GVO, Rn. 4.

1245 *Ingold*, in: Sydow 2018, Art. 13 DS-GVO, Rn. 8.

1246 *Bäcker*, in: Kühling/Buchner 2018, Art. 13 DS-GVO, Rn. 13 f.; mit dem wohl gleichen Begriffsverständnis *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 96 ff.

teiligt ist.[1247] Was das aber genau bedeutet, ist unklar. *Schmidt-Wudy*[1248] geht selbst davon aus, dass eine offene Videoüberwachung unter Art. 13 DS-GVO fiele, eine verdeckte unter Art. 14 DS-GVO. Mental passive Beteiligung soll dann wohl heißen, dass die betroffene Person die offene Überwachung erkennen kann und sie darum unter Art. 13 DS-GVO fällt. Begrifflich bereitet es aber auch keine Probleme, eine verdeckt überwachte Person als passiv körperlich beteiligt anzusehen. Immerhin bildet sie das Überwachungsobjekt. Das dürfte allerdings nicht gemeint sein. Schlafende Personen sollen nach *Schmidt-Wudy*[1249] nämlich gar nicht an der Datenerhebung beteiligt sein.

1045 Führt man den Abgrenzungsversuch auf seine Ursprungsthese zurück, wonach „bei" den Ort der Datenerhebung meint, wird die Formel etwas klarer. Da unter den Bedingungen des Internets hier sicherlich nicht der physische Ort gemeint sein kann, lässt sich der Ort der Datenerhebung so verstehen, dass sich die betroffene Person und der Verantwortliche in irgendeiner Form bei der Erhebung begegnen, also nach der Art der Datenerhebung die Möglichkeit der Interaktion besteht. Das ist weniger voraussetzungsvoll als aktive Mitwirkung oder Kenntnis, würde verdeckte Maßnahmen aber immer noch nicht erfassen.

3.4.1.5.3.2 Abgrenzung nach der Datenquelle

1046 Es spricht viel dafür, dem strengen Abgrenzungsansatz zu folgen, der darauf abstellt, ob die betroffene Person als unmittelbare Datenquelle dient. Bei allen anderen Ansätzen bleibt es dem Verantwortlichen durch entsprechende Gestaltung der Datenerhebung überlassen, welche Norm zur Anwendung kommt. Damit kann er bis zu einem gewissen Punkt selbst darüber entscheiden, wann er die betroffene Person von der Datenerhebung informiert.

1047 Die Entscheidung zwischen Art. 13 und 14 DS-GVO, zwischen einer offenen und einer verdeckten Maßnahme wäre zwar nicht gänzlich frei. Der Verantwortliche bliebe immer noch an die Grundsätze des Datenschutzes gebunden, insbesondere an die allgemeinen Transparenzanforderungen in Art. 5 Abs. 1 lit. a DS-GVO. Auch ließe sich die Entscheidung in die Erfor-

1247 *Dix*, in: Simitis et al. 2019, Art. 14 DS-GVO, Rn. 3; BeckOK DSR/*Schmidt-Wudy*, Art. 14 DS-GVO, Rn. 31.
1248 BeckOK DSR/*Schmidt-Wudy*, Art. 14 DS-GVO, Rn. 31.2.
1249 BeckOK DSR/*Schmidt-Wudy*, Art. 14 DS-GVO, Rn. 31.1.

derlichkeitsprüfung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO einbeziehen. Bei beiden Instrumenten wäre der Rechtsanwender aber nur auf allgemeine Verhältnismäßigkeitserwägungen zurückgeworfen. Dagegen hat der Verordnungs- bzw. Gesetzgeber eigens geregelt, unter welchen Voraussetzungen die Informationspflichte nach Art. 13 DS-GVO nicht erfüllt werden müssen. Die Ausnahme in Art. 13 Abs. 4 DS-GVO und die Beschränkungen in Art. 23 DS-GVO i.V.m. § 32 BDSG 2018 sind vorrangig zu prüfen und können nicht durch allgemeine Erwägungen umgangen werden.

3.4.1.5.3.3 Grundsätzlicher Ausschluss der verdeckten Erhebung von Beschäftigtendaten

Dieser strenge Abgrenzungssatz wirft unweigerlich die Frage auf, inwiefern eine verdeckte Datenerhebung im Beschäftigungsverhältnis damit überhaupt noch vereinbar ist. Auch bisher hat der Verhältnismäßigkeitsgrundsatz einem solchen Vorgehen enge Grenzen gesetzt. Sie war aber zugelassen, wenn gegen den Betroffenen ein konkreter Verdacht einer Verfehlung bestand und die Maßnahme das allerletzte Mittel darstellte, den fraglichen Sachverhalt aufzuklären. Eine gefestigte Meinung hatte sich diesbezüglich aber bisher nur für die Aufdeckung von Straftaten gebildet.[1250] Sie ging auch in die Regelung in Art. 32 Abs. 1 S. 2 BDSG 2003 ein,[1251] die in § 26 Abs. 1 S. 2 BDSG 2018 fortgeführt wird.[1252] 1048

Die Informationspflichten nach Art. 13 DS-GVO können gemäß Art. 23 Abs. 1 lit. j DS-GVO i.V.m. § 32 Abs. 1 Nr. 4 BDSG 2018 zwar eingeschränkt werden, wenn sie andernfalls die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen. Dadurch können aber nicht die Pflichten nach Art. 13 Abs. 1 und 2 DS-GVO beschränkt werden, sondern nur diejenigen nach Absatz 3. Art. 13 Abs. 3 DS-GVO bezieht sich nur auf eine zweckändernde Weiterverarbeitung. Außerdem passt die 1049

1250 EGMR v. 5.10.2010 – 420/07, S. 11 – *Köpke/Deutschland*; EGMR v. 9.1.2018 – 1874/13, Rn. 68 – *López Ribalda/Spanien*; BAG v. 27.3.2003 – 2 AZR 51/02, E 105, S. 356, Rn. 28 (=NZA 2003, S. 1193); BAG v. 22.9.2016 – 2 AZR 848/15, E 156, S. 370, Rn. 30 (=NZA 2017, S. 112); BAG v. 20.10.2016 – 2 AZR 395/15, E 157, S. 69, Rn. 22 (=NZA 2017, S. 443).

1251 BT-Drucks. 16/13657, S. 21.

1252 BT-Drucks. 18/11325, S. 97.

Durchsetzung zivilrechtlicher Ansprüche – zumindest bei der Aufdeckung von Straftaten – nicht wirklich auf die Motivlage des Arbeitgebers. Beim Verdacht auf Fehlverhalten des Arbeitnehmers dürfte eher Art. 23 Abs. 1 lit. i DS-GVO einschlägig sein,[1253] der u.a. Ausnahmen zum Schutz der Rechte anderer Personen erlaubt, hier also des Recht des Arbeitgebers, weiteren Schaden zu vermeiden.

1050 Eine unmittelbar passende gesetzliche Beschränkung besteht darum nicht. Auch höchstrichterliche Rechtsprechung allein kann die Anforderungen an eine Beschränkung der Informationspflichten nicht erfüllen. Gemäß Art. 23 Abs. 1 DS-GVO bedarf es einer gesetzgeberischen Maßnahme.[1254]

3.4.1.5.3.4 Ausnahmen für die verdeckte Erhebung von Beschäftigtendaten

1051 Auf den ersten Blick scheint eine verdeckte Datenerhebung bei der betroffenen Person damit ausgeschlossen. Dieses Ergebnis wird aber der gemäß Art. 16 GRC ebenfalls grundrechtlich geschützten unternehmerischen Freiheit des Arbeitgebers nicht gerecht. Es liegt auf der Hand, dass er zumindest irgendeine Methode zur Verfügung haben muss, schwerste Pflichtverletzungen von Arbeitnehmern aufzudecken und zu würdigen.[1255] Auch der – letztlich nicht übernommene – Entwurf des Europäischen Parlaments erkannte dieses Interesse an.[1256] Methoden, die von der Erhebung von Daten absehen und nur auf die Beobachtung durch Menschen setzen (siehe 3.3.1.1, S. 315), sind nicht vergleichbar geeignet. Zudem hat sich der deutsche Gesetzgeber in der Begründung zu § 26 BDSG 2018 vorbehalten, „den expliziten Ausschluss von heimlichen Kontrollen im Beschäftigungsverhältnis“ später zu regeln.[1257] Auch der Gesetzgeber geht also davon aus, dass die verdeckte unmittelbare Datenerhebung noch grundsätzlich möglich ist.

1253 *Bäcker*, in: Kühling/Buchner 2018, Art. 13 DS-GVO, Rn. 92.
1254 Zu beidem *Maschmann*, in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 47.
1255 *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 99; in der Sache auch *Byers*, NZA 2017, S. 1086, 1087, der auf Art. 14 GG abstellt. Nach der hier vertretenen Abgrenzung geht es aber nur für die Gestaltung arbeitsrechtlicher Pflichten um eine Abwägung nach deutschen Grundrechten. Die Abwägung zwischen deren Durchsetzung und dem damit einhergehenden Überwachungsdruck ist eine Frage der europäischen Grundrechte, siehe 3.2.2.5.2, S. 281.
1256 *Maschmann*, in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 4.
1257 BT-Drucks. 18/11325, S. 97.

Um eine verdeckte Datenerhebung unter den bisherigen – ohnehin schon restriktiven – Bedingungen zu ermöglichen, stehen methodisch zwei Wege zur Verfügung. 1052

Man könnte mit *Forst*[1258] eine Analogie zu Art. 14 Abs. 5 lit. b Alt. 3 DS-GVO oder §§ 32 Abs. 1 Nr. 4, 33 Abs. 1 Nr. 2 lit. a BDSG 2018 bilden. Die hierfür notwendige planwidrige Regelungslücke soll sich daraus ergeben, dass der deutsche Gesetzgeber insbesondere den Anwendungsbereich von § 32 Abs. 1 Nr. 4 BDSG 2018 zu eng gefasst habe. Dies wird man angesichts der oben geschilderten Defizite bejahen können. Es ist allerdings zweifelhaft, ob auch eine vergleichbare Interessenlage besteht. Dagegen spricht zum einen, dass die Durchsetzung zivilrechtlicher Ansprüche in §§ 32 Abs. 1 Nr. 4, 33 Abs. 1 Nr. 2 lit. a BDSG 2018 nur teilweise zur Motivlage des Arbeitgebers passt. Zum anderen ist die Ausnahme in Art. 14 Abs. 5 lit. b Alt. 3 DS-GVO, wonach die Informationspflichten nicht erfüllt werden müssen, wenn dies die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt sehr stark auf Situationen zugeschnitten, bei denen wie in der Forschung oder dem Archiv- und Statistikwesen kein direkter Kommunikationskanal zur betroffenen Person besteht. Damit ist die Situation im Beschäftigungsverhältnis nicht vergleichbar.[1259] 1053

Deutlich näher liegt dagegen der Weg über Art. 88 DS-GVO. Die mitgliedstaatlichen Gesetzgeber sind für die Beschränkung der Informationspflichten nämlich nicht allein auf die Öffnungsklausel in Art. 23 DS-GVO angewiesen. Sie können auch die bereichsspezifischen Öffnungsklauseln nutzen.[1260] Dass Art. 88 Abs. 1 DS-GVO auch spezifischere Regelungen zu den Informationspflichten erlaubt, zeigt sich schon an Art. 88 Abs. 2 DS-GVO, der Maßnahmen zur Wahrung der Grundrechte der betroffenen Person u.a. für den Fall fordert, dass Überwachungssysteme am Arbeitsplatz eingesetzt werden. 1054

Demnach bedarf es aber immer noch einer deutschen bereichsspezifischen Beschränkung der Informationspflichten nach Art. 13 Abs. 1 und 2 DS-GVO, mit der die Öffnungsklausel in Art. 88 Abs. 1 DS-GVO aufgegrif- 1055

1258 *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 100; i.E. ebenso *Byers*, NZA 2017, S. 1086, 1090.

1259 Allgemein gegen eine analoge Anwendung von Art. 14 Abs. 5 DS-GVO *Dix*, in: Simitis et al. 2019, Art. 14 DS-GVO, Rn. 22; BeckOK DSR/*Schmidt-Wudy*, Art. 14 DS-GVO, Rn. 95.

1260 *Bäcker*, in: Kühling/Buchner 2018, Art. 13 DS-GVO, Rn. 101.

fen wird. Diese Funktion erfüllt § 26 Abs. 1 S. 2 DS-GVO,[1261] wonach die Verarbeitung von Beschäftigtendaten zur Aufdeckung von Straftaten nur zulässig ist, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

1056 Die Norm in § 26 Abs. 1 S. 2 BDSG 2018 erwähnt zwar die verdeckte Datenverarbeitung nicht ausdrücklich. Sie wäre aber wenig wert, wenn sie nicht auch und vor allem dieses Vorgehen legitimieren würde. Dann ist es nur folgerichtig, dass auch die Informationspflichten nach Art. 13 Abs. 1 und 2 DS-GVO beschränkt werden. Dabei unterliegt sie nicht den Anforderungen aus Art. 23 DS-GVO, sondern denen aus Art. 88 DS-GVO, insbesondere den Maßnahmen aus Absatz 2. Dem hat der deutsche Gesetzgeber mit der Einschränkung der Tatbestandsmerkmale in § 26 Abs. 1 S. 2 BDSG 2018 Rechnung getragen. Einer Regelung, wie und wann die Informationspflichten nachzuholen sind, insbesondere für den Fall, dass sich der Verdacht nicht erhärtet, wie in § 32 Abs. 2, 3 BDSG 2018 wäre wünschenswert gewesen, ist nach § 88 Abs. 2 DS-GVO aber nicht zwingend. Hier wird man auf Art. 14 Abs. 3 DS-GVO zurückgreifen müssen.

1057 Im Umkehrschluss ist die verdeckte Datenerhebung außerhalb von § 26 Abs. 1 S. 2 BDSG 2018, also zu anderen Zwecken als zur Aufdeckung von Straftaten, nicht zulässig. Dies gilt insbesondere auch für die Datenerhebung zu Kontrollzwecken (zur Kategorisierung der Zwecke siehe 3.6.1.2.3.1, S. 508).[1262] Die praktischen Konsequenzen hierfür sind aber überschaubar. Eine verdeckte Datenerhebung zu Kontrollzwecken, etwa eine verdeckte Ortung als Maßnahme gegen „Arbeitszeitbetrug" wäre nicht selten ungeeignet und damit nicht erforderlich,[1263] jedenfalls aber unangemessen und damit rechtswidrig.[1264]

1261 I.E. BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 149, 153; *Seifert*, in: Simitis et al. 2019, Art. 88 DS-GVO, Rn. 136; wohl auch.

1262 A.A. *Chandna-Hoppe*, NZA 2018, S. 614, 617, der für die entscheidende Frage auf BAG v. 29.6.2017 – 2 AZR 597/16, E 159, S. 278–293 (=NZA 2017, S. 1179) abstellt. Die Entscheidung erging aber noch zum Verhältnis von § 32 Abs. 1 S. 1 und 2 BDSG 2003. A.A. zur Ortung, aber auch nach der alten Rechtslage *Gola*, ZD 2012, S. 308, 310; *Göpfert/Papst*, DB 2016, S. 1015, 1018.

1263 VG Lüneburg v. 19.3.2019 – 4 A 12/19, CR 2019, S. 367, Rn. 46 ff.

1264 Zur Ortung *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 113.

Umstritten sind damit lediglich Konstellationen, in denen die Arbeitsleistung – vergleichbar derjenigen in einem Callcenter[1265] – nicht nur mithilfe, sondern allein durch das technische System erfolgt und sich ohne die Überwachung des Systems weder im Hinblick auf das Leistungsverhalten noch im Hinblick auf das Leistungsergebnis kontrollieren lässt. Eine Beschränkung der Informationspflichten ließe sich nur über Art. 88 DS-GVO i.V.m. § 26 Abs. 1 S. 1 BDSG 2018 konstruieren. Dieser Erlaubnistatbestand ist nach der hier vertretenen Meinung (siehe 3.1.5.2, S. 248) aber in vielen Konstellationen nicht anwendbar. Und selbst wenn man mit der Gegenmeinung argumentierte, § 26 Abs. 1 S. 1 BDSG müsse in seiner durch die Rechtsprechung ausgestalteten Form bewertet werden, würde sich hieran nichts ändern. Die verdeckte Erhebung von Beschäftigtendaten zu Kontrollzwecken für diese speziellen Situationen ist nämlich keineswegs höchstrichterlich geklärt. 1058

3.4.1.5.3.5 Umsetzung für Assistenz- und Produktionssysteme

Der Arbeitgeber kann seine Assistenz- und Produktionssysteme grundsätzlich zwar so gestalten, dass der betroffene Beschäftigte die Datenerhebung nicht unterbinden kann. Er muss ihm aber zum Zeitpunkt der Erhebung die Informationen nach Art. 13 Abs. 1 und 2 DS-GVO mitteilen. Das betrifft vor allem den – genauen – Zweck der Verarbeitung (Abs. 1 lit. c), die Dauer oder die Kriterien für die Festlegung der Dauer (Abs. 2 lit. a), das Recht auf Auskunft und auf Beschwerde (Abs. 2 lit. b und d) und den Einsatz von Systemen zur automatischen Entscheidungsfindung (Abs. 2 lit. f). 1059

Der verantwortliche Arbeitgeber muss den betroffenen Beschäftigten zumindest vor[1266] dem ersten Datenerhebungsvorgang aktiv informieren. Dass die Informationen lediglich abrufbar sind, genügt nicht. Anders als Art. 15 DS-GVO statuiert Art. 13 DS-GVO kein reines Auskunftsrecht. Es 1060

1265 Für die ausnahmsweise Zulässigkeit des heimlichen Mithörens für den Fall, dass es bereits zu Kundenbeschwerden gekommen ist *Kort,* RdA 2018, S. 24, 28; BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 172.1; *Zöll,* in: Taeger/Gabel 2019, § 26 BDSG, Rn. 42; sogar ohne diese Einschränkung (und darum abzulehnen) *Jordan et al.,* BB 2008, S. 2626, 2628.

1266 *Bäcker,* in: Kühling/Buchner 2018, Art. 13 DS-GVO, Rn. 57; a.A. *Ingold,* in: Sydow 2018, Art. 7 DS-GVO, Rn. 12, der aber auch einen anderen Anwendungsbereich für Art. 13 DS-GVO zugrunde legt.

genügt aber, wenn die aktive Mitteilung lediglich einen Hinweis enthält, wo die Informationen abgerufen werden können.[1267]

1061 Auf eine Folgeinformation kann gemäß Art. 13 Abs. 4 DS-GVO verzichtet werden, wenn die betroffene Person bereits über die Informationen verfügt. Was sich wie ein weitgehender Ausschluss von Folgeinformationen anhört, ist durchaus voraussetzungsvoll. Zum einen müssen die Informationen in dem Umfang von Art. 13 Abs. 1 und 2 DS-GVO vorliegen. Dass der betroffene Beschäftigte grob weiß, welche Daten zu welchem Zweck wie verarbeitet werden, reicht nicht aus.[1268] Zudem müssen sich die Informationen im Herrschaftsbereich der betroffenen Person befinden, sodass sie ohne die Mitwirkung des Verantwortlichen abgerufen werden können.[1269]

1062 Damit ein datenerhebendes Assistenzsystem- und Produktionssystem selbst diese Anforderungen für den Ausschluss der Folgeinformationen nach Art. 13 Abs. 4 DS-GVO erfüllt, müssten zum einen alle Informationen nach Art. 13 Abs. 1 und 2 DS-GVO auf seinem lokalen Speicher abgelegt sein. Denn wenn die Informationen auf einem Server des Arbeitgebers bereitlägen, bedürfte es wieder seiner, also des Verantwortlichen Mitwirkung. Zum anderen müsste es dem Beschäftigten zum jederzeitigen Zugriff bereitstehen, also auch außerhalb der Arbeitszeit. Hier muss der Arbeitgeber auf andere Formen der Information setzen, insbesondere auf schriftliches Informationsmaterial.[1270]

3.4.1.6 Die sonstigen Grundsätze

1063 Die übrigen Grundsätze spielen für diese Arbeit keine zentrale Rolle und sollen darum nur der Vollständigkeit halber erläutert werden.

3.4.1.6.1 Rechtmäßigkeit

1064 Nach Art. 5 Abs. 1 lit. a DS-GVO müssen Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Das Merkmal der Rechtmäßigkeit,

1267 *Bäcker,* in: Kühling/Buchner 2018, Art. 13 DS-GVO, Rn. 59.
1268 *Bäcker,* in: Kühling/Buchner 2018, Art. 13 DS-GVO, Rn. 84.
1269 *Bäcker,* in: Kühling/Buchner 2018, Art. 13 DS-GVO, Rn. 87.
1270 Kritisch zum Medienbruch *Breyer,* DuD 2018, S. 311, 312.

das wie eine bloße Selbstverständlichkeit anmutet, erschließt sich vor dem Hintergrund der Vorgabe des Art. 8 Abs. 2 S. 1 GRC, wonach Daten nur mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen. Diese lediglich für Grundrechtsadressaten geltende Regelung des Primärrechts wird über Art. 5 Abs. 1 lit. a DS-GVO in das Sekundärrecht überführt. Damit gilt es für selbst nicht unmittelbar grundrechtsgebundene Private.

Wie aus ErwG 40 hervorgeht, ist mit der Formulierung „auf rechtmäßige Weise" nämlich gemeint, dass personenbezogene Daten nur mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden dürfen, die sich aus der Verordnung oder – soweit die Verordnung darauf Bezug nimmt – aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedstaaten ergibt. 1065

Dieses Prinzip wird verbreitet als „Verbot mit Erlaubnisvorbehalt"[1271] bezeichnet. Nähme man diese Formulierung ernst, müsste jede Datenverarbeitung von einer Behörde zugelassen werden. Solche Regelungen gibt es im Datenschutzrecht nur vereinzelt, z.B. im Sozialdatenschutz in § 287 Abs. 1 SGB V und § 75 IV SGB X.[1272] Im Grundsatz bedarf es aber lediglich eines Erlaubnistatbestands, etwa eines aus Art. 6 Abs. 1 UAbs. 1 DS-GVO. Besser ist es darum vom „Erlaubnisprinzip" zu sprechen.[1273] 1066

Die zweite Dimension des Rechtmäßigkeitsgebots nimmt die Mitgliedstaaten in die Pflicht, wenn diese eine der vielen Öffnungsklauseln der Datenschutz-Grundverordnung nutzen.[1274] Die Vorgabe aus Art. 8 Abs. 2 S. 1 GRC, der zufolge eine gesetzlich geregelte Grundlage legitim sein muss, wird so in die Verordnung transferiert. Gemäß ErwG 41 sollte die mitgliedstaatliche Rechtsgrundlage klar und präzise und in ihrer Anwendung für den Rechtsunterworfenen vorhersehbar sein. 1067

1271 Z.B. *Buchholtz/Stentzel,* in: Gierschmann et al. 2018, Art. 5 DS-GVO, Rn. 24; *Ingold,* in: Sydow 2018, Art. 7 DS-GVO, Rn. 8 f.; *Kramer,* in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 10; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 5.

1272 *Roßnagel,* in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 35 f.; *Roßnagel,* NJW 2019, S. 1, 5.

1273 *Roßnagel,* NJW 2019, S. 1, 5.

1274 *Herbst,* in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 8.

3.4.1.6.2 Treu und Glauben im Übrigen

1068 Die Formel Treu und Glauben in Art. 5 Abs. 1 lit. a DS-GVO ist ähnlich wie auch z.B. im Zivilrecht nach § 242 BGB ein Ansatzpunkt für Rücksichtnahmepflichten,[1275] die in ihrer Abstraktheit aber so schwer zu fassen sind, dass sie lediglich anhand typischer Fallgruppen bestimmt werden können.[1276] Das darf nicht dazu verleiten, die zu § 242 BGB anerkannten Fallgruppen eins zu eins auf Art. 5 Abs. 1 lit. a DS-GVO zu übertragen; die Begriffe der Datenschutz-Grundverordnung sind autonom auszulegen, damit das Unionsrecht einheitlich bleibt.[1277] Das dahinterliegende Prinzip unterscheidet sich indessen nicht. So darf der Verantwortliche keine Fehlvorstellungen der betroffenen Person ausnutzen[1278] oder sich nicht widersprüchlich verhalten[1279] und hat grundsätzlich die Datenverarbeitung zu wählen, die von der betroffenen Person am besten überblickt und kontrolliert werden kann.[1280]

1069 Aus diesen Rücksichtnahmepflichten wird z.B. abgeleitet, dass bei der betroffenen Person nicht der Eindruck entstehen darf, die Datenverarbeitung beruhe auf ihrer Einwilligung, wenn sie in Wahrheit auf einem anderen Erlaubnistatbestand beruht. Die betroffene Person unterläge dann nämlich der irrigen Vorstellung, die Zulässigkeit der Datenverarbeitung über ihre Einwilligung bzw. deren Widerruf steuern zu können.[1281] Im Verbund mit anderen Anforderungen an die Einwilligung (siehe 3.6.1.5, S. 523) kann dies deren praktische Tauglichkeit als Verarbeitungsgrundlage empfindlich einschränken.

3.4.1.6.3 Richtigkeit

1070 Gemäß Art. 5 Abs. 1 lit. d DS-GVO müssen personenbezogenen Daten sachlich und erforderlichenfalls auf dem neusten Stand sein. Dadurch wird auch klargestellt, dass es für die Frage, ob ein Datum personenbezogen ist,

---

1275 Kritisch *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 20.
1276 *Buchholtz/Stentzel*, in: Gierschmann et al. 2018, Art. 5 DS-GVO, Rn. 25; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 7.
1277 *Kramer*, in: Auernhammer 2020, Art. 5 DS-GVO, Rn. 14.
1278 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 8.
1279 *Buchholtz/Stentzel*, in: Gierschmann et al. 2018, Art. 5 DS-GVO, Rn. 25.
1280 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 9.
1281 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 8.

nicht darauf ankommt, ob die betreffende Information zutrifft[1282] oder aktuell ist. Gerade in Situationen, in denen es zulässig ist, personenbezogene Daten für bestimmte Entscheidungen heranzuziehen, kann die betroffene Person ein starkes Interesse daran haben, dass diese Entscheidungen auf der Grundlage sachlich richtiger Informationen getroffen werden.

Der Verantwortliche muss angemessene Maßnahmen ergreifen, um unrichtige Daten zu löschen oder zu berichtigen. Zur Berichtigung kann bei veralteten Daten auch zählen, einen Hinweis auf ihren Stand aufzunehmen, wenn der Zweck ihrer fortwährenden Speicherung gerade darin besteht, Vergangenes zu dokumentieren.[1283] Sie sind dann nach Art. 5 Abs. 1 lit. d DS-GVO im Hinblick auf die Zwecke ihrer Verarbeitung richtig und müssen bzw. dürfen nicht gelöscht oder inhaltlich verändert werden.[1284] Daten zu berichtigen bedeutet also nicht in jedem Fall, sie auf den aktuellen Stand zu bringen. 1071

Im hier zu untersuchenden Beschäftigungskontext betrifft dies vor allem personelle Einzelentscheidungen, etwa zur Einstellung, Beförderung, Versetzung oder Kündigung. Die Daten hierfür zu ermitteln ist aber nicht der Hauptzweck von Assistenzsystemen. Sie dienen vielmehr der Organisation der Arbeit und der Optimierung der damit verbundenen Prozesse. Der für die Datenverarbeitung verantwortliche Arbeitgeber hat hier bereits ein vitales Eigeninteresse an der Richtigkeit der Daten. Im Mittelpunkt der Untersuchung steht darum die Fragen, welche Daten verarbeitet werden dürfen und weniger, welcher Aufwand zumutbar ist, diese Daten richtig zu halten. 1072

3.4.1.6.4 Speicherbegrenzung

Gemäß Art. 5 Abs. 1 lit. e Hs. 1 DS-GVO müssen Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dieser Grundsatz der Speicherbegrenzung konkretisiert das allgemeine Erforderlichkeitsprinzip, wie es auch in den Erlaubnistatbeständen nach Art. 6 Abs. 1 UAbs. 1 lit. b bis f DS-GVO niedergelegt ist, in 1073

1282 *Karg,* in: Simitis et al. 2019, Art. 4 Nr. 1 DS-GVO, Rn. 29.
1283 *Roßnagel,* in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 141.
1284 BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 31.

zeitlicher Hinsicht. Insofern könnte man den eigenständigen Regelungsgehalt der Norm anzweifeln.

1074 Für einen eigenen Regelungsgehalt spricht dagegen bereits der Umstand, dass der Verordnungsgeber die Speicherbegrenzung eigens geregelt hat. Setzt man das hier vertretene umfassende Verständnis der Datenminimierung voraus, wonach nicht allein die Daten – also ihre Erhebung –, sondern sämtliche Datenverarbeitung – also auch ihre Speicherung – auf das zur Zweckerreichung notwendige Maß zu beschränken ist (siehe 3.4.1.3.1, S. 374), ist der Grundsatz der Speicherbegrenzung zwar bereits vollständig in Prinzip der Datenminimierung enthalten. Dass der Verarbeitungsvorgang des Speicherns so hervorgehoben wird, zeigt zusammen mit der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO aber sehr deutlich, dass der Verantwortliche nicht mehr benötigte Daten auf eigene Initiative löschen muss.[1285] Seine Handlungspflicht entsteht nicht erst mit einem Löschverlangen der betroffenen Person nach Art. 17 Abs. 1 DS-GVO.[1286]

1075 Ein weiteres Argument für einen eigenen Regelungsgehalt kann der ausdrücklichen Erwähnung der Formel „die die Identifizierung der betroffenen Person ermöglicht" entnommen werden. Damit ist in der Sache zwar nichts Anderes gemeint als der Personenbezug von Daten nach Art. 4 Nr. 1 DS-GVO. Da sich aber Art. 5 Abs. 1 DS-GVO ausweislich der Eingangsworte von vornherein auf personenbezogenen Daten bezieht, ist die Formulierung genau genommen redundant. Sie betont aber, dass es zur Einhaltung der Speicherbegrenzung (und damit der Datenminimierung) nicht notwendig ist, die Daten zu löschen, sondern es genügt, den Personenbezug zu entfernen.[1287]

1076 Schließlich spricht auch die Stellung der Worte „nur so lange" für einen eigenen Regelungsgehalt. Die Vorgabe lautet nicht, Daten nur so lange wie nötig in einer personenbezogenen Form zu speichern, sondern vielmehr sie in einer Form zu speichern, die nur so lange wie nötig einen Personenbezug aufweist. Die Form bezieht sich also nicht auf das einzelne Datum, sondern auf das gesamte Datenverarbeitungssystem des Verantwortlichen. Dadurch wird deutlich, dass sich der Personenbezug nicht aus dem Datum selbst ergeben muss, sondern dass er auch erst durch zusätzliches

1285 EuGH, ECLI:EU:C:2014:317, Rn. 72 – *Google Spain*.
1286 *Herbst*, in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 67; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 33.
1287 I.E. *Frenzel*, in: Paal/Pauly 2018, Art. 5 DS-GVO, Rn. 45; *Herbst*, in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 66.

Wissen hergestellt werden kann, insbesondere solches, das an anderen Stellen im Datenverarbeitungssystem gespeichert ist.

Im Übrigen ergeben sich für den Grundsatz der Speicherbegrenzung aber keine Besonderheiten. Für die Details kann darum auf die Ausführungen zum Grundsatz der Datenminimierung verwiesen werden. 1077

3.4.1.6.5 Integrität und Vertraulichkeit

Gemäß Art. 5 Abs. 1 lit. f DS-GVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Die Norm fokussiert dabei auf das unbefugte Löschen und Verändern sowie die unbefugte Kenntnisnahme von Daten, was durch geeignete technische und organisatorische Maßnahmen unterbunden werden soll. 1078

Die Datensicherheit ist ein selbstverständlicher Bestandteil des Datenschutzes. Sie zielt auf die technische und organisatorische Sicherung der übrigen Grundsätze[1288] und ist insofern eine der grundlegenden Voraussetzungen, um überhaupt erst Daten verarbeiten zu dürfen. In der Industrie 4.0 werden die hiermit verbundenen Anforderungen an den Verantwortlichen steigen, schon allein, weil mehr Daten erhoben werden und sich durch die zunehmende Vernetzung mehr Angriffspunkte bieten.[1289] Dieses enorme technische Problem ist aber aus rechtlicher Sicht keine Besonderheit der Industrie 4.0 und soll hier darum nicht vertieft diskutiert werden. 1079

3.4.1.6.6 Rechenschaftspflicht

Die beiden wesentlichen Aussagen der Rechenschaftspflicht sind, dass der Verantwortliche erstens von sich aus für die Einhaltung der Datenschutzgrundsätze in Art. 5 Abs. 1 DS-GVO zu sorgen hat, sich seine Rolle also nicht darauf beschränkt, auf entsprechende Verlangen der betroffenen Person zu reagieren. Zweitens muss er die Einhaltung nachweisen können. Wie sich aus der Konkretisierung dieses Grundsatzes nach Art. 24 Abs. 1 DS-GVO ergibt, hat er für diesen Nachweis technische und organisatorische Maßnahmen zu treffen. 1080

1288 *Roßnagel*, in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 168.
1289 *Acatech* 2013, S. 50 f.

1081 Es genügt folglich nicht, nachweisen zu können, dass es im Ergebnis zu keinen Verstößen gekommen ist. Der Verantwortliche muss vielmehr bereits im Vorfeld und durch die Aufsichtsbehörden überprüfbar Maßnahmen ergreifen, die dies sicherstellen. Der Verordnungsgeber legt dadurch größeres Gewicht auf die – kontrollierbare – Eigenverantwortung des Verantwortlichen.[1290]

3.4.2 Datensparsamkeit und Datenschutz durch Technikgestaltung

1082 Das Prinzip des Datenschutzes durch Technik nach Art. 25 DS-GVO ist kein Teil der Datenschutzgrundsätze in Art. 5 Abs. 1 DS-GVO. Vor allem in einer stark technisch geprägten Umgebung wie der Industrie 4.0 stellt es aber ein wesentliches Instrument zur Sicherstellung dieser Grundsätze und damit zu Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO dar. Die Anforderungen, die an die Technikgestaltung in Art. 25 DS-GVO gestellt werden, wirken dadurch gleichsam auf diese Grundsätze zurück. So beeinflussen sie nicht zuletzt dasjenige, was nach dem Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO zur Zweckerreichung erforderlich ist.

1083 Für ein tieferes Verständnis vor allem der Grundsätze der Zweckbindung und der Datenminimierung nach Art. 5 Abs. 1 lit. b und c DS-GVO muss darum auch das Prinzip des Datenschutzes durch Technik näher untersucht werden. Hierzu wiederum ist es hilfreich, die aktuelle Rechtslage vom aus dem alten Recht bekannten Prinzip der Datensparsamkeit abzugrenzen, das ebenfalls eng mit den genannten Grundsätzen in Verbindung stand.

3.4.2.1 Das Konzept der Datensparsamkeit im alten Recht

1084 Das Bundesdatenschutzgesetz enthielt bis zu seiner Anpassung an die Datenschutz-Grundverordnung mit dem Prinzip der Datenvermeidung und Datensparsamkeit ein Prinzip, welches dem Prinzip der Datenminimierung sehr nahesteht. Nach § 3a S. 1 BDSG 2003 waren die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie die Auswahl und

1290 Zum Ganzen *Herbst*, in: Kühling/Buchner 2018, Art. 5 DS-GVO, Rn. 78 f.; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 38.

Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Gemäß Satz 2 waren dazu personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich war und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erforderte.

Das Prinzip der Datenvermeidung und Datensparsamkeit ist dem ersten Anschein nach nicht in die Datenschutz-Grundverordnung übernommen worden. Zumindest findet sich keine Norm, die in ihrem Wortlaut der Regelung in § 3a BDSG 2003 ähneln würde. Regeln zum technischen Datenschutz finden sich dagegen weiterhin in der Datenschutz-Grundverordnung, in Art. 25 DS-GVO. Dies allein wäre nicht weiter bedeutsam, schließlich hat die Datenschutz-Grundverordnung eine Reihe von Änderungen mit sich gebracht, ohne dass sich der Regelungsgehalt der Verordnung nur mit dem Wissen um die Vorgängerregelung erklären ließe. 1085

Das alte Prinzip der Datenvermeidung und Datensparsamkeit hat aber durchaus noch für die Kenntnis des heutigen Rechts Bedeutung. Es eignet sich zum einen gut dazu, die verschiedenen Ebenen zu illustrieren, die für die Entscheidung über die Gestaltung eines Datenverarbeitungssystems relevant sind und welcher rechtlichen Kontrolle die einzelnen Ebenen unterliegen (siehe 3.4.2.1.3.1.3, S. 430 und zur Parallele im Beschäftigtendatenschutz 3.6.1.2.1.6, S. 505). Darüber hinaus ist z.B. *Roßnagel* der Auffassung, dass das Prinzip der Datensparsamkeit weiter im primärrechtlichen Prinzip der Verhältnismäßigkeit enthalten ist und so auf den Grundsatz der datenschutzgerechten Systemgestaltung in Art. 25 Abs. 1 DS-GVO einwirkt.[1291] Um zu ermitteln, ob und inwieweit das Prinzip der Datensparsamkeit und der mit ihm verbundene technische Datenschutz Spuren im geltenden Recht hinterlassen hat, ist es angezeigt, den Inhalt und die Wirkweise dieses Prinzips genauer zu betrachten. 1086

Angesichts der augenfälligen Nähe des Prinzips der Datenvermeidung und Datensparsamkeit zum in Art. 5 Abs. 1 lit. b DS-GVO geregelten Prinzip der Datenminimierung gilt es zunächst, die beiden Prinzipien gegeneinander abzugrenzen. Da das Prinzip der Datenminimierung mit dem althergebrachten Prinzip der Erforderlichkeit des Datenumgangs übereinstimmt, wie es in Art. 6 Abs. 1 lit. c DSRL niedergelegt und z.B. in den Erlaubnistatbeständen des §§ 28 Abs. 1 Nr. 1 und 32 Abs. 1 S. 1 BDSG 2003 enthal- 1087

1291 *Roßnagel,* in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 124.

ten war, kann hier auf die zum alten Recht formulierten Abgrenzungsversuche zurückgegriffen werden.

1088 Unter dem Begriff der Datenvermeidung wird der völlige, unter dem der Datensparsamkeit der möglichst weitgehende Verzicht auf die Verarbeitung personenbezogener Daten verstanden. Insofern kann auch einfach nur von Datensparsamkeit gesprochen werden; der Begriff der Datenvermeidung bedeutet lediglich die Vollendung der Datensparsamkeit und hat keine eigenständige Bedeutung.

3.4.2.1.1 Gemeinsames Ziel

1089 Die Verarbeitung personenbezogener Daten möglichst zu vermeiden ist – anders, als es der Begriff nahelegt – kein Alleinstellungsmerkmal des Prinzips der Datensparsamkeit. Auch das Erforderlichkeitsprinzip verlangt, nur jene personenbezogenen Daten zu verarbeiten, die zur gleich wirksamen Zweckerreichung gebraucht werden. Kann der Zweck auch komplett ohne eine solche Datenverarbeitung verfolgt werden, ist dies auch auf diese Weise zu realisieren.

1090 Die beiden Prinzipien verfolgen demnach dasselbe Ziel, nämlich Eingriffe in das Recht auf informationelle Selbstbestimmung auf ein notwendiges Maß zu beschränken. Es ergibt sich aus dem allgemeinen Prinzip der Verhältnismäßigkeit, das durch die Grundrechtecharta bzw. das Grundgesetz vorgegeben wird und im Ergebnis sowohl für den unmittelbar gebundenen Staat als auch für den mittelbar gebundenen privaten Akteur gelten. Der Unterschied betrifft vielmehr die Methode und insbesondere den genauen Punkt, an dem die beiden Prinzipien anknüpfen.

3.4.2.1.2 Ansatzpunkt der Datenminimierung bzw. des Erforderlichkeitsprinzips

1091 Das Erforderlichkeitsprinzip setzt an einem Verarbeitungszweck an,[1292] den der Verantwortliche entweder allein oder im Zusammenwirken mit dem Betroffenen festlegt (siehe 3.4.1.4, S. 389). Steht dem Verantwortlichen – wie im Arbeitsverhältnis dem Arbeitgeber nach § 106 GewO – als

1292 *Bäumler*, DuD 1999, S. 258, 260; BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 25.

Ausfluss seiner wirtschaftlichen Betätigungsfreiheit ein Leistungsbestimmungsrecht zu, ist ihm bei der Konkretisierung dieses Zwecks ein gewisser Spielraum zuzubilligen. Der genaue Umfang dieses Spielraums ist in erster Linie dem jeweiligen Rechtsgebiet zu entnehmen – hier also dem Arbeitsrecht.

Einem etwaigen Entscheidungsspielraum erwachsen auch aus den Grundsätzen der Zweckbindung und der Datenminimierung gewisse Grenzen. So darf ein Zweck auf der einen Seite nicht so abstrakt sein, dass das Merkmal der Vereinbarkeit der Weiterverarbeitung mit dem Erhebungszweck seine Eigenständigkeit verliert (siehe 3.4.1.2.3.4, S. 367). Auf der anderen Seite darf er aber auch nicht so konkret sein, dass die Erforderlichkeitsprüfung im engeren Sinne leerläuft (siehe 3.4.1.4.2.3, S. 394). Die Anforderungen sind aber genau genommen nicht inhaltlicher Art, sondern betreffen nur den Präzisierungsgrad, mit dem Zwecke zu formulieren sind. Zu einer inhaltlichen Prüfung kommt es nach dem Prinzip der Datenminimierung erst im Punkt der Angemessenheit. Hier werden aber nur jene Zwecke ausgeschieden, die unmäßig in die Interessen der betroffenen Person eingreifen. Konstellationen, die im Ergebnis noch als angemessen bewertet werden, die aber mit einigem Aufwand des Verantwortlichen noch besser hätten gestaltet werden können, sind nicht erfasst. Der Grundsatz der Datenminimierung enthält kein Optimierungsgebot. 1092

Aus diesen Beschränkungen des Prinzips der Datenminimierung folgt, dass der Zweck innerhalb der genannten Grenzen nicht hinterfragt wird. Wie er inhaltlich zu konkretisieren ist, also in Richtung datenintensiver oder datenschutzfreundlicher Prozesse, wird zumindest nicht umfassend thematisiert. Darin liegt der Unterschied zum Prinzip der Datensparsamkeit. 1093

3.4.2.1.3 Ansatzpunkt der Datensparsamkeit

Das Prinzip der Datensparsamkeit nach § 3a BDSG fristete in der datenschutzrechtlichen Diskussion eher ein Schattendasein. Das mag vor allem dem Umstand geschuldet gewesen sein, dass weder der Inhalt dieses Prinzips noch der Grad der Verpflichtung, der für die verantwortliche Stelle von der Regelung ausgehen sollte, umfassend geklärt oder allgemein anerkannt worden war. Die Meinungen reichten hier von der Einordnung als 1094

bloße Wiederholung des Erforderlichkeitsprinzips[1293] bis zur Anerkennung der Datensparsamkeit als eigenständiges Prinzip[1294] bzw. von der Einstufung als reine gesetzgeberische Zielvorstellung ohne jede Bindungskraft[1295] bis hin zur verbindlichen – wenn auch nicht sanktionsbewehrten[1296] – Rechtspflicht[1297].

3.4.2.1.3.1 Gestaltung und Auswahl von Datenverarbeitungssystemen

1095 Die Regelungen in § 3a BDSG 2003 lassen sich besser verstehen, wenn man sie nach Systematik und Gesetzgebungshistorie in drei Bereiche aufteilt. Der erste und ältere Bereich in § 3a S. 1 BDSG 2003 betraf die Auswahl und Gestaltung von Datenverarbeitungssystemen. Die Regelung wurde 1997 mit § 3 Abs. 4 TDDSG ins Datenschutzrecht eingeführt[1298] und von dort 2001 im Wesentlichen wortgleich in § 3a S. 1 BDSG 2003 übernommen. Sie lautete in der damaligen Fassung[1299] in § 3a S. 1 BDSG 2003 „Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen." Mit einer Erweiterung im Jahr 2009 (siehe 3.4.2.1.3.2.1, S. 432) war sie bis zur Anpassung des Bundesdatenschutzgesetzes an die Datenschutz-Grundverordnung in Kraft. Sie enthielt zwei Aussagen, die sich erst bei genauerem Hinsehen voneinander abgrenzen ließen.

1293 *Simitis,* DuD 2000, S. 714, 716; *Simitis,* KritV 2000, S. 359, 373.

1294 *Dix,* in: Roßnagel 2003, Kapitel 3.5, Rn. 25; *Richter,* DuD 2012, S. 576, 577; *Roßnagel, et al.* 2001, S. 101; *Scholz,* in: Simitis 2014, § 3a BDSG, S. 33 f.

1295 *Gola/Schomerus* 2015, § 3a BDSG, Rn. 2.

1296 *Scholz,* in: Simitis 2014, § 3a BDSG, Rn. 57 f.; für eine nur mittelbare Wirkung BeckOK DSR/*Schulz*, § 3a BDSG, Rn. 28.

1297 *Dix,* in: Roßnagel 2003, Kapitel 3.5, Rn. 23; *Scholz,* in: Simitis 2014, § 3a BDSG, Rn. 27.

1298 § 3 TDDSG in der Fassung vom 22.7.1997, BGBl. I, S. 1870: „Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat (sic!) sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen."

1299 Fassung vom 18.5.2001, eingefügt durch Art. 1 Nr. 5 des G v. 18.5.2001, BGBl. I S. 904.

3.4.2.1.3.1.1 Bekräftigung des technischen Datenschutzes

Betrachtet man die zeitgenössische Literatur zu § 3 Abs. 4 TDDSG, so schien die Regelung zunächst dem ärgerlichen Umstand Rechnung zu tragen, dass die Erforderlichkeit der Datenverarbeitung damals wie auch heute mit der Systemgestaltung gerechtfertigt wird – und nicht umgekehrt, wie es das Erforderlichkeitsprinzip vorsieht (siehe 3.4.1.4).[1300] In diesem Punkt hatte § 3a BDSG 2003 nur deklaratorische Wirkung. 1096

Daran änderte auch der Umstand nichts, dass die Regelung ausdrücklich den technischen Datenschutz in Form der Auswahl und Gestaltung der Datenverarbeitungssysteme ansprach. Dieser Ansatz mag 1998, als das Teledienstedatenschutzgesetz in Kraft trat,[1301] innovativ gewesen sein. Allerdings waren in § 9 BDSG 2003 auch damals schon technische und organisatorische Maßnahmen verlangt, „um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten." Diese Regelung wurde überwiegend auf die in der Anlage genannten und vornehmlich auf Datensicherheit ausgerichteten Ziele reduziert.[1302] Zu den Anforderungen des Bundesdatenschutzgesetzes gehörte aber immer auch das in den einzelnen Erlaubnistatbeständen verankerte Erforderlichkeitsprinzip. Der technische Datenschutz wurde also nicht erst mit § 3 Abs. 4 TDDSG oder § 3a S. 1 BDSG 2003 in das Datenschutzrecht eingeführt. Ob dies in der Praxis gelebt wurde und wird, ist eine andere Frage. 1097

3.4.2.1.3.1.2 Anforderungen an die Zwecksetzung selbst

Der Aussagegehalt der Norm erschöpfte sich aber nicht in deklaratorischen Bekräftigungen des Erforderlichkeitsprinzips. Anders als das Erforderlichkeitsprinzip war der Grundsatz der Datensparsamkeit nicht etwa auf das Ziel ausgerichtet, nur *so viele* Daten wie *nötig*, sondern *so wenig wie möglich* zu verarbeiten. Die Datensparsamkeit betrifft demnach zwar auch die konkrete Zweckerreichung, wie sie vom Erforderlichkeitsprinzip adres- 1098

1300 So jedenfalls kann *Bäumler,* DuD 1999, S. 258, 260 verstanden werden, wenn dieser davon spricht, dass systemseitig erzeugte Daten bisher nicht wirksam hätten kontrolliert werden können, weil sie im Zweifel als erforderlich, weil vermeintlich unvermeidbar angesehen worden sein.

1301 Art. 11 IuKDG, BGBl. I 1997, S. 1870.

1302 *Ernestus,* in: Simitis 2014, § 9 BDSG, Rn. 2.

siert wird. Die eigentliche Innovation bestand beim Grundsatz der Datensparsamkeit aber darin, dass er über die Erforderlichkeitsprüfung hinausging und auch inhaltliche Anforderungen an den Zweck selbst formulierte, statt ihn als festgelegt zu akzeptieren.[1303]

1099 Eine datensparsame Zwecksetzung sollte so erfolgen, dass in letzter Konsequenz so wenig personenbezogene Daten wie möglich verarbeitet werden. Wie schon der auf die Auswahl und die Gestaltung des Datenverarbeitungssystems gerichtete Ansatz zeigt, wird diese Möglichkeit in erster Linie durch die technische Verfügbarkeit innovativer datenschutzfreundlicher Produkte geprägt. Was das betrifft, zielte der Grundsatz der Datensparsamkeit auf eine optimale Systemgestaltung, sodass sich der Verantwortliche nicht auf gemeinhin übliche oder auch nur verbreitete Lösungen zurückziehen konnte, wie dies im Beispiel des Bezahlvorgangs beschrieben wurde (siehe 3.4.1.4.8.1, S. 404).

1100 Die Zielstellung, so wenig personenbezogene Daten wie möglich zu erheben, verarbeiten und zu nutzen, taugte allein allerdings noch nicht dazu, das gewünschte Optimum zu bestimmen. Denn wenn der Verantwortliche gehalten ist, den gewählten Zweck zu hinterfragen und ggf. einen alternativen Zweck zu wählen, der auf der Ebene der Erforderlichkeit dann zu einer geringeren Datenverarbeitung führt, so bedarf es eines Kriteriums, um zu bestimmen, ob dieser alternative Zweck immer noch dem eigentlichen Interesse des Verantwortlichen – im Folgenden unternehmerisches Ziel genannt – entspricht. Es stellt sich also die Frage, wie das Primärziel zu bestimmen ist, an dem sich die Möglichkeit seiner datensparsamen Verfolgung messen lassen muss.

3.4.2.1.3.1.3 Primärziel als Ansatzpunkt der Datensparsamkeit

1101 Da das Prinzip der Datensparsamkeit Anforderungen an den Zweck selbst formulierte, brauchte es eines Ansatzpunktes, der logisch eine Abstraktionsebene über der Zwecksetzung stand. Eine aus sich selbst heraus verständliche oder auch nur übliche Begrifflichkeit existierte hier nicht. Wie bereits angedeutet, soll im Folgenden der Einfachheit halber für diese Abstraktionsebene der Begriff des unternehmerischen Ziels verwendet wer-

1303 *Dix*, in: Roßnagel 2003, Kapitel 3.5, Rn. 25; *Richter*, DuD 2012, S. 576, 577; *Roßnagel, et al.* 2001, S. 101; *Scholz*, in: Simitis 2014, § 3a BDSG, S. 33 f.; kritisch *Simitis*, DuD 2000, S. 714, 716; *Simitis*, KritV 2000, S. 359, 373.

den. Mit diesem unternehmerischen Ziel stand das gesetzgeberisch vorgegebene Ziel der datensparsamen Gestaltung in der Regel zu einem gewissen Grad im Widerspruch. Dieser Konflikt kann – wenn überhaupt – erst durch eine bewusste und abwägende Entscheidung des Verantwortlichen aufgelöst werden.

Im nichtöffentlichen Bereich beschreibt das unternehmerische Ziel in der Regel einen betriebswirtschaftlich vorteilhaften Zustand, den der Verantwortliche erreichen will. Um dieses Ziel zu erreichen, greift der Verantwortliche zu bestimmten Mitteln, von denen er glaubt, damit sein Ziel erreichen zu können. Mit dieser Wahl der Mittel definiert er den Zweck einer späteren Datenverarbeitung entweder gleich selbst oder bereitet zumindest den Boden für eine spätere einvernehmliche Zweckkonkretisierung mit dem Betroffenen. 1102

Das Prinzip der Datensparsamkeit knüpfte an diese Wahl der Mittel an und verlangte, zumindest solche Alternativen anzubieten, mit deren Benutzung gar keine oder wenigstens eine nicht so umfangreiche oder intensive Verarbeitung personenbezogener Daten verbunden ist. Eine datensparsame Gestaltung ist darauf gerichtet, bereits den Zweck so festzulegen, dass eine im Anschluss durchzuführende Erforderlichkeitsprüfung in einen möglichst kleinen Eingriff in die informationelle Selbstbestimmung der betroffenen Person mündet. Ob dies möglich ist, hängt davon ab, ob technische Lösungen existieren, welche die Erreichung des unternehmerischen Ziels auch auf datensparsame Weise erlauben. 1103

3.4.2.1.3.1.4 Beispiel eines Bezahlsystems

Bleibt man im oben angeführten Beispiel des Online-Handels wäre dies z.B. das Ziel, die Zahlung des Kunden zu möglichst niedrigen Transaktionskosten entgegennehmen zu können, mit einem System, das weit verbreitet ist und bei seinen Kunden auf hohe Akzeptanz stößt. Legt man diese Kriterien zu Grunde, würde der Verkäufer wahrscheinlich gängige Systeme wie die Zahlung per Kreditkarte, über einen Online-Bezahldienst wie PayPal oder per Überweisung anbieten. 1104

Eine datensparsame Gestaltung des Prozesses „Bezahlen“ liefe dagegen darauf hinaus, z.B. auch das Zahlen mit Gutscheinkarten zu erlauben. Wählt der Käufer diese Option im Rahmen der Vertragsanbahnung, wäre der Zweck entsprechend hierauf konkretisiert. Eine Verarbeitung personenbezogener Daten wäre dann nicht mehr erforderlich, selbst wenn der Käufer noch weitere Zahlungsdaten angegeben hätte und die Transaktionskosten 1105

für die entsprechenden Systeme für den Verkäufer niedriger lägen. Der Bezahlvorgang wurde bereits auf die datensparsame Methode festgelegt.

3.4.2.1.3.2 Gestaltung der Datenverarbeitung allgemein

1106 Im weiteren Verlauf der Normgeschichte wurde 2009 der spezifisch auf technische Instrumente gerichtete Ansatz des Prinzips der Datensparsamkeit in § 3a S. 1 BDSG 2003 erweitert. Statt nur die Auswahl und Gestaltung von Datenverarbeitungssystemen sollten nun auch ganz allgemein die Erhebung, Verarbeitung und Nutzung personenbezogener Daten an dem Ziel ausgerichtet sein, so wenig wie möglich davon zu erheben, zu verarbeiten und oder zu nutzen. Auch dieser Teil der Datensparsamkeit enthielt wieder zwei Aussagen. Mit der ersten bekräftigte er – rein deklaratorisch – den Grundsatz der Erforderlichkeit. Insofern ergaben sich keine Unterschiede zu den Ausführungen unter dem Punkt 3.4.2.1.3.1.1, S. 429.

3.4.2.1.3.2.1 Der Grundsatz der nichttechnischen Datensparsamkeit

1107 Die zweite Aussage setzte, wie auch die Regeln zur Technikgestaltung, vor der Zwecksetzung an. Der Unterschied bestand lediglich darin, dass es sich nicht um Entscheidungen über den Einsatz von Technik handeln musste, sondern sämtliche Entscheidungen beeinflusst werden sollten, die sich auf die Zwecksetzung auswirkten.[1304] Das konnte zum einen darin bestehen, in nicht technisierten Bereichen datensparsame Alternativen anzubieten. Im Beispiel des Online-Handels wäre das etwa die Möglichkeit gewesen, online bestellte Ware gegen Zahlung vor Ort am Lager abzuholen. Auf diese Weise müsste der Käufer seine Adresse nicht angeben, ohne dass es hierfür einer spezifischen technischen Lösung bedurft hätte.

1108 Der erweiterte, allgemeine Ansatz in § 3a S. 1 BDSG 2003 konnte sich aber auch auf Bereiche des Datenumgangs beziehen, die in erster Linie technisch realisiert werden.[1305] Entscheidend war nämlich nicht, wie der unter dem Gesichtspunkt der Datensparsamkeit zu optimierende Datenumgang durchgeführt wurde, sondern welcher Gestalt die dazu ergriffene Lösung war. Der Datensparsamkeit konnte nämlich auch schlicht dadurch gedient

1304 BT-Drucks. 16/13657, S. 17; *Scholz,* in: Simitis 2014, § 3a BDSG, Rn. 43; BeckOK DSR/*Schulz*, § 3a BDSG, Rn. 5.

1305 A.A. *Scholz,* in: Simitis 2014, § 3a BDSG, Rn. 39.

sein, dass man bestimmte datenintensive Funktionen nicht realisierte. Im Unterschied zum Erforderlichkeitsprinzip ging es dabei um Funktionen, deren Umsetzung rechtmäßig gewesen wäre, u.a. deswegen, weil sie zwar in das Recht der betroffenen Person auf informationelle Selbstbestimmung eingriffen, dieser Eingriff aber als erforderlich und angemessen zu bewerten gewesen wäre. Der Grundsatz der Datensparsamkeit verlangte, auch solche rechtmäßigen Funktionen anders zu gestalten oder eben schlicht nicht umzusetzen, soweit sich dies als möglich erwies.[1306]

Dieser Ansatz war in vielfacher Hinsicht problematisch. Erstens griff er enorm in die grundrechtlich geschützte Entscheidungsfreiheit der Beteiligten ein.[1307] Zweitens konnte er in bestimmten Bereichen zu Konflikten mit anderen Rechtsprinzipien, also gewissermaßen zu unerwünschten Nebenwirkungen führen. Und drittens neigte er schließlich dazu, das Datenschutzrecht zu überfrachten und die Abgrenzung zu anderen Gebieten zu verwischen.[1308] Dies kann am besten an dem folgenden Beispiel erläutert werden. 1109

3.4.2.1.3.2.2 Beispiele datenintensiver Anwendungen

Im Beispiel des Online-Handels wären wohl personalisierte Angebote als besonders datenintensiv zu qualifizieren gewesen. Die Alternative hätte folglich darin bestanden, auf eine eher allgemein gehaltene Kundenansprache zu setzen. 1110

Anschaulicher lässt sich die Problematik der nichttechnischen Datensparsamkeit am Beispiel verschiedener Preismodelle beschreiben. So werden von einigen Autoversicherern Versicherungspolicen angeboten, deren Prämie sich nach dem tatsächlichen Fahrverhalten der jeweiligen Fahrer des Autos bemisst.[1309] Solange sich aus den Daten über das Fahrverhalten – etwa wie intensiv ein Auto beschleunigt oder abgebremst wird[1310] – valide 1111

1306 So ähnlich *Roßnagel, et al.* 2001, S. 102; *Scholz,* in: Simitis 2014, § 3a BDSG, Rn. 34; kritisch *Bull,* NJW 2006, S. 1617, 1619; BeckOK DSR/*Schulz*, § 3a BDSG, Rn. 52.

1307 *Roßnagel, et al.* 2001, S. 102.

1308 Zum unklaren Verhältnis zu bekannten Verhältnismäßigkeitsprinzip, *Simitis,* DuD 2000, S. 714, 716; *Simitis,* KritV 2000, S. 359, 373.

1309 *Schwichtenberg,* DuD 2015, S. 378 f.

1310 Zur Funktionsweise sog. Pay-As-You-Drive-Versicherungen *Gerpott/Berg,* ZVersWiss 2012, S. 3, 7 f.

Schadensrisiken ableiten lassen, ist an dieser auf freiwilliger Basis erfolgenden Datenerhebung aus datenschutzrechtlicher Sicht kein Anstoß zu nehmen. Die Herausforderungen liegen hier darin, grundlegenden Anforderungen wie denen an die Datensicherheit, die Transparenz oder die Wahrung des Erforderlichkeitsprinzips gerecht zu werden. Auch kann ein solcher Datenumgang unangemessen sein, wenn nicht mit hinreichender Wahrscheinlichkeit ausgeschlossen werden kann, dass der Verantwortliche mit Hilfe der Daten einen besonders tiefen Einblick in die Persönlichkeit des jeweiligen Fahrers nehmen kann.[1311] Sind aber alle diese – gewissermaßen nachgelagerten – Anforderungen erfüllt, hätten auch sehr datenintensive Preismodelle datenschutzkonform gestaltet werden können.[1312]

1112 Mit dem Prinzip der Datensparsamkeit hätte ein solches Preismodell aber nicht überein gebracht werden können.[1313] Ein datensparsamer Ansatz hätte hier darin bestanden, bewusst auf relevante Informationen zu verzichten, das Preismodell also u.U. ungerechter zu gestalten, weil man es weniger am individuell beeinflussbaren Risikoverhalten ausgerichtet hätte. Dies barg aber nicht zuletzt einen Konflikt mit Vorgaben zur Diskriminierungsfreiheit. Wo nämlich keine individuellen Merkmale herangezogen werden könnten, müsste womöglich auf gruppenbezogene Annahmen abgestellt werden. Statt also die individuelle Risikogeneigtheit eines Fahrstils zu ermitteln, würden also u.U. alle jungen Fahrer pauschal als riskant eingestuft, das Individuum also für seine Altersgenossen „in Haftung" genommen.

1113 Hieran zeigt sich auch eine Überfrachtung des Datenschutzes. Argumentiert man nämlich pauschal mit dem Anpassungsdruck, den das Bundesverfassungsgericht im Volkszählungsurteil zur Begründung des Rechts auf informationelle Selbstbestimmung herangezogen hat, gehen dadurch notwendige Differenzierungen verloren. So dürften gegen einen Anpassungsdruck hin zu einer weniger gefährlichen Fahrweise wesentlich weniger Bedenken vorzubringen sein als in anderen Bereichen. Wäre beispielsweise

1311 *Lüdemann,* ZD 2015, S. 247, 250.

1312 So zumindest grundsätzlich *Metzger,* GRUR 2019, S. 129, 132; einschränkend auf den Fall, dass der Versicherte der einzige Fahrer ist *Lüdemann,* ZD 2015, S. 247, 252.

1313 Kritisch zu einem solchen Effekt allgemein *Bull,* NJW 2006, S. 1617, 1619; BeckOK DSR/*Schulz*, § 3a BDSG, Rn. 52.

die Prämie einer privaten[1314] Krankenversicherung davon abhängig gemacht worden, wie viele Schritte eine mit dem Internet verbundene und auf den Versicherten registrierte Armbanduhr aufzeichnet, hätte dies ungleich mehr Bedenken hervorgerufen. Schließlich wäre der Anpassungsdruck, seinen Lebenswandel möglichst gesund zu gestalten, weit kritischer zu beurteilen, als derjenige möglichst unfallfrei Auto zu fahren. Die Gesundheit ist ein sensibler Bereich, deren Nachteile allein das Individuum selbst spürt; das Fahrverhalten weist dagegen einen weit größeren Gesellschaftsbezug auf. Durch das Ziel der Datensparsamkeit ist hier allein wenig gewonnen. Es kommt vielmehr auf die Wertung desjenigen Rechtsgebiets an, an die das Datenschutzrecht anknüpft.

3.4.2.2 Technischer Datenschutz in der Datenschutz-Grundverordnung

Wie bereits erwähnt enthält die Datenschutz-Grundverordnung mit dem Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO und den Vorgaben zum Datenschutz durch Technikgestaltung in Art. 25 Abs. 1 DS-GVO Regelungen, die den in § 3a BDSG 2003 normierten Grundsätzen der Datensparsamkeit und des technischen Datenschutzes sehr nahekommen.[1315] Bei einem direkten Vergleich ist allerdings Vorsicht geboten. Die Vorschriften der Datenschutz-Grundverordnung basieren auf der Datenschutzrichtlinie 95/46/EG, nicht auf den die Richtlinie umsetzenden nationalen Vorschriften. Die Regelung in § 3a BDSG, speziellen deren Satz 2, ist zwar 2001 im Zuge der Umsetzung der Richtlinie in das Bundesdatenschutzgesetz aufgenommen worden; sie hat in der Richtlinie aber keine Wurzeln, ist also eher nur bei dieser Gelegenheit ins Gesetz gelangt (siehe 3.4.2.1.3.1, S. 428). 1114

Im Hinblick auf das Prinzip, das den beiden Regelungen – § 3a BDSG 2003 und Art. 25 Abs. 1 DS-GVO – zugrunde liegt, lässt sich aber dennoch eine gewisse Kontinuität beobachten. Mit gewissen Einschränkungen gilt dies auch für Art. 17 Abs. 1 DSRL, in dem sich ebenfalls Ansätze zum Datenschutz durch Technik finden. Die Regelung zielte zwar schwerpunktmäßig auf die Sicherheit der Verarbeitung ab, forderte ihrem Wortlaut 1115

1314 Die gesetzliche Krankenversicherung beruht auf dem Solidaritätsprinzip *Becker/Kingreen*, in: Becker/Kingreen 2018, § 1 SGB V, Rn. 4. Risikoausschlüsse sind hier nicht zugelassen. Die Missbrauchsmotivation ist entsprechend niedriger als im Bereich der risikobasierten privaten Krankenversicherungen.

1315 So auch *Hartung*, in: Kühling/Buchner 2018, Art. 25 DS-GVO, Rn. 3.

nach aber auch Maßnahmen „gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten."[1316]. Bei allen hier noch darzulegenden Unterschieden bleibt der Grundgedanke nämlich derselbe: Der Schutz der informationellen Selbstbestimmung kann nicht allein auf Ge- oder Verbote gestützt werden, sondern bedarf auch einer Absicherung durch technische und organisatorische Maßnahmen.[1317]

3.4.2.2.1 Struktur von Art. 25 Abs. 1 DS-GVO

1116 Nach Art. 25 Abs. 1 DS-GVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen sowie die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. Dabei hat er den Stand der Technik, die Implementierungskosten und die Art, den Umfang und die Zwecke der Verarbeitung zu berücksichtigen, sowie auch die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen. Im Hinblick auf den Zeitpunkt wird schließlich verlangt, dass die Maßnahmen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung getroffen werden.

1117 Die Regelung in Art. 25 Abs. 1 DS-GVO ist in ihrer mangelnden Strukturiertheit und unnötigen Redundanz ein Paradebeispiel für die unglückliche Regelungstechnik in der Datenschutz-Grundverordnung. Auf ihren Kern zurückgeführt verlangt die Norm vom Verantwortlichen, verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um die Einhaltung der Anforderungen der Datenschutz-Grundverordnung entsprechend abzusichern. Wie noch zu zeigen ist, setzt die Regelung dabei aber teilweise eigene Akzente, die auf die technisch umzusetzenden Anforderungen zurückwirken können.

1316 Zu einer ähnlichen Interpretation zu § 9 BDSG 1990, siehe 3.4.2.1.3.1.1, S. 429.

1317 *Hansen*, in: Simitis et al. 2019, Art. 25 DS-GVO, Rn. 17; *Mantz*, in: Sydow 2018, Art. 25 DS-GVO, Rn. 2.

3.4.2.2.2 Zielsetzung

Die Zielsetzung des Art. 25 Abs. 1 DS-GVO ist denkbar breit und umfasst die Einhaltung sämtlicher Anforderungen der Datenschutz-Grundverordnung.[1318] Insofern steht die Norm noch am ehesten in einer Linie mit § 9 BDSG 2003 und weniger mit § 3a S. 2 BDSG 2003 oder mit ihrer – im weitesten Sinne – Vorgängernorm in Art. 17 DSRL. Die beiden letztgenannten fokussieren nämlich eher auf die Minimierung bzw. die Rechtmäßigkeit der Verarbeitung, während Art. 25 Abs. 1 DS-GVO alle Anforderungen der Datenschutz-Grundverordnung anspricht. Vom Wortlaut der Norm sind damit z.B. auch ohne Weiteres die Anforderungen hinsichtlich der Rechte der Betroffenen in Kapitel 3 der Datenschutz-Grundverordnung erfasst,[1319] ohne dass es darauf ankäme, ob die Verletzung dieser Rechte auch die Rechtmäßigkeit der Verarbeitung nach sich zöge. 1118

Um die Zielsetzung zu unterstreichen werden zwei Aussagen herausgehoben. Die erste betrifft die Datenschutzgrundsätze nach Art. 5 DS-GVO, insbesondere den Grundsatz der Datenminimierung. Der zweite betrifft den Schutz der Rechte der betroffenen Person, der zum Ende des Absatzes genannt wird. Beide Aussagen sind rein deklaratorischer Natur.[1320] Die Datenschutzgrundsätze sind keine Programmsätze, sondern echte Rechtsnormen und insofern eigenständige Anforderungen der Datenschutz-Grundverordnung; der Schutz der Rechte der betroffenen Person ist bereits in Art. 1 Abs. 2 DS-GVO als Ziel genannt, gilt also ohnehin für alle Normen der Datenschutz-Grundverordnung. 1119

Der Betonung der Datenminimierung lässt sich eine gewisse Schwerpunktsetzung entnehmen, welche die Norm insbesondere von der Regelung zur Datensicherheit in Art. 32 DS-GVO abgrenzt.[1321] Es zeigt aber auch, dass der Ansatz der Datensparsamkeit nach § 3a S. 1 BDSG 2003 der Regelung in Art. 25 Abs. 1 DS-GVO fremd ist. Die Datenminimierung formuliert wie das Erforderlichkeitsprinzip (siehe 3.4.2.1.2, S. 426) und anders als der Grundsatz der Datensparsamkeit (siehe 3.4.2.1.3, S. 427) keine Anforderungen an die Zwecksetzung, sondern knüpft vielmehr an einen bereits ge- 1120

1318 *Hansen*, in: Simitis et al. 2019, Art. 25 DS-GVO, Rn. 31; *Mantz*, in: Sydow 2018, Art. 25 DS-GVO, Rn. 19.
1319 *Mantz*, in: Sydow 2018, Art. 25 DS-GVO, Rn. 19.
1320 So auch *Hansen*, in: Simitis et al. 2019, Art. 25 DS-GVO, Rn. 31 f.
1321 Eine genaue Abgrenzung der beiden Normen ist kaum zu leisten, siehe *Brüggemann*, in: Auernhammer 2020, Art. 25 DS-GVO, Rn. 7; *Mantz*, in: Sydow 2018, Art. 25 DS-GVO, Rn. 83.

setzten Zweck an. Entsprechend kann Art. 25 Abs. 1 DS-GVO im Gegensatz zu § 3a S. 1 BDSG nicht die Forderung entnommen werden, die Auswahl und Gestaltung von Datenverarbeitungssystemen nach dem Prinzip der Datensparsamkeit auszurichten.

1121 Die technischen und organisatorischen Maßnahmen nach Art. 25 Abs. 1 DS-GVO müssen demnach lediglich sicherstellen, dass die Datenverarbeitung im für die Zweckerfüllung notwendigen Rahmen bleibt. Ein Optimierungsgebot hin zu immer datenschutzfreundlicherer Technik, wie es – wenn auch nicht durchsetzbar – in § 3a S. 1 BDSG normiert war (siehe 3.4.2.1.3.1.2, S. 429), ist hiermit nicht verbunden. Dies steht auf den ersten Blick in einem Spannungsverhältnis mit der Vorgabe, die Maßnahmen unter Berücksichtigung des Stands der Technik zu treffen, der zwar kein technisches Optimum bedeutet, sich aber auch nicht von vornherein auf das weithin übliche begrenzen lässt. Hierauf wird bei den Maßnahmen (siehe 3.4.2.2.5, S. 444) näher einzugehen sein.

3.4.2.2.3 Adressatenkreis des technischen Datenschutzes

1122 Um ihre Ziele zu verfolgen, nimmt die Norm ihrem Wortlaut nach lediglich den Verantwortlichen in die Pflicht. Auftragsdatenverarbeiter werden – anders als in Art. 32 DS-GVO – in Art. 25 Abs. 1 DS-GVO nicht erwähnt. Da eine Auftragsdatenverarbeitung gemäß Art. 28 Abs. 1 DS-GVO aber nur zulässig ist, wenn Auftragsdatenverarbeiter „hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt", dürften seine Pflichten nicht wesentlich anders ausfallen.[1322]

1123 Auch im Ergebnis nicht erfasst sind dagegen die Hersteller der Datenverarbeitungssysteme.[1323] Der Verordnungsgeber setzt hier allein auf die Steuerung der Nachfrage. Dies zeigt sich ausdrücklich in ErwG 78, demzufolge die Hersteller zu einer datenschutzkonformen Gestaltung ihrer Produkte lediglich angehalten werden sollen. Zur Stärkung der Grundsätze des Datenschutzes durch Technik sollte diesen u.a. bei öffentlichen Ausschreibungen Rechnung getragen werden.

1322 *Hartung,* in: Kühling/Buchner 2018, Art. 25 DS-GVO, Rn. 12.

1323 *Hartung,* in: Kühling/Buchner 2018, Art. 25 DS-GVO, Rn. 13; kritisch *Hornung,* ZD 2011, S. 51, 54 f.; *Jandt,* DuD 2017, S. 562 f.; *Richter,* DuD 2012, S. 576, 578 ff.

Der Verordnungsgeber formuliert hier vergleichsweise zurückhaltend und nimmt zumindest ausdrücklich nur öffentliche Stellen in die Pflicht. Der nachfrageorientierte Ansatz ist aber nur konsequent, wenn sich der Verantwortliche nicht darauf zurückziehen kann, dass die notwendige Technik am Markt nicht oder nur im Bündel mit im konkreten Fall unzulässigen Funktionen verfügbar ist. Nachfragedruck kann nämlich nur aufgebaut werden, wenn eine Datenverarbeitung auch mangels geeigneter Technik unzulässig sein kann. Ansonsten bliebe Art. 25 Abs. 1 DS-GVO ähnlich zahnlos wie § 3a BDSG 2003. 1124

3.4.2.2.4 Risikobewertung im Rahmen von Art. 25 Abs. 1 DS-GVO

In der Abwägung, welche technischen und organisatorischen Maßnahmen der Verantwortliche gemäß Art. 25 Abs. 1 DS-GVO letztlich zu treffen hat, sind mehrere Kriterien zu berücksichtigen. Die Grundlage hierfür muss aber stets eine Risikobewertung liefern. Der Verantwortliche muss klären, wie groß die mit der Verarbeitung verbundene Gefahr für die Rechte des Betroffenen ist und welche Maßnahmen folglich überhaupt als geeignet in Betracht kommen. 1125

Auch hinsichtlich der Risikobewertung verwendet der Verordnungsgeber in Art. 25 Abs. 1 DS-GVO sich in ihrem Bedeutungsgehalt wenigstens überschneidende Formulierungen. Das Risiko wird der allgemeinen Wortbedeutung folgend als Kombination aus Eintrittswahrscheinlichkeit und (Schadens-)Schwere definiert. Statt um die „Eintrittswahrscheinlichkeit und Schwere der […] *Risiken*“ müsste es aber um die Eintrittswahrscheinlichkeit und Schwere des *Schadens* gehen, in deren Abhängigkeit sich die Höhe des Risikos,[1324] letztlich also des zu erwartenden Schadens bemisst.[1325] 1126

Neben diesem Risiko sollen auch die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung in der Entscheidung eine Rolle spielen, welche technischen und organisatorischen Maßnahmen getroffen werden. Diese Kriterien können im weitesten Sinne als Verarbeitungskontext bezeichnet werden. Da sie – wie auch in ErwG 76 festgehalten ist – maßgeblich über die Eintrittswahrscheinlichkeit und die Schwere der Rechtsguts- 1127

1324 So auch *Piltz,* in: Gola 2018, Art. 24 DS-GVO, Rn. 25.

1325 Zu dieser grundlegenden Definition des Risikobegriffs statt Vieler *Hansen,* in: Simitis et al. 2019, Art. 32 DS-GVO, Rn. 28.

verletzung entscheiden, nehmen sie als Prüfungspunkt keine eigenständige, sondern nur eine der Risikobewertung untergeordnete Rolle ein.

1128 Die näheren Vorstellungen zu den einzelnen Punkten in Art. 25 Abs. 1 DS-GVO werden vom Verordnungsgeber im ErwG 75 erläutert. Hier listet er eine Reihe potenzieller Rechtsgutsverletzungen, Schäden und Begehungsweisen auf, die bei der Risikobewertung zu berücksichtigen sind. Diese Erwägungen sind nicht normativ zwingend (siehe 3.4.1.2.3.3, S. 362), geben aber einen Einblick in den Willen des Verordnungsgebers.

3.4.2.2.4.1 Rechtsgutsverletzungen

1129 Als Schutzgüter, deren Verletzung überhaupt erst einen relevanten Schaden herbeiführen kann, werden in ErwG 75 erneut – der Zielsetzung der DS-GVO in Art. 1 Abs. 2 DS-GVO folgend – alle Rechte oder Freiheiten der betroffenen Person genannt. Neben der einleitenden Erwähnung ergibt sich dies aus der Formulierung, wonach es als potenzieller Schaden zu werten ist, wenn „die betroffenen Personen um ihre Rechte und Freiheiten gebracht" werden – wobei die Bezeichnung als Schaden nichts daran ändert, dass es sich zunächst nur um eine Rechtsgutsverletzung handelt, aus der ein Schaden entstehen könnte.

1130 Indem alle Rechte und Freiheiten einbezogen werden, kommt zum Ausdruck, dass Datenschutz als Schutz der informationellen Selbstbestimmung der betroffenen Person als Vorfeldschutz wirkt. Er verfolgt zwar durchaus einen Selbstzweck, weil er z.B. die Entscheidungsautonomie der betroffenen Person stärkt, dient aber letztlich auch wesentlich dazu, die informationelle Grundlage der Ausübung anderer Grundrechte und Freiheiten zu gewährleisten. Potenzielle Auswirkungen auf andere Grundrechte, insbesondere auf die Berufsfreiheit nach Art. 12 GG[1326] – die gerade bei der spezifischen Betrachtung des Beschäftigungsverhältnisses im weiteren Verlauf dieser Arbeit eine Rolle spielt – sind folglich auch im Rahmen der Risikobewertung zu beachten.

1326 Die spezifischen Gefahren für die im Arbeitsrecht verankerten Rechte der betroffenen Person sind an den nationalen Grundrechten zu messen, siehe 3.1.6, S. 255.

3.4.2.2.4.2 Schäden

Auch hinsichtlich der aus den Rechtsgutsverletzungen potenziell resultierenden Schäden ergibt sich aus ErwG 75 ein denkbar weiter Fokus. Erfasst sind sowohl physische und materielle als auch immaterielle Schäden. Beispielhaft werden Diskriminierungen, finanzielle Verluste und Rufschädigungen genannt, aber auch andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile sollen bei der Risikobewertung berücksichtigt werden. Der letzten Formulierung lässt sich eine gewisse Filterwirkung entnehmen, dergestalt, dass außerhalb physischer Schäden – die wohl vor allem bei der fehlerhaften oder sonst unrechtmäßigen Verarbeitung von Gesundheitsdaten auftreten können – nur solche potenziellen Schäden berücksichtigt werden sollen, die eine Erheblichkeitsschwelle überschreiten. 1131

Wo diese Erheblichkeitsschwelle liegt, lässt sich nicht abstrakt bestimmen, zumal auch immaterielle – also finanziell nicht oder nur schwer fassbare – Schäden abgedeckt werden sollen. Es dürfte allerdings klar sein, dass nicht jede unrechtmäßige Verarbeitung zu einem Schaden führt.[1327] Es gilt zwar nach wie vor die Grundannahme des Bundesverfassungsgerichts, dass es keine per se belanglosen Daten gibt,[1328] ein Schaden infolge der unrechtmäßigen Verarbeitung also nie allein deshalb ausgeschlossen werden kann, weil die Daten für sich genommen vermeintlich keinen oder so gut wie keinen Aussagewert hätten. Das bedeutet aber nicht, dass nicht andere Umstände, insbesondere aus dem Verarbeitungskontext, einen Schaden sehr unwahrscheinlich oder nur marginal gravierend erscheinen lassen können. Gerade wenn die Möglichkeiten fehlen, die Daten mit weiteren Informationen über die betroffene Person zu verknüpfen, können sie tatsächlich nahezu belanglos bleiben. 1132

3.4.2.2.4.3 Begehungsweisen und Verarbeitungskontext

Im ErwG 75 werden zusätzlich zu Schutzgütern und Schäden noch bestimmte Begehungsweisen und Verarbeitungskontexte aufgelistet, was wohl betonen soll, dass es sich dabei um besonders risikoreiche Phänomene handelt. Neben den unmittelbar als problematisch erkennbaren Fällen, in denen große Mengen oder besondere Kategorien personenbezogener 1133

1327 *Mantz*, in: Sydow 2018, Art. 25 DS-GVO, Rn. 77; a.A. wohl *Hansen*, in: Simitis et al. 2019, Art. 32 DS-GVO, Rn. 28.

1328 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 45 – *Volkszählung*.

Daten verarbeitet oder von denen viele Personen betroffen sind, werden hier auch die unbefugte Aufhebung der Pseudonymisierung und die Profilbildung genannt.

1134 Die Aufdeckung von Pseudonymen ist insofern risikoreich, als hierdurch auf einen Schlag eine Vielzahl an Daten mit der betroffenen Person in Bezug gesetzt werden können. Der Profilbildung kommt eine besondere Bedeutung zu, weil sie ein ungewöhnlich umfassendes Bild von der betroffenen Person zeichnet. Dass es dabei nicht allein um die privaten Angelegenheiten der Person gehen muss, zeigt die Erwähnung der Aspekte Arbeitsleistung, Zuverlässigkeit, Verhalten und Aufenthaltsort, die sämtlich auch im Beschäftigungskontext eine Rolle spielen können. In diesen Fällen wird man wohl im Zweifel von einem hohen Risiko für die Rechte der betroffenen Person ausgehen müssen.[1329]

1135 Die Aufzählung im ErwG 75 ist ausdrücklich nicht abschließend gemeint. So ließe sich die Reihe nach der Profilbildung auch ohne Weiteres mit der automatisierten Einzelentscheidung fortsetzen.[1330] Beide Phänomene werden in Art. 22 Abs. 1 DS-GVO in einem Atemzug genannt. Diese typisierte Risikobewertung des Verordnungsgebers wirkt sich auch auf die Gestaltung von Assistenzsystemen aus, die der besseren Koordinierung der Arbeit dienen, etwa indem sie Aufgaben nach dem individuellen Fähigkeits- und Kenntnisstand der Beschäftigten oder ihrer Entfernung zum Einsatzort vergeben (siehe 1.3.2, S. 71). Sie basieren notwendigerweise auf einem Profil – auch wenn es durchaus unterschiedlich detailliert ausgestaltet sein kann – und können prinzipiell auch vollautomatisch ablaufen.

1136 Den in ErwG 75 angesprochenen Kriterien der Menge der Daten sowie der betroffenen Personen lassen sich ebenfalls weitere Kategorien hinzufügen. So wirkt sich z.B. auch die Anzahl derer, die tatsächlich auf die Daten zugreifen können, auf die Risikoträchtigkeit der Verarbeitung aus. In die Risikobewertung eines Systems kann darum auch eingehen, über welche Schnittstellen es verfügt, über die – u.U. auch unbeabsichtigt – Daten intern oder extern weitergegeben werden könnten.[1331]

1137 Der Zweck einer Datenverarbeitung ist in mehrfacher Hinsicht relevant. Erstens steht er über das Erforderlichkeitsprinzip in direkter Verbindung

---

1329 In die Richtung auch *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 41.

1330 *Brüggemann,* in: Auernhammer 2020, Art. 25 DS-GVO, Rn. 17; *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 23.

1331 Zum Zusammenhang von Schnittstellen und dem Prinzip der Datenminimierung *DSK* 2018, S. 13.

mit der Art und dem Umfang der Datenverarbeitung. Da die beiden letzten Punkte aber ohnehin zu berücksichtigen sind, kommt diesem Aspekt des Zwecks keine eigenständige Bedeutung zu. Zweitens kann sich der Zweck auch auf Schutzgüter außerhalb des Rechts auf Schutz personenbezogener Daten auswirken. Ist er nämlich von vornherein darauf ausgelegt, auch in andere Rechte und Freiheiten der betroffenen Person einzugreifen, ergibt sich daraus ein höheres Risiko, als wenn die Verarbeitung allein am Datenschutzrecht zu messen wäre. Drittens spielt es eine Rolle, ob er vom Verantwortlichen vollständig einseitig gesetzt oder – wie im Bereich der Verarbeitung zur Erfüllung eines Vertrags – auf einer Grundlage bestimmt wird, die im Einvernehmen mit dem Betroffenen geschaffen wurde.[1332]

Dies spricht dafür, grundrechtsintensivere Situationen wie den Beschäftigungsbereich, in denen die betroffene Person der Leitungs- und damit auch Zwecksetzungsmacht des Verantwortlichen ausgesetzt ist, zwar nicht prinzipiell als hochriskant, aber doch als tendenziell riskanter einzustufen. Dies gilt umso mehr, wenn eine Datenverarbeitung potenziell zu arbeitsrechtlichen Maßnahmen führen, welche die wirtschaftliche Existenz des Beschäftigten bedrohen können (siehe dazu 3.6.1.2.3.1, S. 508). 1138

3.4.2.2.4.4 Risikostufen

Für die Risikobewertung empfiehlt sich ein strukturiertes Vorgehen,[1333] bei dem die Risiken nach objektiver Betrachtung verschiedenen Stufen zugeordnet werden. Nach ErwG 76 kann man dabei nur zu dem Ergebnis kommen, dass ein (normales) Risiko oder ein hohes Risiko vorliegt; ein geringes Risiko ist nicht vorgesehen.[1334] Diese Einschätzung des Verordnungsgebers geht wohl auf die Einsicht zurück, dass es im Anwendungsbereich der Datenschutz-Grundverordnung per Definition zu einem Eingriff in das Grundrecht der betroffenen Person auf den Schutz ihrer personenbezogenen Daten nach Art. 8 GRC kommen muss – ansonsten wäre die 1139

1332 *Brüggemann,* in: Auernhammer 2020, Art. 25 DS-GVO, Rn. 17. Die einvernehmliche Zwecksetzung führt hier nicht dazu, dass die betroffene Person in die Position des Verantwortlichen rückt, siehe 3.4.1.4.4, S. 395.

1333 Dazu ausführlich *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 27 ff.

1334 *Piltz,* in: Gola 2018, Art. 24 DS-GVO, Rn. 46; a.A. wohl *Bieker,* DuD 2018, S. 27, 31; *Brüggemann,* in: Auernhammer 2020, Art. 25 DS-GVO, Rn. 18; *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 23.

Verordnung gemäß Art. 2 Abs. 1 DS-GVO nicht anwendbar. Wo aber Grundrechte betroffen sind, kann das Risiko a priori nicht gering sein.[1335] Immerhin lässt sich nicht ausschließen, dass ein immaterieller Schaden entsteht, und sei es „nur" eine Einschränkung der Entscheidungsfreiheit der betroffenen Person. Wie eine Risikoabstufung typisiert vorgenommen werden kann, wird für den Beschäftigungskontext später noch genauer auszuführen sein (siehe 3.4.2.2.7, S. 460).

1140 Praktisch folgt aus dieser Einschätzung, dass der Verantwortliche wohl unter keinen Umständen auf Schutzmaßnahmen verzichten können wird. Sobald personenbezogene Daten verarbeitet werden, muss er die Einhaltung der Anforderungen der Datenschutz-Grundverordnung technisch und organisatorisch absichern. Er kann diese Standards nicht allein mit einem Hinweis auf ein vermeintlich geringes Risiko absenken; hierzu müssen weitere Umstände hinzukommen (siehe 3.4.2.2.5.4.2, S. 453). Ist umgekehrt sogar ein hohes Risiko zu attestieren, sind diese Maßnahmen aber nicht einfach nur zu verstärken, es ist auch eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO vorzunehmen, die der Risikobewertung nach Art. 25 Abs. 1 DS-GVO zwar im Grundsatz ähnelt, aber weitaus umfangreicher ausfällt.[1336] Die Risikobewertung nach Art. 25 Abs. 1 DS-GVO fungiert insofern als Schwellwertanalyse für die Datenschutz-Folgenabschätzung.

3.4.2.2.5 Maßnahmen

1141 Die vom Verantwortlichen zu ergreifenden technischen und organisatorischen Maßnahmen müssen geeignet sein, die Zielsetzung in Art. 25 Abs. 1 DS-GVO (siehe 3.4.2.2.2, S. 437) zu erfüllen, also sicherstellen, dass den Anforderungen der Datenschutz-Grundverordnung genügt wird. In Frage kommen sowohl Maßnahmen, welche die Eintrittswahrscheinlichkeit des Schadens verringern, als auch solche, welche die potenzielle Schadenshöhe senken, oder beides zugleich bewirken.

1335 Eine ähnliche Einschätzung enthält das Standard-Datenschutzmodell der Datenschutzbehörden, *DSK* 2018, S. 32, das aber zusätzlich noch den sehr hohen Schutzbedarf kennt. Dazu auch *Bieker,* DuD 2018, S. 27, 31, der aus dem Eingriff in Art. 8 GRC allerdings lediglich den Schluss zieht, dass stets ein Risiko vorliegt, es also keine Verarbeitung ohne Risiko geben kann. Die Einstufung nimmt er abweichend zu dem Vorschlag hier in gering, normal und hoch vor.

1336 *Brüggemann,* in: Auernhammer 2020, Art. 25 DS-GVO, Rn. 18.

3.4.2.2.5.1 Typische Maßnahmen

Der Verordnungsgeber zählt hierzu in ErwG 78 DS-GVO einige Maßnahmen auf. Entsprechend der Schwerpunktsetzung im Wortlaut des Art. 25 Abs. 1 DS-GVO werden zunächst Maßnahmen zur Minimierung der Datenverarbeitung allgemein und insbesondere die frühestmögliche Pseudonymisierung erwähnt. 1142

Zu den gängigen, hier aber nicht eigens erwähnten Maßnahmen gehört aber auch die Implementierung von Löschroutinen, Verfallsterminen[1337] und dem Vier-Augen-Prinzip.[1338] Spezifisch auf den Personenbezug von Daten zielen die nachträgliche Anonymisierung oder gar Aggregation[1339] der Daten, ebenso wie die bereits anfängliche anonyme oder pseudonyme Datenverarbeitung. Werden bei letzterer mehrere zweckbezogene Pseudonyme verwendet, kann dies ähnlich der Datentrennung dazu eingesetzt werden, die Zweckbindung umzusetzen.[1340] Wo beides nicht möglich ist, wird der Einsatz sog. Sticky Policies empfohlen, durch die der Kontext der Datenerhebung und die sich daraus ableitenden Verarbeitungsrechte maschinenlesbar mit dem jeweiligen Datensatz verbunden werden.[1341] 1143

Die Grundlage für die Beurteilung, welche Maßnahme geeignet – und in dem Sinne dann auch notwendig – ist, bildet die eben beschriebene Risikobewertung. Ein hohes Risiko muss mit einer hochwirksamen Maßnahme beantwortet werden. Das allein sagt aber noch wenig über den Maßstab, anhand dessen diese Wirksamkeit bestimmt wird. Nach Art. 25 Abs. 1 DS-GVO soll hierfür auf den Stand der Technik zurückgegriffen werden. Abschließend ist dann noch eine Abwägung vorzunehmen, bei welcher dem Risiko die Implementierungskosten der Maßnahmen gegenübergestellt werden. 1144

1337 Ein solches Vorgehen wurde teilweise aus Art. 17 DS-GVO als zwingend abgeleitet. Eine derartige allgemeine Pflicht besteht jedoch nicht, *Hornung/Hofmann,* JZ 2013, S. 163, 166.

1338 *Körner* 2017, S. 65.

1339 *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 57.

1340 *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 58; *Margraf/Pfeiffer,* DuD 2015, S. 246, 248 f.

1341 *Dix,* in: Roßnagel 2003, Kapitel 3.5, S. 45 f.; *Hansen/Thiel,* DuD 2012, S. 26, 30; *Kühling,* Verw 2007, S. 153, 163.

3.4.2.2.5.2 Maßnahmen zur Transparenz

1145 Vergleichsweise breite Erwähnung findet in ErwG 78 DS-GVO auch das in Art. 5 Abs. 1 lit. a DS-GVO angesprochene Transparenzprinzip. Datenverarbeitungssysteme sollen gemäß ErwG 78 S. 3 DS-GVO transparent in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten gestaltet sein und der betroffenen Person ermöglichen die Verarbeitung zu überwachen. Diese Formulierung steht in Verbindung mit dem Transparenzgebot in Art. 5 Abs. 1 lit. a DS-GVO, geht aber zumindest über die Anforderungen hinsichtlich der Betroffenenrechte nach Art. 12 ff. DS-GVO, die diesen Grundsatz ausgestalten, hinaus.

1146 Die Informationspflichten nach Art. 13 und 14 DS-GVO sind so ausgestaltet, dass der betroffenen Person zum Zeitpunkt der Erhebung (Art. 13 Abs. 1 DS-GVO) bzw. spätestens innerhalb eines Monats (Art. 14 Abs. 3 lit. a DS-GVO) eine abstrakte Verfahrensbeschreibung vorgelegt werden muss. In ihr müssen u.a. die Zwecke, die Grundlage und die Dauer der Verarbeitung sowie – wenn die Daten nicht bei der betroffenen Person erhoben werden – die verarbeiteten Datenkategorien ausgeführt werden. Verlangt die betroffene Person Auskunft, müssen ihr gemäß Art. 15 Abs. 1 DS-GVO die konkreten personenbezogenen Daten sowie diese eher abstrakten Informationen mitgeteilt werden. Der Unterschied zu den Informationspflichten nach Art. 13 f. DS-GVO besteht aber nicht darin, dass die betroffene Person über den Zeitpunkt der Unterrichtung bestimmen kann. Ihr ist nach Art. 15 Abs. 3 DS-GVO auch eine Kopie jener personenbezogenen Daten zur Verfügung zu stellen, die Gegenstand der Verarbeitung sind. Statt lediglich Angaben über die Kategorien der Daten nach Art. 15 Abs. 1 lit. b DS-GVO sind folglich die konkret gespeicherten Daten selbst zu übermitteln.

1147 Die Formulierung in ErwG 78, die betroffene Person solle die Verarbeitung der Daten überwachen können, geht noch eine Stufe höher. Sie könnte so verstanden werden, dass die betroffene Person Einsicht in den tatsächlichen Verarbeitungsprozess nehmen können muss. Gerade persönliche Assistenzsysteme könnten hier ein Werkzeug sein, mit dem der betroffene Beschäftigte die relevanten Informationen einsehen könnte. Dies erinnert an die im Rahmen der Diskussion zum Ubiquitous Computing vorgeschlagenen Datenschutz-Assistenten, die gewissermaßen im Auftrag des Nutzers und nach seinen Präferenzen die Datenerhebung anderer Sys-

teme beeinflussen, Betroffenenrechte ausüben oder Pseudonyme wechseln können sollen.[1342]

Ein solch weitreichender Ansatz lässt sich allerdings kaum mit den beschriebenen Anforderungen übereinbringen, die durch die technischen und organisatorischen Maßnahmen lediglich umgesetzt und nicht erweitert werden sollen. Eine solch weitreichende Maßnahme ließe sich nur als Umsetzung des allgemeinen Transparenzgebots nach Art. 5 Abs. 1 lit. a DS-GVO konstruieren, wobei es dafür auch eines entsprechenden Risikos bedürfte. So dürfte dieser Passus als ein nur in Ausnahmefällen bindender Vorschlag zur idealen Umsetzung des Transparenzgebots nach Art. 5 Abs. 1 lit. a DS-GVO zu verstehen sein. 1148

3.4.2.2.5.3 Das Regelungskonzept der normativen Standards

Art. 25 Abs. 1 DS-GVO verlang vom Verantwortlichen, bei der Erfüllung seiner Pflicht den Stand der Technik zu berücksichtigen. Beim Stand der Technik handelt es sich um einen sog. normativen Standard, welchen der Verordnungsgeber verwendet, um die Dynamik der technischen Entwicklung in die Anforderungen der Datenschutz-Grundverordnung zu überführen. 1149

Dieses Regelungskonzept ist auch außerhalb des Datenschutzrechts, vor allem im Umwelt- und Technikrecht, üblich[1343] und wird insbesondere im technischen Arbeitsschutzrecht[1344] verwendet. Welche Maßnahme konkret gefordert ist, bestimmt sich hier wie dort nicht allein anhand des Stands der Technik – dieser ist eben nur zu berücksichtigen –, sondern Einbeziehung der zu begegnenden Gefährdung bzw. des Risikos und den Kosten für den Arbeitgeber. Insofern können gerade was den Grad der Verpflichtung des Arbeitgebers und die Abwägungsfestigkeit einzelner Ziele betrifft durchaus Parallelen gezogen werden. Das setzt allerdings voraus, dass die Regelungskonzepte des Datenschutzrechts und des Arbeitsschutzrechts insofern vergleichbar sind. 1150

1342 *Roßnagel* 2007b, S. 281 f.
1343 Z.B. auch Art. 14 Abs. 1 S. 2 und Art. 16 Abs. 1 S. 2 der NIS-Richtlinie RL 2016/1148/EU, Art. 11 lit. b der Industrieemissionenrichtlinie RL 2010/75/EU („beste verfügbare Techniken").
1344 Z.B. Art. 6 Abs. 2 lit. e der Arbeitsschutz-Rahmenrichtlinie 89/391/EWG.

3.4.2.2.5.3.1 Gemeinsamkeiten im Daten- und im Arbeitsschutzrecht

1151 Zunächst basieren sowohl das Daten- als auch das Arbeitsschutzrecht auf dem Präventionsgedanken. Das Datenschutzrecht zeichnet sich dadurch aus, dass es bereits weit im Vorfeld einer konkreten Beeinträchtigung eingreift, insofern also bereits abstrakte Gefahren reguliert. Anknüpfungspunkt ist das weitgehend nur potenziell gefährliche Verarbeiten von personenbezogenen Daten. Das Arbeitsschutzrecht setzt ebenfalls bereits im Vorfeld von Rechtsgutsverletzungen an, und will bereits bloße Gesundheitsgefährdungen – die erst über einen längeren Zeitraum zu einer spürbaren Gesundheitsbeeinträchtigung führen – möglichst vermeiden (siehe 2.3.2.4.2.1, S. 130). Der Anknüpfungspunkt ist z.B. im technischen Datenschutz die Verwendung von Arbeitsmitteln. Im Vergleich zu Datenverarbeitung ist hier der Gefahrenbezug zwar sichtbarer, im Grunde genommen aber ebenfalls abstrakt.

1152 Die zweite – insofern bedeutendere – Übereinstimmung betrifft das Regelungskonzept. Beide Rechtsgebiete enthalten nur wenige und dazu noch vergleichsweise abstrakte materielle Anforderungen. In der Datenschutz-Grundverordnung beschränken sie sich im Wesentlichen auf die Grundsätze in Art. 5 DS-GVO und die Erlaubnistatbestände in Art. 6 DS-GVO. Im Bereich des technischen Arbeitsschutzes sind dies die Schutzziele in § 2 Abs. 1 ArbSchG, § 3a ArbStättV und § 6 BetrSichV, die ihrerseits wieder in der Arbeitsschutz-Rahmenrichtlinie 89/391/EWG und den dazu erlassenen Einzelrichtlinien wurzeln. Danach sollen Gefährdungen für die Sicherheit und die Gesundheit der Beschäftigten, insbesondere durch Belastungen und Fehlbeanspruchungen möglichst vermieden oder geringgehalten werden.

1153 Die Maßstäbe, anhand derer beurteilt wird, ob die Schutzziele erreicht wurden, werden in normative Standards gefasst. So beurteilen sich nicht nur die Maßnahmen des technischen Datenschutzes nach Art. 25 Abs. 1 DS-GVO, sondern auch die Schutzmaßnahmen bei der Verwendung von Arbeitsmitteln nach § 4 Abs. 1 Nr. 2 BetrSichV nach dem Stand der Technik (siehe 2.3.2.4.2.1, S. 130). Dadurch werden die normativen Anforderungen an den technischen Fortschritt gekoppelt, ohne dass der Gesetzgeber die jeweiligen Regelungen fortwährend anpassen müsste.[1345]

1154 Allein aus Schutzzielen und normativen Standards lässt sich aber nicht ermitteln, welche Maßnahmen der Arbeitgeber bzw. der Verantwortliche zu

1345 Für das Arbeitsschutzrecht MHdB ArbR/*Kohte*, § 174, Rn. 14.

ergreifen hat. Zentral sind darum nicht die materiellen Anforderungen selbst, sondern das Verfahren, mit dem sie konkretisiert werden. Im Arbeitsschutzrecht werden die konkreten Anforderungen durch eine Gefährdungsbeurteilung ermittelt, die bspw. gemäß § 4 Abs. 2 Nr. 1 BetrSichV vor der Verwendung von Arbeitsmitteln zwingend vorgeschrieben ist. Im Datenschutzrecht ist immerhin bei einem hohen Risiko gemäß Art. 35 DS-GVO eine Datenschutz-Folgenabschätzung vorzunehmen. Im Übrigen sind in den Art. 13, 14 und 30 DS-GVO umfangreiche Informations- und Dokumentationspflichten niedergelegt.

Diese Gefährdungsbeurteilungen bzw. Folgenabschätzungen werden nicht etwa von den Aufsichtsbehörden durchgeführt, sondern sind – ggf. unter Beteiligung des Betriebsrats – von dem Arbeitgeber bzw. dem Verantwortlichen selbst durchzuführen. Die zwingende Beschäftigung mit dem Problem soll bei den Beteiligten ein Bewusstsein dafür erzeugen. Die Durchführung dieser Verfahren ist im Vergleich zu den materiellen Anforderungen detailliert geregelt. Sie muss dokumentiert und – wie Art. 5 Abs. 2 und 24 Abs. 1 DS-GVO für den Datenschutz ausdrücklich festschreibt – den Aufsichtsbehörden gegenüber nachgewiesen werden können.[1346] Dieses Regelungskonzept basiert auf der Annahme, dass ein ordentliches Verfahren auch zu einem interessengerechten Ergebnis führt. Anstatt also detaillierte materielle Anforderungen zu normieren, die ohnehin ständig angepasst werden müssten, wird das Verfahren dort geregelt. Das gewünschte und überdies stärker an den Besonderheiten des Einzelfalls angepasste Ergebnis entsteht dann gewissermaßen wie von selbst. 1155

3.4.2.2.5.3.2 Der Stand der Technik

Mit dem Stand der Technik werden vergleichsweise hohe Anforderungen verbunden. Die Formulierung nimmt allgemein Bezug auf den Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der die praktische Eignung einer Maßnahme gesichert erscheinen lässt,[1347] 1156

1346 Für das Arbeitsschutzrecht MHdB ArbR/*Kohte*, § 174, Rn. 92; für das Datenschutzrecht BeckOK DSR/*Schantz*, Art. 5 DS-GVO, Rn. 38.

1347 So z.B. die Legaldefinition in § 2 Abs. 10 BetrSichV; MHdB ArbR/*Kohte*, § 174, Rn. 27; *Wlotzke* 1999, S. 664. Im Kern entspricht dem auch die Legaldefinition in § 3 Abs. 6 S. 1 BImSchG.

ohne dass diese sich bereits entsprechend bewährt haben muss.[1348] Nach oben lassen sich die Anforderungen vom Stand der Wissenschaft und Technik abgrenzen, nach unten zu den anerkannten Regeln der Technik.

1157 Die anerkannten Regeln der Technik geben die herrschende Auffassung unter technischen Praktikern wieder,[1349] sind also solche, die einem nach neustem Erkenntnisstand ausgebildeten Fachmann bekannt sind, und sich aufgrund fortdauernder praktischer Erfahrung bewährt haben.[1350] Auf in dieser Weise etablierte Standards kann sich der Verantwortliche bei seinen technischen und organisatorischen Maßnahmen folglich nicht beschränken.[1351] Auf der anderen Seite ist aber auch keine Vorsorge gegen Schäden geboten, wie sie nach den neuesten wissenschaftlichen Erkenntnissen für erforderlich gehalten wird, ohne dass es auf die gegenwärtige praktische Machbarkeit ankäme. Das entspräche bereits dem Stand der Wissenschaft und Technik.[1352] Welche Standards dem jeweiligen Stand entsprechen, kann anhand der Reifegradmodelle der ENISA[1353] oder des BSI[1354] bestimmt werden.[1355]

3.4.2.2.5.4 Widerspruch zum allgemeinen Maßstab der Datenminimierung

1158 Der Verordnungsgeber hat mit dem Stand der Technik einen durchaus strengen Maßstab angelegt. Er übersteigt dasjenige, was grundsätzlich bei der Durchführung vieler Verträge geschuldet ist. Solange keine abweichende Vereinbarung getroffen wurde und sich aus den Umständen des Ver-

---

1348 BVerfG v. 8.8.1978 – 2 BvL 8/77, E 49, S. 89, 135 f. – *Kalkar I*. Zu demselben Begriff in Art. 32 DS-GVO *Bartels/Backer,* DuD 2018, S. 214, 215 f.; *Knopp,* DuD 2017, S. 663, 664 f.; a.A. *Nolte/Werkmeister,* in: Gola 2018, Art. 25 DS-GVO, Rn. 23; *Wedde,* in: Däubler et al. 2020, Art. 25 DS-GVO, Rn. 34, letzterer unter Verweis auf BT-Drucks. 16/13657, S. 23.

1349 BVerfG v. 8.8.1978 – 2 BvL 8/77, E 49, S. 89, 135 – *Kalkar I*.

1350 Zu der vergleichbaren Definition im Bauwesen BGH v. 7.7.2010 – VIII ZR 85/09, NJW 2010, S. 3088, Rn. 14.

1351 *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 38.

1352 BVerfG v. 8.8.1978 – 2 BvL 8/77, E 49, S. 89, 136 – *Kalkar I*.

1353 *ENISA* 2015.

1354 *BSI* 2016.

1355 *Brüggemann,* in: Auernhammer 2020, Art. 25 DS-GVO, Rn. 15; *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 39; kritisch in Bezug auf die Verfügbarkeit entsprechender Aussagen über den Reifegrad von Maßnahmen *Hansen,* in: Simitis et al. 2019, Art. 25 DS-GVO, Rn. 38.

trags auch nichts anderes ergibt, ist der Vertragspartner der betroffenen Person nämlich in der Regel nur verpflichtet, die üblichen, weithin anerkannten und erprobten Methoden anzuwenden (siehe 3.4.1.3.4.3, S. 386). Dieser Maßstab wird auch durch das allgemeine Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO nicht verschärft. Das Gegenteil ist der Fall: Der subjektiv übereinstimmende Maßstab der Parteien beeinflusst die Anforderungen der Datenminimierung, speziell den Maßstab der Angemessenheit. Es wäre demnach in der Regel auch angemessen, nur das weithin übliche zu tun.

Dem Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. b DS-GVO lässt sich folglich kein allgemeines Optimierungsgebot entnehmen (siehe 3.4.1.3.5, S. 388). Übersetzt in Technikregeln würde dies bedeuten, dass der Verantwortliche prinzipiell[1356] nach den anerkannten Regeln der Technik vorzugehen hat. Dies steht – was den Teilaspekt von Art. 25 Abs. 1 DS-GVO betrifft, ob die Verarbeitung personenbezogener Daten gestützt auf Technik überhaupt vermieden werden kann – offenkundig im Widerspruch mit der Vorgabe aus Art. 25 Abs. 1 DS-GVO, im Hinblick auf den technischen Datenschutz Maßnahmen nach dem Stand der Technik zu treffen. 1159

Um zu ermitteln, wie dieser Widerspruch aufzulösen und ggf. in eine Richtung zu entscheiden ist, müssen zwei Fragen beantwortet werden: Erstens im welchem Verhältnis der technische Datenschutz nach Art. 25 Abs. 1 DS-GVO zum Prinzip der Datenminimierung steht und zweitens, wie sich die Technikregeln in der Abwägung mit den Implementierungskosten verhalten. 1160

3.4.2.2.5.4.1 Technischer Datenschutz und Datenminimierung

Nach dem Wortlaut des Art. 25 Abs. 1 DS-GVO müssen die technischen und organisatorischen Maßnahmen darauf ausgelegt sein, die Datenschutzgrundsätze wie etwa die Datenminimierung wirksam umzusetzen. Dies deutet auf eine klare Hierarchie der Normen hin, in welcher der einzuhaltende Maßstab über die Datenminimierung abstrakt definiert und über 1161

1356 Dies kann von Branche zu Branche variieren. So wird im Automobilbau der Stand der Technik gefordert, *Eggert,* DS 2009, S. 247–253, handwerkliche Gewerke müssen dagegen den anerkannten Regeln der Technik entsprechen, BGH v. 7.3.2013 – VII ZR 134/12, NJW 2013, S. 1226–1227; *Pauly,* ZfBR 2018, S. 315–319.

technische und organisatorische Maßnahmen nur noch konkret umgesetzt wird. Nach diesem Verständnis hätte die technische Umsetzung keine Auswirkung darauf, welche Datenverarbeitung zur Erreichung des jeweiligen Zwecks erforderlich ist.

1162 Folglich stünden Maßnahmen im Vordergrund, durch welche die Anzahl der abgefragten und vorgehaltenen Daten oder die Zugriffe[1357] auf diese Daten auf das geplante Maß beschränkt blieben. In die erste Kategorie, also Maßnahmen zur Begrenzung der Menge der Daten, fielen z.B. Löschkonzepte oder eine nachträgliche zeitbezogene Aggregierung, die zwar den Personenbezug der Daten nicht entfallen ließe, aber deren Detailierungsgrad maßgeblich reduzierte, weil sie größere Zeiträume zusammenfasste. Zur zweiten Kategorie der Zugriffsbeschränkungen, zählte z.B. die Verschlüsselung von Daten oder der Einsatz von Rollenkonzepten, die beide den unberechtigten Zugriff auf die Daten durch externe bzw. interne Täter verhinderten. Nicht erfasst wären dagegen fortschrittliche technische Maßnahmen, mit denen etwa von vornherein auf die Verarbeitung personenbezogener Daten verzichtet werden könnte. Durch sie würde nämlich der Maßstab der Datenminimierung verändert, der sich dann nicht mehr daran bemäße, was unter Verwendung etablierter Methoden, sondern daran, was unter Verwendung fortschrittlicher Methoden erforderlich wäre.

1163 Gegen eine strikt am Wortlaut der Norm ausgerichtete Auslegung spricht dagegen der Sinn der Regelung. Hinter dem technischen Datenschutz steht die Diagnose, dass ein rein regelbasierter Datenschutz in seiner Durchsetzung keine hinreichende Gewähr für den Schutz der Rechte der betroffenen Person bietet.[1358] Angesichts immer zahlreicherer Möglichkeiten, personenbezogene Daten zu verarbeiten, müsse die Technik selbst reguliert werden, also nicht nur das Dürfen, sondern auch das Können.[1359]

1164 Bei diesem Grundansatz des technischen Datenschutzes geht es aber nicht nur darum, den Missbrauch neuer Verarbeitungsmöglichkeiten zu verhindern, indem man bestimmte problematische Aspekte sogleich wieder technisch einschränkt. Es ist auch anzuerkennen, dass mit neuen, weitergehenden Verarbeitungsmöglichkeiten ein berechtigtes Interesse des Verantwortlichen einhergehen kann, diese Möglichkeiten auch wahrzunehmen. Dies ist zwar kein Automatismus, dergestalt, dass stets getan wird, was ge-

---

1357 Das Prinzip der Datenminimierung bezieht sich nicht nur auf die Menge der Daten, sondern auch auf die Intensität der Verarbeitung, siehe 3.4.1.3.1, S. 374.

1358 *Jandt,* DuD 2017, S. 562.

1359 *Roßnagel, et al.* 2001, S. 36.

tan werden kann. Wenn sich aber handfeste Vorteile für den Verantwortlichen bieten – etwa, weil ihm die neue Technik erlaubt, wesentliche Effizienzgewinne zu realisieren oder neue Geschäftsmodelle zu verfolgen –, kann dies durchaus ein Mehr an Datenverarbeitung rechtfertigen.

Neue technische Möglichkeiten können also die Grenzen dessen verschieben, was an Datenverarbeitung zur Zweckerreichung erforderlich ist. Die technische Entwicklung darf aber nicht nur zulasten der betroffenen Person gehen; sie muss auch zu seinen Gunsten wirken. Wo technische Innovationen also dazu führen, dass für das Erreichen bestimmter Zwecke weniger Daten verarbeitet werden müssen, hat sich dies folglich auch auf den Grundsatz der Datenminimierung auszuwirken. 1165

Ihrem Sinn entsprechend stehen die Regelungen zur Datenminimierung in Art. 5 Abs. 1 lit. c DS-GVO und zum technischen Datenschutz in Art. 25 Abs. 1 DS-GVO folglich in Wechselwirkung zueinander. Das Prinzip der Datenminimierung bestimmt maßgeblich, welche technischen und organisatorischen Maßnahmen vom Verantwortlichen getroffen werden müssen. Umgekehrt richtet sich der Maßstab der Datenminimierung nach der technischen Realisierbarkeit, wofür in Art. 25 Abs. 1 DS-GVO der Stand der Technik als – vergleichsweise strenge – Richtschnur angelegt wird. 1166

3.4.2.2.5.4.2 Auswirkungen auf den Maßstab der Angemessenheit

Legt man ein Verhältnis zugrunde, in dem sich das Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO und der technische Datenschutz in Art. 25 Abs. 1 DS-GVO gegenseitig beeinflussen, kann die Anforderung, den Stand der Technik zu berücksichtigen, nicht folgenlos bleiben. Der Maßstab der Angemessenheit ist danach so zu verschärfen, dass es dem Verantwortlichen grundsätzlich zumutbar ist, innovative Maßnahmen entsprechend diesem Standard einzusetzen. Ihm bleibt es danach verwehrt, unter Berufung auf die jeweils geltenden Verkehrssitten lediglich etablierte Methoden einzusetzen. 1167

Dieser strenge Maßstab gilt jedoch nicht absolut, da nach Art. 25 Abs. 1 DS-GVO auch die Implementierungskosten einer Maßnahme zu berücksichtigen sind. Im Arbeitsschutzrecht (siehe 2.3.2.5, S. 139) bedeutet berücksichtigen in diesem Kontext, dass der Verantwortliche von bestimmten Vorgaben abweichen darf, wenn dies anderweitig gerechtfertigt ist. Diese Auslegung liegt auch im Datenschutzrecht nahe, zumal in Art. 25 Abs. 1 DS-GVO bereits die relevanten Kriterien für die Abwägung genannt 1168

sind.[1360] Bei zu hohen Implementierungskosten dürfte der Verantwortliche demnach u.U. Maßnahmen ergreifen, die lediglich den anerkannten Regeln der Technik entsprechen.

1169 Diese Abwägung mit den Implementierungskosten ist nicht zu verwechseln mit der Erforderlichkeitsprüfung i.e.S. Dort gilt, dass höhere Kosten die gleiche Eignung eines alternativen Mittels entfallen lassen. Dieser Prüfungspunkt besteht weiterhin und wird durch die Vorgaben zum technischen Datenschutz in Art. 25 Abs. 1 DS-GVO nicht beeinflusst. Verschärft wird lediglich der Maßstab der Angemessenheit, sodass es wahrscheinlicher ist, dass eine im engeren Sinne erforderliche Datenverarbeitung unangemessen und in der Folge unzulässig wird. Im Rahmen der Angemessenheitsprüfung sind die Implementierungskosten niedriger zu gewichten als bei der Prüfung der Erforderlichkeit i.e.S. Dies ergibt sich schon daraus, dass sie nur als ein Kriterium unter mehreren in Art. 25 Abs. 1 DS-GVO genannt werden. Nicht jeder Mehraufwand im Hinblick auf die Implementierung einer Maßnahme rechtfertigt es also, vom Stand der Technik abzuweichen.

3.4.2.2.5.5 Implementierungskosten

1170 Die Höhe dieser Erheblichkeitsschwelle für Implementierungskosten ist wieder eine Frage des Einzelfalls und lässt sich kaum abstrakt bestimmen. Aus der Zusammenschau mit dem anderen Hauptkriterium in Art. 25 Abs. 1 DS-GVO, dem Risiko für die Rechte und Freiheiten natürlicher Personen, lassen sich aber bestimmte Richtwerte festlegen. So ist davon auszugehen, dass die Anforderung hinsichtlich des Stands der Technik auf der einen und diejenigen hinsichtlich der Implementierungskosten auf der anderen Seite in einem ausgewogenen Verhältnis stehen. Kein Kriterium hat von vornherein dem anderen zu weichen.

1171 Fraglich ist nun, ab welchem Punkt das jeweilige Kriterium in seinem Geltungsanspruch betroffen ist, ab welcher Beeinträchtigung also davon auszugehen ist, dass es nicht berücksichtigt wurde oder werden konnte. Beim Stand der Technik wäre dies der Fall, wenn eine Maßnahme nicht mehr als fortschrittlich bezeichnet werden könnte. Dabei muss es sich nicht zwingend um die allerneuste Technik handeln; ein allzu weiter Abstand wird aber nicht gelassen werden dürfen. Da dieses Kriterium also vergleichswei-

1360 So ebenfalls zu Art. 32 DS-GVO *Bartels/Backer,* DuD 2018, S. 214, 216 ff.

se streng ist, bedarf es entsprechend hoher Implementierungskosten, um es auszuhebeln. Andernfalls liefe die Anforderung, den Stand der Technik zu berücksichtigen, praktisch leer.

3.4.2.2.5.5.1 Berücksichtigung der Leistungsfähigkeit

Neben der Frage nach der Höhe der Implementierungskosten stellt sich auch die Frage, wie diese zu bemessen sind. Einer Meinung zufolge soll dabei die wirtschaftliche Situation des Verantwortlichen herangezogen werden. Einem leistungsfähigeren Unternehmen seien höhere Implementierungskosten zuzumuten.[1361] Demgegenüber steht die Meinung, die zumutbaren Kosten objektiv anhand der bestehenden Risiken zu beurteilen.[1362] Dies deckt sich mit der zu dem Problemkreis vertretenen Meinung im Arbeitsschutzrecht (siehe 2.3.2.5.2, S. 140). 1172

Die beiden Herangehensweisen – die auf den Verantwortlichen bezogene und die objektive – können überlappen, weil wirtschaftlich leistungsfähigeren Unternehmen in der Regel mehr Verarbeitungsmöglichkeiten zur Verfügung stehen und sie insofern ein höheres Risiko erzeugen. Entscheidend ist dabei aber ausschließlich letzteres; die individuelle Leistungsfähigkeit ist lediglich ein Indiz für das Risiko. 1173

Gegen die Einbeziehung der wirtschaftlichen Leistungsfähigkeit spricht, dass diese auch sonst in der Datenschutz-Grundverordnung keine Rolle spielt. Wenn aber die umzusetzenden Anforderungen objektiv zu bestimmen sind, hat dies auch für deren technische Absicherung nach Art. 25 Abs. 1 DS-GVO zu gelten. Darüber hinaus entspricht es dem üblichen Regulierungsansatz, gewerbsmäßige im Unterschied zu gewerblicher Tätigkeit zu erfassen, weil der gewerbsmäßig Handelnde entsprechend der Dauer und Häufigkeit seiner Tätigkeit ein höheres Risiko erzeugt. Ob er mit der regulierten Tätigkeit Einkommen generiert und entsprechend leistungsfähig ist, spielt dagegen keine Rolle. Schließlich ist es dem wirtschaftlichen Risiko des Verantwortlichen zuzuordnen, wenn sich seine Strukturen und seine Betriebsgröße angesichts der durch ihn erzeugten Risiken 1174

1361 *Brüggemann*, in: Auernhammer 2020, Art. 25 DS-GVO, Rn. 16.

1362 Gegen die Berücksichtigung der Leistungsfähigkeit in Art. 25 Abs. 1 DS-GVO auch *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 46; *Varadinek, et al.* 2018, S. 81; *Wedde*, in: Däubler et al. 2020, Art. 25 DS-GVO, Rn. 37; noch zu § 3a BDSG 2003 *Scholz,* in: Simitis 2014, § 3a BDSG, Rn. 55.

und der daran geknüpften gesetzlichen Anforderungen als ineffizient erweisen.

1175 In dieses Bild passt auch, dass die Datenschutz-Grundverordnung nach Art. 2 Abs. 2 DS-GVO auf die Datenverarbeitung durch – u.U. auch sehr leistungsfähige – natürliche Personen keine Anwendung findet, wenn diese ausschließlich ihrer persönlichen oder familiären Tätigkeit nachgehen. Das Risiko für die Rechtsgüter der betroffenen Person ist hier wesentlich geringer. Dagegen fallen sämtliche Verarbeitungen außerhalb dieser Tätigkeiten in den Anwendungsbereich der Verordnung. Dies trifft auch sehr kleine, wenig leistungsfähige Verantwortliche.

3.4.2.2.5.5.2 Implementierungskosten oder laufende Kosten

1176 In Art. 25 Abs. 1 DS-GVO ist ausdrücklich von Implementierungskosten die Rede. Dem Wortlaut der Norm zufolge wäre also – anders als im Rahmen der Erforderlichkeitsprüfung nach Art. 5 Abs. 1 lit. c DS-GVO (siehe 3.4.1.3.3.2, S. 377) – nicht jeder Aufwand auf Seiten des Verantwortlichen berücksichtigungsfähig. Insbesondere die Betriebs- und Folgekosten blieben außen vor.[1363] Dagegen möchte eine Meinung das Kriterium der Implementierungskosten weit auslegen und plädiert dafür, sämtliche Kosten, also auch Betriebs- und Folgekosten miteinzubeziehen.[1364]

1177 Der letztgenannten Meinung ist zuzustimmen, schon deshalb, weil kein sachlicher Grund besteht, die verschiedenen Aufwände auf Seiten des Verantwortlichen unterschiedlich zu gewichten. Im Grunde genommen stellt sich das Problem aber erst deswegen, weil die Vertreter der ersten, die Folgekosten nicht berücksichtigenden Meinung den Begriff der Implementierung künstlich eng fassen. Als Synonyme zur Implementierung werden im Duden Begriffe wie der Einbau, die Einrichtung oder Installation genannt, also eher aufwändige Vorgänge, die am Beginn der technischen Umsetzung bestimmter Strukturen oder Prozessabläufe stehen. Das englische Wort „implementation“ kann aber auch schlicht mit Aus- oder Durchfüh-

---

1363 *Mantz*, in: Sydow 2018, Art. 25 DS-GVO, Rn. 45; *Martini*, in: Paal/Pauly 2018, Art. 25 DS-GVO, Rn. 41; *Wedde*, in: Däubler et al. 2020, Art. 25 DS-GVO, Rn. 36.

1364 *Brüggemann*, in: Auernhammer 2020, Art. 25 DS-GVO, Rn. 16; *Hartung*, in: Kühling/Buchner 2018, Art. 25 DS-GVO, Rn. 22; *Nolte/Werkmeister*, in: Gola 2018, Art. 25 DS-GVO, Rn. 24.

rung oder Vollzug übersetzt werden. So verstanden werden sämtliche Durchführungsschritte erfasst, auch Betriebs- oder Folgekosten.

Dieses Ergebnis wird auch durch einen Vergleich mit den Sprachfassungen der Datenschutzrichtlinie gestützt. In den Vorgaben zur Sicherheit der Datenverarbeitung in Art. 17 DSRL, die in erster Linie die Vorgängerin zu Art. 32 DS-GVO, mittelbar aber auch zu Art. 25 Abs. 1 DS-GVO darstellt, ist in der englischen Sprachversion von „the cost of their implementation" die Rede. In der deutschen Version der Richtlinie wurde das mit „der bei ihrer Durchführung entstehenden Kosten" übersetzt. Gemeint sind jeweils die Kosten der technischen und organisatorischen Maßnahmen zum Schutz gegen unrechtmäßige Verarbeitung. In Art. 25 Abs. 1 DS-GVO wird die Formulierung in der englischen Version nur unwesentlich geändert in „costs of implementation", in der deutschen Version der Verordnung wird dies nun aber nicht mehr in den sprechenden Begriff der Durchführung, sondern in den der Implementierung übersetzt. Gemeint war aber jedes Mal dasselbe: Die – d.h. alle – Kosten der Durchführung der Maßnahmen. Aus der von Art. 17 DSRL abweichende Formulierung in Art. 25 Abs. 1 DS-GVO kann kein inhaltliches Argument gezogen werden.[1365] 1178

3.4.2.2.5.6 Abwägung auf der Grundlage der Risikobewertung

Die Analyse hat gezeigt, dass die Implementierungskosten vergleichsweise hoch sein müssen, damit der Stand der Technik unterschritten werden darf. Dies wäre jedenfalls dann der Fall, wenn die Mehrkosten den Zweck der gesamten Datenverarbeitung in Zweifel zögen. Als Anhaltspunkt kann – entsprechend der objektiven Bestimmung der Implementierungskosten – der betriebswirtschaftliche Mehrwert der Datenverarbeitung dienen. Würde er durch die Mehrkosten der Implementierung einer datenschutzfreundlicheren Lösung aufgezehrt, könnte dies eine Abweichung vom (teuren) Stand der Technik rechtfertigen. 1179

Dieser Ansatz einer Kosten-Nutzen-Analyse basiert im Bereich der Datenverarbeitung zur Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO auf der Annahme, dass der Zweck einer Maßnahme einer durch die Parteien einvernehmlich geschaffenen Grundlage entspringt. Folglich werden auch die wirtschaftlichen Erwartungen, die der Verantwortliche 1180

1365 So aber *Martini,* in: Paal/Pauly 2018, Art. 25 DS-GVO, Rn. 41.

mit der Datenverarbeitung verbindet, grundsätzlich durch die betroffene Person akzeptiert. Anders ausgedrückt: Eine betroffene Person, die einen kostenlosen Dienst nutzt, muss sich im Klaren sein, dass die Marge dieses Dienstes entweder dünn und die verfügbaren Mittel für datenschutzfreundliche Technik entsprechend begrenzt sind oder aber die intensive Datenverarbeitung gerade Teil der Kommerzialisierungsstrategie des Anbieters ist.[1366] Das ist die logische Konsequenz seiner Entscheidung und damit Teil seiner Privatautonomie.[1367]

1181 Die vorgeschlagene Kosten-Nutzen-Analyse gerät dann an ihre Grenzen, wenn der Zweck der Maßnahme von einem Vertragspartner einseitig bestimmt wird – sei es bereits rechtlich in Fällen eines Leistungsbestimmungsrechts wie z.B. des Weisungsrechts, sei es in Fällen eines rein tatsächlichen Machtgefälles. Hier kann man sich nicht auf den Maßstab der Parteien verlassen, was als relevanter Nutzen eingestuft werden muss, dessen Gefährdung es rechtfertigen würde, den Schutzstandard des Art. 25 Abs. 1 DS-GVO zu senken. Überließe man dies dem Verantwortlichen, so würden tendenziell ineffiziente Strukturen bevorzugt, weil das Kosten-Nutzen-Verhältnis zwischen der Datenverarbeitung und der schützenden technischen Maßnahme hier vergleichsweise schnell kippen würde.

1182 Die Antwort hierauf ist in der Zweckkontrolle zu sehen, die je nach dem Rechtsgebiet, welches den der Datenverarbeitung zugrundeliegenden Lebenssachverhalt regelt, unterschiedlich bewirkt wird. Innerhalb der Datenschutz-Grundverordnung geschieht dies z.B. im Fall des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO über das Element des berechtigten Interesses. Im vertraglichen Bereich, also im Fall des Erlaubnistatbestands nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO, geschieht dies durch Instrumente wie die

---

1366 Die Beispiele Google und Facebook zeigen, dass Unternehmen auch mit dem Anbieten von kostenlosen Dienstleistungen hochprofitabel sein können. Insofern dürfte man in Sachen Datensicherheit nach Art. 32 DS-GVO sicherlich keine Konzessionen machen. Etwas anderes sind Maßnahmen, welche die Funktionalität der Dienste stören, zu deren integralen Bestandteilen es zählt, personalisierte Werbung auszuspielen. Es ist aus datenschutzrechtlicher Sicht nicht per se unzulässig, diese Dienstleistungen anzubieten. Der Hebel gegen solche Geschäftsmodelle liegt darum eher im AGB-Recht (KG v. 24.1.2014 – 5 U 42/12, ZD 2014, S. 412–421) oder im Kartellrecht (*BKartA* 2017; *BMWi* 2017; BGH v. 23.6.2020 – KVR 69/19, Z 226, S. 67–116 – *Facebook I*, siehe auch Fn. 1207, S. 388). Die beiden Beispiele dürften darum durch die Besonderheiten digitaler Plattformen geprägte Ausnahmen darstellen, die den hier beschriebenen simplen Grundsatz nicht in Frage stellen.

1367 Ähnlich *Grimm,* JZ 2013, S. 585, 588.

AGB-Kontrolle, den Verbraucherschutz oder – im hier besonders relevanten Beschäftigungsbereich – die Ausübungskontrolle des Weisungsrechts nach Art. 106 S. 1 GewO (siehe 3.4.1.4.6, S. 401). Zwecksetzungen, die hiernach zulässig sind, rechtfertigen die Annahme eines relevanten Nutzens, der durch kostspielige Maßnahmen des technischen Datenschutzes nur bei einem gesteigerten Risiko für die Rechte des Betroffenen zunichtegemacht werden darf.

3.4.2.2.6 Zwischenergebnis

Als Zwischenergebnis lässt sich folgende Grundkonstellation festhalten: 1183
Die Vorgaben in Art. 25 Abs. 1 DS-GVO hinsichtlich des Stands der Technik einerseits und hinsichtlich der Implementierungskosten andererseits, sind nicht ohne Weiteres in einen Konflikt zu führen, der unter Hinzuziehung weiterer Kriterien gelöst werden müsste. Dies ist nur dann der Fall, wenn die Implementierungskosten für eine Maßnahme, die dem Stand der Technik entspricht oder ihn nur unwesentlich unterbietet, derart hoch sind, dass sie die Wirtschaftlichkeit der Datenverarbeitung gefährdeten. Alle hierunter liegenden Kosten sind ohne Weiteres vom Verantwortlichen zu tragen.

Kommt es aber zum Konflikt, ist für die Frage, in welche Richtung das 1184
Pendel ausschwingt, die ebenfalls in Art. 25 Abs. 1 DS-GVO vorgesehene Risikobewertung heranzuziehen. Als hilfreich erweist sich dabei der Umstand, dass der Verordnungsgeber ausweislich des ErwG 76 ein digitales System der Risikostufen vorgesehen hat; die Datenverarbeitung kann nur ein (normales) Risiko oder ein hohes Risiko bergen. Bei einem normalen Risiko ist folglich zugunsten des Verantwortlichen zu entscheiden. Würde eine Maßnahme nach dem Stand der Technik die erwähnten hohen Implementierungskosten nach sich ziehen, darf er auch eine Maßnahme nach den anerkannten Regeln der Technik wählen. Liegt dagegen ein hohes Risiko vor, darf der in Art. 25 Abs. 1 DS-GVO vorgesehene Schutzstandard nicht unterschritten werden. Ein Verantwortlicher, der ein derartiges Risiko nicht wirksam kontrollieren kann, muss auf diese riskante Datenverarbeitung schlicht verzichten. Hier wäre also zugunsten der betroffenen Person zu entscheiden. Wie hoch sich das Risiko darstellt, ist im Rahmen der Risikobewertung zu ermitteln (3.4.2.2.4, S. 439).

3.4.2.2.7 Beispiele für die Abwägung

1185 Die erläuterten Abwägungsmaßstäbe lassen sich an zwei Beispielen deutlich machen. Da hierbei nicht auf alle Besonderheiten des Einzelfalls eingegangen werden kann, handelt es sich notwendigerweise um vereinfachte Einschätzungen. Sie können aber als Leitbilder für eine in der Praxis umfangreichere Abwägung herangezogen werden.

3.4.2.2.7.1 Versandhandel

1186 Das erste Beispiel betrifft den Versandhandel und die dort erwähnte datenschutzfreundliche Treuhänderlösung, die ermöglichen würde, dass ein Versendungskauf so anonym wie im stationären Handel abgewickelt werden könnte (siehe 3.4.1.4.8.2.2, S. 406). Der Verantwortliche müsste diese Maßnahme wohl schon allein deswegen nicht ergreifen, weil sie nicht dem Stand der Technik, sondern dem Stand der Wissenschaft und Technik entspräche.[1368] Sie könnte also selbst bei maßvollen Implementierungskosten nicht gefordert werden.

1187 Aber selbst, wenn sie den Kriterien des Stands der Technik entspräche, stünden dieser Lösung wahrscheinlich ihre Implementierungskosten entgegen. Die Risiken, die für die betroffene Person mit dem Erheben und dem Übermitteln der Absender- und Adressdaten an den Frachtführer verbunden sind, dürften als normal einzuschätzen sein. Der Verkäufer verfügt nicht notwendigerweise über Informationen zu der Person, die über die bestellte Ware, die Zahlungsart und seine Adresse hinausgehen. In der Regel wird er sich dadurch z.B. kein Bild über die Persönlichkeit der betroffenen Person machen oder andere tiefergehende Informationen über sie erhalten können. Insbesondere ist nicht ersichtlich, dass gerade die Verbindung der ersten drei Informationen mit der Adresse zu einer erheblichen Risikosteigerung führen würde. Schließlich ist auch nicht erkennbar, inwiefern hier eine der unter Gliederungspunkt 3.4.2.2.4.3, S. 441 beschriebenen riskanten Begehungsweisen oder Verarbeitungskontexte eine Rolle spielen könnte.

1368 Das unter dem Gliederungspunkt angesprochene System 3.4.1.4.8.2.2 (S. 406) findet sich nur in wissenschaftlichen Publikationen und ist – soweit erkennbar – nie in einem Massenverfahren eingesetzt worden.

Angesichts des lediglich normalen Risikos liegt der Fokus in diesem Fall auf den Implementierungskosten. Wenn sie die Marge des Versandhändlers erheblich belasten, wäre es ihm nicht zumutbar, diese über das übliche Maß hinausgehende Maßnahme zu ergreifen. Er dürfte dann nach Methoden vorgehen, die im Hinblick auf die Datenverarbeitung den anerkannten Regeln der Technik entsprechen. 1188

Etwas anderes gilt, wenn der Verkäufer bereits über sensible oder auch nur sehr viele Informationen über den Käufer verfügt, die ihm Einblick etwa in seine Vorlieben und aktuellen Lebensumstände gewähren. Das kann neben Verkäufern sozial auffälliger Ware wie etwa dem Erotikhandel z.B. bei "Vollsortimentern“ der Fall sein, die – selbst oder als Verkaufsplattform – nahezu alle Bedürfnisse ihres Kunden beantworten können und folglich mit vielen Aspekten seiner Persönlichkeit in Berührung kommen. Bei ersterem könnte es den Empfänger peinlich berühren, wenn der Paketbote oder der das Paket in Verwahrung nehmende Nachbar weiß, wo bestellt wurde. Bei letzterem könnte die Adresse für den Verkäufer eine Information sein, die das Risiko auf eine höhere Stufe springen lässt, etwa weil sie die Wahrscheinlichkeit erhöhen, dass die im Kundenprofil gespeicherten Daten diesen Kontext verlassen. 1189

3.4.2.2.7.2 Persönliches Assistenzsystem

Eine sehr genaue Aufstellung des betriebswirtschaftlichen Nutzens eines Assistenzsystems sowie der Implementierungskosten einer datenschutzfreundlichen Maßnahme findet sich im Beitrag von *Müller* (2014). Den Untersuchungsgegenstand bildet das System „AssiEff“, dass die Energieeffizienz der Fertigung in kleinen und mittleren Unternehmen steigern soll. Dazu wird überwacht, wie stark die einzelnen Komponenten eines Produktionssystems genutzt werden, und ob dies dem aktuellen Bedarf im Produktionsprozess entspricht. Der zuständige Maschinenbediener bekommt dann auf seinem Tablet die Empfehlung angezeigt, die Komponente auszuschalten. Die Grundlage hierfür bildet eine umfassende Verarbeitung von Maschinendaten, und – wenn auch vermutlich nicht im selben Umfang – von Beschäftigtendaten. 1190

3.4.2.2.7.2.1 Problematischer Verarbeitungskontext

1191 In seiner Grundkonfiguration erfasst das System den Benutzernamen, das Passwort, die Benutzerrolle und die Gerätenummer des Tablets. Der erste und letzte Parameter ist relevant, damit die Beschäftigten für eventuelle Bedienfehler und Beschädigungen verantwortlich gemacht und ggf. nachgeschult werden können. Das Kriterium der Benutzerrolle ist vor allem sicherheitsrelevant, weil es definiert, wie umfassend der Bediener Zugriff auf das System erhält.

1192 Das Assistenzsystem dient in erster Linie der besseren Organisation der Arbeit. Es befähigt den Arbeitgeber aber gleichzeitig, die Maschinenbediener im Hinblick auf ihr Arbeitsverhalten zu überwachen – etwa inwiefern sie den Empfehlungen gefolgt sind – und sie dahingehend zu vergleichen. Fraglich ist darum, welche Daten genau der Arbeitgeber hierfür verarbeiten darf und wie dies im Einzelnen technisch umgesetzt werden muss.

3.4.2.2.7.2.2 Denkbare technische und organisatorische Maßnahmen

1193 Als Maßnahme des technischen Datenschutzes wird die Verwendung von Anonymous Credentials[1369] diskutiert, also anonymen Berechtigungsnachweisen. Das Hauptmerkmal dieser Methode besteht darin, dass die Berechtigung des Nutzers überprüft werden kann, ohne dass dieser dazu seine Identität offenlegen muss. Auch kann er nicht über mehrere Anmeldevorgänge hinweg verfolgt werden. Dazu wird zwischen den Nutzern – also den Beschäftigten – und demjenigen, der dessen Berechtigung prüfen möchte – also den Arbeitgeber in seiner Funktion als Betreiber des Assistenzsystems – eine dritte Instanz geschaltet. Sie gibt die Berechtigungsnachweise aus. Die dafür notwendige Infrastruktur kann innerhalb oder außerhalb des Unternehmens betrieben werden.[1370]

1194 Der zweite, im Vergleich zum ersten eher organisatorische Ansatz gewährleistet dem Nutzer lediglich Pseudonymität, ermöglicht es also, seine Identität ggf. offenzulegen. Auch hier wird wieder eine dritte – im Sinne von außerhalb des Assistenzsystems liegend, nicht notwendigerweise unternehmensexterne – Instanz zwischengeschaltet, welche die Pseudonyme ausgibt und die Berechtigung für das System nach Anmeldung bestätigt.

1369 Hierzu näher die eingängige Beschreibung bei *Camenisch* 2014.
1370 *Müller* 2014, S. 181 f.

Beide Maßnahmen wurden grundsätzlich als funktional geeignet eingestuft.[1371] Ihre Implementierungskosten variieren aber erheblich. Die technische Lösung über die anonymen Berechtigungsnachweise benötigt eine Public-Key-Infrastruktur (PKI), deren jährliche Kosten mit etwa 120 € pro Mitarbeiter, in dem betrachteten Szenario für kleine Unternehmen mit 10 Bedienern also 1200 € angegeben werden. Demgegenüber steht bei den fünf Robotern des kleinen Unternehmens eine erwartete Stromersparnis von insgesamt 873,60 €. Die Infrastruktur kann zwar auch noch anderweitig eingesetzt werden, etwa für den sicheren Versand von E-Mails. Allein auf das Assistenzsystem betrachtet würden ihre Implementierungskosten aber dessen Zweck, Kosten zu sparen, nicht nur beseitigen, sondern sogar ins Gegenteil verkehren.[1372] 1195

Die organisatorische Lösung über die Verwendung von Pseudonymen benötigt lediglich einen zusätzlichen Server, auf dem die Pseudonyme getrennt vom eigentlichen Assistenzsystem verarbeitet werden können. Diesen zusätzlichen Server zu betreiben, bedarf zwar ebenfalls einigen Aufwands, weil er z.B. gegen unberechtigten Zugang geschützt werden muss. Im Gegensatz zur Public-Key-Infrastruktur erfordert es aber kein eigens darin geschultes IT-Personal, sondern kann auch von denjenigen Mitarbeitern aufgesetzt und gewartet werden, die auch sonst die Systeme des Unternehmens administrieren. Dafür kann diese Lösung die personenbezogenen Daten der Beschäftigten nicht in dem Maße schützen, wie dies über Anonymous Credentials der Fall wäre. Außerdem müssen die Beschäftigten der Pseudonymisierungsinstanz ein höheres Maß an Vertrauen entgegenbringen.[1373] 1196

3.4.2.2.7.2.3 Bewertung

Für die Bewertung der Maßnahmen im Hinblick auf die Anforderungen nach Art. 25 Abs. 1 DS-GVO wäre gemäß dem hier verfolgten Ansatz zunächst zu prüfen, ob sie dem Stand der Technik entsprechen. Dies ist eine technische Frage, die überdies einer starken Dynamik unterworfen ist, weswegen sie hier nicht beantwortet werden kann. Der Einfachheit halber soll angenommen werden, dass die erste Lösung über die Anonymous Credentials dem Stand der Technik entspricht. Für die zweite Lösung, die bloße 1197

1371 *Müller* 2014, S. 183 ff.
1372 *Müller* 2014, S. 184.
1373 *Müller* 2014, S. 185.

Pseudonymisierung, deuten die Ausführungen zu den Kosten darauf hin, dass sie lediglich den anerkannten Regeln der Technik genügt. Schließlich soll sie zum üblichen Fähigkeitskanon einer IT-Fachkraft gehören. Es erscheint aber auch nicht abwegig, die zweite Lösung ebenfalls dem Stand der Technik zuzuordnen; der Vollständigkeit halber sollen beide Möglichkeiten geprüft werden.

3.4.2.2.7.2.3.1 Anonymous Credentials

1198 Als erstes wären die Implementierungskosten im Verhältnis zum Nutzen der Datenverarbeitung zu ermitteln. Bei der Lösung über die Anonymous Credentials sind sie auf den ersten Blick erheblich und ziehen den Nutzen des gesamten Assistenzsystems und der damit verbundenen Datenverarbeitung in Zweifel. Dabei ist jedoch zu beachten, dass man die Kosten einer Public-Key-Infrastruktur nicht allein diesem Assistenzsystem aufbürden darf, sondern auch diejenigen Anwendungen miteinbezogen werden müssen, die ebenfalls von einer solchen Infrastruktur profitieren würden. Auch darf nicht einseitig auf die geringe Leistungsfähigkeit eines kleinen Unternehmens abgestellt werden, schließlich geht eine ineffiziente Betriebsgröße zu Lasten des verantwortlichen Arbeitgebers, nicht zu Lasten der Beschäftigten.

1199 Selbst bei Berücksichtigung dieser Faktoren dürfte das Kosten-Nutzen-Verhältnis der Lösung über die Anonymous Credentials aber negativ ausfallen. Die Analyse von *Müller* (2014) berücksichtigt lediglich die Kosten einer PKI-Infrastruktur, die der Stromersparnis von 873,60 € gegenübergestellt werden.[1374] Die Anschaffungskosten für das Assistenzsystem „AssiEff" bleiben unerwähnt. Das dürfte die oben erwähnten Effekte zu einem guten Teil wieder aufwiegen, schmälert es doch den Nutzen, den der Verantwortliche durch die Datenverarbeitung für sich verbuchen kann, und damit auch den Spielraum für datenschutzfreundliche Lösungen.

1200 Diese erheblichen Implementierungskosten würden an sich schon rechtfertigen, dass der verantwortliche Arbeitgeber einen weniger datenschutzfreundlichen Ansatz wählt. Ein hohes Risiko auf Seiten der betroffenen Beschäftigten würde dem jedoch entgegenstehen. Gemäß ErwG 75 der Verordnung wirkte es sich z.B. risikoerhöhend aus, wenn persönliche Aspekte bewertet würden. So wäre es denkbar, die Arbeitsleistung und Zuverlässig-

1374 *Müller* 2014, S. 184.

keit der Maschinenbediener in Bezug auf den Umgang mit dem Assistenzsystem zu ermitteln. Das allein kann die Annahme eines hohen Risikos aber nicht rechtfertigen. Der Arbeitgeber ist der Gläubiger dieser Leistungspflicht und darum grundsätzlich berechtigt, hierin Einsicht zu nehmen, etwa um Schulungsbedarf zu identifizieren.[1375]

Soweit der Arbeitgeber dies in sein Datenverarbeitungskonzept mit aufgenommen hat, könnte man bereits an der funktionalen Eignung der Anonymisierungslösung zweifeln, weil sie diese legitime Funktion unmöglich machen würde. Jedenfalls kann aber dann nicht von einem hohen Risiko gesprochen werden, wenn – z.B. in einer Betriebsvereinbarung – wirksam ausgeschlossen ist, dass die Daten aus dem Assistenzsystem für arbeitsrechtliche Maßnahmen wie Kündigungen herangezogen werden können.[1376] Bei einem dann lediglich normalen Risiko für die Beschäftigten wäre der Arbeitgeber gemäß Art. 25 Abs. 1 DS-GVO nicht verpflichtet, derart hohe Implementierungskosten in Kauf zu nehmen. Er müsste die Anonymisierungslösung folglich nicht einsetzen. 1201

3.4.2.2.7.2.3.2 Pseudonymisierung

Für die Pseudonymisierungslösung sind die Implementierungskosten in dem Beitrag von *Müller* (2014) nicht genau beziffert. Sie werden aber als deutlich niedriger als bei der Anonymisierungslösung angegeben. Insofern ist davon auszugehen, dass die Kosten nicht die kritische Schwelle erreichen, ab der es denkbar wäre, den Schutzstandard des Stands der Technik zu unterschreiten. Der Schutzstandard der anerkannten Regeln der Technik dürfte dann erst recht nicht unterschritten werden. Eine Risikoanalyse würde nämlich jedenfalls ergeben, dass ein normales Risiko vorliegt – immerhin werden in der Grundkonstellation personenbezogene Daten verarbeitet. Egal welchem Schutzstandard man die Pseudonymisierungslösung also zuordnete, der Verantwortliche müsste mindestens diese oder eine ähnlich gut schützende Maßnahme ergreifen. 1202

Ob die Pseudonymisierungslösung nicht nur erforderlich, sondern auch hinreichend wäre, ist wiederum in Abhängigkeit zu ihrer Zuordnung zu einem Schutzstandard zu beantworten. Betrachtete man sie als dem Stand 1203

1375 BAG v. 17.11.2016 – 2 AZR 730/15, NZA 2017, S. 394, 397.

1376 Auf diese Kriterien wird unter Gliederungspunkt 3.6.1.2.3.1, S. 508 noch vertieft eingegangen.

der Technik entsprechend, würde der Verantwortliche mit ihrem Einsatz wohl auch ohne flankierende Schutzmaßnahmen den Anforderungen in Art. 25 Abs. 1 DS-GVO gerecht. Denn auch im Fall eines hohen Risikos können keine über den Stand der Technik hinausgehenden Maßnahmen gefordert werden. Hier bedürfte es aber einer genaueren Bewertung, schließlich kann auch zwischen Maßnahmen, die dem Stand der Technik entsprechen, noch hinsichtlich ihrer Wirksamkeit differenziert werden.

1204 Betrachtete man die Pseudonymisierungslösung schließlich als lediglich den anerkannten Regeln der Technik entsprechend, würde sie den Anforderungen in Art. 25 Abs. 1 DS-GVO nur entsprechen, wenn das Risiko mit flankierenden Maßnahmen – etwa der oben erwähnten Betriebsvereinbarung – auf ein normales Maß begrenzt bliebe. Geht man von diesem normalen Risiko aus und wären auch alle anderen geeigneten und dem Stand der Technik entsprechenden Maßnahmen so kostspielig, wie die Lösung über die Anonymous Credentials, könnte im Ergebnis auch gegen die vorgestellte Pseudonymisierungslösung nichts eingewendet werden.

3.4.2.2.8 Durchsetzung

1205 Die Regelungen zum technischen Datenschutz wirken sich auf die Prüfung der Rechtmäßigkeit der Datenverarbeitung aus (siehe 3.4.2.2.5.4.2, S. 453). Sie statuieren darüber hinaus aber auch eigenständige Rechtspflichten für den Verantwortlichen, die sowohl durch die Aufsichtsbehörden als auch die betroffene Person durchgesetzt werden können.

3.4.2.2.8.1 Aufsichtsbehördliches Handeln

1206 Verstöße gegen die Vorgaben zum Datenschutz durch Technik werden gemäß Art. 83 Abs. 4 lit. a DS-GVO mit einer Geldbuße von bis zu 10.000 € oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs sanktioniert, je nachdem, welcher der Beträge höher ist. Darin unterscheidet sich Art. 25 Abs. 1 DS-GVO von den bisherigen Regelungen in §§ 3a und 9 BDSG 2003, die beide nicht bußgeldbewehrt waren.

1207 Neben oder statt der Verhängung von Bußgeldern können Aufsichtsbehörden auch Anordnungen nach Art. 58 Abs. 2 lit. d DS-GVO treffen, den Verarbeitungsvorgang in Einklang mit der Datenschutz-Grundverordnung

zu bringen. Derartige Anordnungen waren zumindest für die Vorgaben in § 9 BDSG 2003 gemäß § 38 Abs. 5 BDSG 2003 auch bisher möglich.[1377]

Sämtliches aufsichtsbehördliche Handeln wird dabei von der Rechenschaftspflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO unterstützt. Danach muss der Verantwortliche nachweisen können, dass er die Datenschutzgrundsätze nach Art. 5 Abs. 1 DS-GVO einhält. Dies legt den Verantwortlichen beim Verfahren über eine behördliche Anordnung oder ein Bußgeld die Beweislast auf. Auf einen konkreten Schadensfall[1378] kommt es für das beschriebene behördliche Handeln ohnehin nicht an, schon, weil er kein Tatbestandsmerkmal von Art. 83 Abs. 4 lit. a DS-GVO ist. 1208

Die Verordnung geht in Art. 25 Abs. 3 DS-GVO augenscheinlich davon aus, dass sich die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO auch auf die Einhaltung der Vorgaben des technischen Datenschutzes bezieht. Dieser sieht nämlich vor, dass ein genehmigtes Zertifizierungsverfahren nach Art. 42 DS-GVO als Faktor herangezogen werden kann, um die Erfüllung der Vorgaben in Art. 25 Abs. 1 DS-GVO nachzuweisen. Entsprechend wird die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO auch auf die Einhaltung der Art. 25 Abs. 1 und 2 DS-GVO bezogen.[1379] 1209

Eine solche Nachweispflicht ist zwar folgerichtig, da die technische und organisatorische Absicherung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DS-GVO in Art. 25 Abs. 1 DS-GVO eigens betont wird.[1380] Eine ausdrückliche Ausweitung des Anwendungsbereichs des Art. 5 Abs. 2 DS-GVO findet sich in der Verordnung aber nicht. Sie ergibt sich auch nicht aus der Konkretisierung der Rechenschaftspflicht durch Art. 24 Abs. 1 DS-GVO,[1381] demzufolge der Verantwortliche u.a. technische Maßnahmen ergreifen muss, um den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Der Nachweis der Einhaltung der Grundsätze soll mit technischen Mitteln geführt werden und nicht umgekehrt der Einsatz technischer Mittel nachweispflichtig sein. Insofern kann die Erweiterung der Nachweispflicht nur aus Art. 25 Abs. 3 DS-GVO geschlossen werden. 1210

1377 BeckOK DSR/*Karg*, § 9 BDSG, Rn. 116.
1378 *Mantz*, in: Sydow 2018, Art. 25 DS-GVO, Rn. 70 begründet dies mit der Rechenschaftspflicht. Für den Schaden spielt sie aber keine Rolle.
1379 *Hartung*, in: Kühling/Buchner 2018, Art. 25 DS-GVO, Rn. 30; *Mantz*, in: Sydow 2018, Art. 25 DS-GVO, Rn. 70.
1380 So wohl auch *Hansen*, in: Simitis et al. 2019, Art. 25 DS-GVO, Rn. 30.
1381 *Roßnagel*, in: Simitis et al. 2019, Art. 5 DS-GVO, Rn. 176.

3.4.2.2.8.2 Durchsetzung durch den Betroffenen und den Markt

1211 Auf individueller Ebene kann die betroffene Person gemäß Art. 82 Abs. 1 DS-GVO Ersatz des materiellen oder immateriellen Schadens verlangen, der wegen eines Verstoßes gegen die Datenschutz-Grundverordnung entstanden ist. Die Nichteinhaltung der Vorgaben nach Art. 25 Abs. 1 DS-GVO ist dabei – wie jede Vorgabe der Datenschutz-Grundverordnung – der eigentliche Haftungsgrund. Soweit die übrigen Voraussetzungen von Art. 82 Abs. 1 DS-GVO vorliegen spielt es also keine Rolle, ob ein Verstoß gegen Art. 25 Abs. 1 DS-GVO dazu führt, dass die Datenverarbeitung im konkreten Fall rechtswidrig[1382] wird, also nicht mehr auf einen Erlaubnistatbestand nach Art. 6 DS-GVO gestützt werden kann.

1212 Der Datenschutz durch Technik wird schließlich auch mit einem marktförmigen Ansatz zur Durchsetzung verbunden. Dies geht aus dem Einsatz von Zertifizierungsverfahren hervor. Verantwortlichen, die sich die Rechtskonformität ihrer Technikgestaltung[1383] bescheinigen lassen, wird es zum einen leichter fallen, ihre Nichtverantwortlichkeit für einen eventuellen Schaden nach Art. 82 Abs. 3 DS-GVO nachzuweisen. In Hinblick auf die Verhängung aufsichtsbehördlicher Sanktionen ist ein vergleichbarer positiver Effekt der Zertifizierungsverfahren sogar in Art. 83 Abs. 2 S. 1 lit. j DS-GVO ausdrücklich vorgesehen.

1213 Der Vorschlag des Parlaments, öffentliche Aufträge an die Einhaltung der Prinzipien des Datenschutzes durch Technik zu knüpfen, hat dagegen keinen Niederschlag im Verordnungstext gefunden.[1384] Nach ErwG 78 sollen sie aber immerhin berücksichtigt werden.

3.4.2.3 Zweckkontrolle und Datensparsamkeit in der DS-GVO

1214 Das Prinzip der Datensparsamkeit wird in der DS-GVO nicht eigens angesprochen. Soweit § 3a BDSG den Ansatz verfolgte, datenschutzrechtliche Anforderungen durch die Gestaltung von Technik umzusetzen, wird dies

---

1382 Gegen einen solchen Automatismus *Nolte/Werkmeister,* in: Gola 2018, Art. 25 DS-GVO, Rn. 3.

1383 Zum haftungsmindernden Effekt einer Technikgestaltung, die den Anforderungen in Art. 25 Abs. 1 DS-GVO gerecht wird, allgemein *Brüggemann,* in: Auernhammer 2020, Art. 25 DS-GVO, Rn. 2.

1384 *Mantz,* in: Sydow 2018, Art. 25 DS-GVO, Rn. 81. Auf Ebene der Länder wird dies hingegen vereinzelt berücksichtigt, *Hornung/Hartl,* ZD 2014, S. 219, 221.

in Art. 25 Abs. 1 DS-GVO aufgegriffen.[1385] Dabei zeigt sich auch durchaus ein dynamisches, in gewisser Weise auf datenschutzfreundliche Optimierung der Systeme ausgerichtetes Element. Das Zusammenspiel zwischen den Vorgaben zum technischen Datenschutz nach Art. 25 Abs. 1 DS-GVO und dem dadurch umzusetzenden Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO ist so zu interpretieren, dass der Verantwortliche Verfahren einsetzen muss, die im Hinblick auf die Beschränkung der Datenverarbeitung auf das notwendige Maß als fortschrittlich angesehen werden.

Dagegen gibt es in der Datenschutz-Grundverordnung selbst keine Norm, der eine Differenzierung zwischen den Anforderungen an den Zweck (Datensparsamkeit) und den Anforderungen anhand des Zwecks (Erforderlichkeitsprinzip) entnommen werden könnte. Dass dies kein Versehen ist, erkennt man nicht zuletzt an der Konzeption der Zertifizierung in Art. 42 DS-GVO. Eine Zweckkontrolle ließe sich aber u.U. durch Vorgaben außerhalb der Datenschutz-Grundverordnung gewährleisten. 1215

3.4.2.3.1 Eingeschränkter Zertifizierungsmaßstab

Die Tatsache, dass das Prinzip der Datensparsamkeit in der Datenschutz-Grundverordnung – wie auch in der Datenschutzrichtlinie – nicht enthalten ist, lässt sich auch anhand der Wirkweise der Zertifizierung in Art. 42 DS-GVO belegen. Das Zertifizierungsverfahren soll gemäß Art. 42 Abs. 1 S. 1 DS-GVO dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Eine Übererfüllung der Anforderungen – etwa dergestalt, dass die anonyme Nutzung ermöglicht wird, wo üblicherweise der Name des Nutzers erhoben wird – findet im Zertifizierungsprozess keinen Niederschlag[1386] und kann auch folglich von der betroffenen Person nicht sicher erkannt werden. 1216

Dies ist insofern problematisch, als der Zweck zumindest im Rahmen der Verarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 S. 1 DS-GVO maßgeblich davon abhängt, was der Verantwortliche an Verfahren anbietet. Listet ein Versandhändler keine Möglichkeiten zum anony- 1217

1385 *Gierschmann*, ZD 2016, S. 51, 53; *Kort*, DB 2016, S. 711.

1386 *Bergt*, in: Kühling/Buchner 2018, Art. 42 DS-GVO, Rn. 15; *Scholz*, in: Simitis et al. 2019, § 42 DS-GVO, Rn. 25. Noch zum Entwurf *Hartl* 2017, S. 224.

men Bezahlen auf, kann der Zweck auch nicht dahingehend festgelegt werden. Der Kunde kann nur ein datenintensiveres Verfahren wählen, auf das sich dann der Zweck konkretisiert (siehe 3.4.1.4.8.1, S. 404). Diese Zweckfestlegung bestimmt wiederum maßgeblich über die Anforderungen der Datenminimierung nach Art. 5 Abs. 1 lit. b DS-GVO, sodass es letztlich auf diesem Feld zu keinem Fortschritt kommt. Eine Optimierung des Datenschutzes durch Marktanreize, kann so nicht stattfinden.

3.4.2.3.2 Eingeschränkte Zweckkontrolle durch die AGB-Kontrolle

1218 Wie bereits oben ausgeführt (3.4.1.3.4.2.1, S. 381), wird der Zweck für die Datenverarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO in der Regel einvernehmlich durch die Vertragsparteien gesetzt, die sich dabei auf Augenhöhe gegenüberstehen. Wo dies unter tatsächlichen oder – im Falle eines Leistungsbestimmungsrechts – aus rechtlichen Gesichtspunkten nicht zutrifft, greifen verschiedene Schutzinstrumente.

1219 Im Rechtsverkehr mit Verbrauchern, zu denen auch Arbeitnehmer gehören, ist dies zum einen die AGB-Kontrolle, über die auf den Vertragsinhalt eingewirkt werden kann. Die Zweckkontrolle über dieses Instrument wirkt aber nur sehr eingeschränkt, da sie insbesondere das Prinzip der Datenminimierung nicht erfasst (siehe 3.4.1.4.4.1, S. 397).

3.4.2.3.3 Zweckkontrolle durch die menschengerechte Gestaltung der Arbeit

1220 Eine gewisse Zweckkontrolle könnte sich allerdings aus dem Prinzip der persönlichkeitsfördernden menschengerechten Gestaltung der Arbeit ableiten lassen. Neben der Förderung der Fähigkeiten und der sozialen Interaktion der Mitarbeiter geht es bei diesem Gestaltungsansatz auch darum, die Handlungsautonomie und Eigenverantwortlichkeit der betroffenen Beschäftigten zu stärken. Überschneidungen zum Datenschutzrecht zeigen sich bspw. in der Gestaltung der konkreten Tätigkeit. Gerade stark fragmentierte, d.h. in kleine Einzelaufgaben zerlegte Arbeit bietet viele Ansatzpunkte für die Kontrolle der Beschäftigten. Gleichzeitig widerspräche eine solche Arbeit dem Prinzip der menschengerechten Gestaltung, weil den

Beschäftigten keine möglichst vollständigen und problemhaltigen Aufgaben zugewiesen würden (siehe 2.3.5.2.3.2, S. 172).[1387]

Solange der Zweck dieses Arbeitssystems aber zulässigerweise auf eine solche Funktionalität konkretisiert werden dürfte, bliebe das Prinzip der Datenminimierung in einem solchen Fall wirkungslos. Ein Ansatz könnte hier darin bestehen, die Zwecksetzung selbst (dazu näher 3.6.1.2.1, S. 491) am Prinzip der menschengerechten Gestaltung der Arbeit zu messen. Dabei muss jedoch die unterschiedlich ausgeprägte Abwägungsfestigkeit dieses Prinzips beachtet werden (siehe 2.3.6.3, S. 179). Gerade im für das Datenschutzrecht besonders relevanten Bereich der Persönlichkeitsförderung reduzieren sich die Anforderungen an den Arbeitgeber außerhalb der – ohnehin nur in extremen Fallgestaltungen eingreifenden – Mitbestimmung nach §§ 90 f. BetrVG jedoch auf ein Willkürverbot, das nur in Randbereichen greift (siehe 3.6.2.5.2.1, S. 572). Eine strengere Zweckkontrolle würde hier nur greifen, wenn die Arbeitsgestaltung die Grenze zur psychischen Gesundheitsgefährdung überschreitet. 1221

3.5 Verfassungsrechtliche Vorgaben

Die europarechtlichen Regelungen zum Datenschutzrecht ändern im Grundsatz nichts an der zumindest mittelbaren Bindung (siehe 2.2.1, S. 77) der Beteiligten an die Grundrechte des Grundgesetzes. Das europäische Recht beeinträchtigt nicht die Geltung, sondern nur die Anwendung des deutschen Rechts (siehe 3.2.2.1.1, S. 262). Die Analyse der anwendbaren Grundrechte hat zudem gezeigt, dass die Grundrechte des Grundgesetzes nicht vollständig durch die Datenschutz-Grundverordnung und die Grundrechte der Europäischen Union verdrängt werden (siehe 3.2.2.6, S. 283). 1222

Daraus folgt, dass an die für diese Arbeit relevante Verarbeitung von personenbezogenen Beschäftigtendaten durchaus auch verfassungsrechtliche Anforderungen zu stellen sind. Die praktischen Konsequenzen sind aber – um dies vorwegzunehmen – eher als gering einzuschätzen. 1223

1387 *Kuhlmann/Schumann* 2015, S. 130 f.

3.5.1 Der verbleibende Raum für verfassungsrechtliche Anforderungen

1224 Bevor genauere verfassungsrechtliche Anforderungen formuliert werden können, muss jedoch zunächst der Raum bestimmt werden, der hierfür angesichts des breiten Anwendungsvorrangs der Datenschutz-Grundverordnung und damit einhergehend der EU-Grundrechte noch besteht. Hierzu müssen zwei Konstellationen unterschieden werden.

3.5.1.1 Bereiche außerhalb des Anwendungsbereichs der DS-GVO

1225 Die erste Konstellation betrifft Bereiche, die von der Datenschutz-Grundverordnung schlicht nicht geregelt werden. Hier kann das europäische Recht von vornherein keinen Anwendungsvorrang beanspruchen. Es gelten auch keine EU-Grundrechte, weil kein Unionsrecht nach Art. 51 Abs. 1 S. 1 GRC durchgeführt wird (siehe 3.2.2.1.2, S. 263). Die Anwendung der deutschen Grundrechte steht unter keiner Bedingung.

1226 Am augenfälligsten ist dieser Effekt dort, wo der Schutzbereich eines deutschen Grundrechts über den Anwendungsbereich der Datenschutz-Grundverordnung hinausgeht. So muss das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG aufgrund seiner mittelbaren Drittwirkung auch von privaten Akteuren beachtet werden, die nicht automatisiert und nicht dateisystembezogen personenbezogene Daten verarbeiten (siehe 3.5.3.2, S. 477). Gleiches gilt für das korrespondierende Grundrecht des für die Datenverarbeitung verantwortlichen Grundrechtsträgers. Die Datenschutz-Grundverordnung findet dagegen nach Art. 2 Abs. 1 DS-GVO nur auf automatisierte oder dateisystembezogene Verarbeitung Anwendung. Der deutsche Gesetzgeber hat dieser Diskrepanz für den Beschäftigungskontext in § 26 Abs. 7 BDSG 2018 (siehe 3.1.6, S. 255) Rechnung getragen.

1227 Der zweite Bereich im Datenschutzrecht, bei dem dieser Effekt zum Tragen kommt, ist die Legitimität der Zweckbestimmung. Bei der Zweckfestlegung sind zwar auch europarechtliche Anforderungen an die Bestimmtheit des Zwecks zu beachten. An die Legitimität des Zwecks formuliert die Datenschutz-Grundverordnung aber keine Anforderungen (siehe 3.4.1.2.1.2, S. 357). Hier sind die Maßstäbe der deutschen Grundrechte anzulegen. Dies gilt vor allem im Hinblick auf diejenige Verarbeitung von Beschäftigtendaten, die zur Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO vorgenommen wird. Die arbeitsrechtlichen Pflichten sind nach den Wertungen des jeweiligen nationalen Arbeitsrechts zu bestim-

men, also auch unter Beachtung der entsprechenden verfassungsrechtlichen Vorgaben (siehe 3.2.2.5.2, S. 281).

3.5.1.2 Bereiche innerhalb der Öffnungsklausel in Art. 88 DS-GVO

Die zweite Konstellation, in der deutsche Grundrechte zur Anwendung kommen, betrifft die Öffnungsklausel in Art. 88 DS-GVO, der zufolge durch Gesetz oder Kollektivvereinbarung spezifische Regelungen für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext erlassen werden dürfen. Das europäische Recht enthält durchaus Regelungen für den Beschäftigtendatenschutz (siehe 3.1.2, S. 241), hält sich aber zurück, falls und soweit die Öffnungsklausel zulässigerweise genutzt wird. Inwieweit verfassungsrechtliche Anforderungen zum Tragen kommen können, hängt folglich von der Reichweite der Öffnungsklausel in Art. 88 DS-GVO (siehe 3.1.3, S. 242) ab. 1228

Zunächst gilt es zu beachten, dass die Grundrechte des Grundgesetzes allein keine spezifischen Vorschriften im Sinne von Art. 88 Abs. 1 DS-GVO sein können. Die spezifischen Regelungen müssen in der mitgliedstaatlichen oder kollektivvertraglichen Rechtsvorschrift selbst getroffen werden (vgl. zu § 26 Abs. 1 S. 1 BDSG 2018, 3.1.5.2, S. 248). Die besonderen Anforderungen, die in Art. 88 Abs. 1 und 2 DS-GVO an die Umsetzungsnorm gestellt werden, sind für die grundrechtliche Diskussion folglich ohne Belang. Insbesondere spielt es keine Rolle, ob die deutschen Grundrechte genauere Anforderungen an die Verarbeitung von Beschäftigtendaten als das europäische Recht enthalten. 1229

Dagegen kommt den allgemeinen Anforderungen der Öffnungsklausel in Art. 88 DS-GVO – also der Frage, ob die Verordnung im Beschäftigtendatenschutz voll- oder mindestharmonisierend wirkt (siehe 3.1.3.1, S. 243) – auch im grundrechtlichen Diskurs Bedeutung zu. Diejenigen, die eine spezifische Regelung nach Art. 88 Abs. 1 DS-GVO erlassen dürfen, verfügen hinsichtlich der richtlinienartig formulierten Datenschutzgrundsätze in Art. 5 Abs. 1 DS-GVO lediglich über eine Konkretisierungs-, aber keine Abweichungsbefugnis. In der Folge können auch den deutschen Grundrechten diesbezüglich nur konkretere, aber keine anderen Anforderungen entnommen werden. Diese Möglichkeit zur Abweichung nach oben oder unten besteht lediglich hinsichtlich der verordnungstypisch detailliert geregelten Anforderungen, wie etwa denen zur Transparenz. 1230

3.5.2 Für die grundrechtlichen Vorgaben relevante Bereiche

1231 Von der Frage des rechtlichen Spielraums, den das europäische Recht für verfassungsrechtliche Vorgaben lässt, ist die Frage zu unterscheiden, wo welche deutschen Grundrechte für das Thema dieser Arbeit eine Rolle spielen können.

1232 In jenen Bereichen, in denen die Öffnungsklausel in Art. 88 DS-GVO zulässigerweise genutzt wurde oder noch zulässigerweise genutzt werden kann, finden die deutschen Grundrechte für die gesamte datenschutzrechtliche Prüfung Anwendung. Diese Bereiche sind die Einwilligung nach § 26 Abs. 2 BDSG 2018 und die – im Beschäftigungsverhältnis deutlich relevanteren[1388] – Kollektivvereinbarungen nach § 26 Abs. 4 BDSG 2018. In den aufgezeigten Grenzen kommen die Berufsfreiheit nach Art. 12 Abs. 1 GG von Arbeitgeber und Arbeitnehmer sowie das Recht der Arbeitnehmer auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zum Tragen.

1233 Von den Bereichen außerhalb der Öffnungsklausel ist für diese Arbeit allein die Zwecksetzung relevant. Die Festlegung ist im Arbeitsverhältnis vor allem anhand der konkurrierenden Berufsfreiheiten nach Art. 12 Abs. 1 GG von Arbeitgeber und Arbeitnehmer vorzunehmen. Die nicht automatisierte und nicht dateisystembezogene Datenverarbeitung nach § 26 Abs. 7 BDSG 2018 ist dagegen für die Spezifika der Datenverarbeitung in der Industrie 4.0 ohne Bewandtnis, sodass auch die hier geltenden verfassungsrechtlichen Anforderungen keiner eingehenden Erörterung bedürfen.

1234 Für die verfassungsrechtlichen Fragen im Zusammenhang mit der Berufsfreiheit, insbesondere deren Schutzgewährleistung und Wirkung im Arbeitsverhältnis kann auf die Ausführungen unter Gliederungspunkt 2.2 (S. 76) verwiesen werden. Einer eingehenden Erörterung bedarf darum nur das Recht der Beschäftigten auf informationelle Selbstbestimmung.

3.5.3 Das Recht auf informationelle Selbstbestimmung der Beschäftigten

1235 Die grundrechtlichen Anforderungen an die Verarbeitung von Beschäftigtendaten sind in erster Linie anhand des Rechts der Beschäftigten auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

1388 Zur sehr eingeschränkten Bedeutung der Einwilligung im Beschäftigtendatenschutz siehe 3.6.1.5, S. 523.

zu ermitteln. Dieses Recht ist im Grundgesetz anders als das Recht auf Schutz personenbezogener Daten in der EU-Grundrechtecharta nicht ausdrücklich normiert. Es ist aber mittlerweile als Ausprägung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG in der ständigen Rechtsprechung des Bundesverfassungsgerichts anerkannt.[1389]

Die wichtigste Quelle für das Verständnis des Rechts auf informationelle Selbstbestimmung stellt das in seinen Grundaussagen ungebrochen aktuelle Volkszählungsurteil[1390] des Bundesverfassungsgerichts dar, das auch als die „Bergpredigt des Datenschutzes"[1391] bezeichnet wird. Das Grundrecht wurde in der Folgezeit vor allem durch die Rechtsprechung fortentwickelt und etwa um Aussagen zur Eingriffstiefe und den sich daraus ergebenden Anforderungen ergänzt. Diese Rechtsprechung bezieht sich zwar durchgehend auf staatliche Datenverarbeitung, da aber die Datenverarbeitung durch Private prinzipiell auch grundrechtsbeeinträchtigend wirkt, können Kernaussagen der Rechtsprechung hierfür im Rahmen der mittelbaren Drittwirkung herangezogen werden. 1236

3.5.3.1 Die Begründung des Rechts auf informationelle Selbstbestimmung

Das Bundesverfassungsgericht argumentiert in seinem Grundsatzurteil mit der im allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verankerten Selbstbestimmung, die auch gegen informationelle Eingriffe abgesichert werden müsse.[1392] Die – plausible, aber nicht weiter belegte – Grundannahme des Gerichts lautet, dass derjenige, der unsicher sei, ob abweichendes Verhalten notiert und dauerhaft gespeichert werde, 1237

1389 Zuletzt z.B. BVerfG v. 27.2.2008 – 1 BvR 370, 595/07, E 120, S. 274, 312 – *Online-Durchsuchungen*; BVerfG v. 24.1.2012 – 1 BvR 1299/05, E 130, S. 151, 183 – *Dynamische IP-Adressen*; BVerfG v. 20.4.2016 – 1 BvR 966/09, E 141, S. 220–378 – *BKA-Gesetz*; BVerfG v. 21.6.2016 – 2 BvR 637/09, E 142, S. 234, 251 – *Cybercrime*; BVerfG v. 13.10.2016 – 2 BvE 2/15, E 143, S. 101, 148 – *NSA-Untersuchungsausschuss*; BVerfG v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244, Rn. 37 ff. – *Kfz-Kennzeichenerfassung II*.

1390 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1–71 – *Volkszählung*; zur Kritik an der damaligen Entscheidung siehe die Nachweise bei *Simitis,* in: Simitis 2014, Einleitung, Rn. 38.

1391 Dieser Ausdruck stammt von *Meister,* DuD 1986, S. 173, 175, der damit weniger die Bedeutung des Urteils herausstellt, sondern vielmehr den Ansatz des Bundesverfassungsgerichts kritisiert. Dazu auch *Lewinski* 2016; *Veil,* NVwZ 2018, S. 686–696.

1392 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 42 f. – *Volkszählung*.

von vornherein versuchen werde, nicht durch solches Verhalten aufzufallen. Es stelle sich ein „Einschüchterungseffekt“[1393] ein. Der Einzelne sei in seiner Entscheidungs- und Handlungsfreiheit gehemmt, wenn er nicht überschauen könne, wem in seiner sozialen Umwelt welche Informationen über ihn vorlägen. Es bestehe die Gefahr, dass der Grundrechtsberechtigte allein deswegen von der Ausübung seiner Rechte absehe, weil er damit rechne, dies werde (behördlich) registriert und könne darum für ihn risikobehaftet sein.[1394]

1238 Die Ausweitung des Persönlichkeitsschutzes auf jede Verarbeitung personenbezogener Daten begründet das Gericht im Volkszählungsurteil mit den Möglichkeiten der modernen Informationsverarbeitung. Einzelangaben über die sachlichen und persönlichen Verhältnisse einer bestimmten oder bestimmbaren Person könnten danach unbegrenzt gespeichert und durch die Integration verschiedener Informationssysteme zu einem weitgehend vollständigen Persönlichkeitsbild vervollständigt werden.[1395]

1239 Es kommt also nicht mehr darauf an, dass das Informationshandeln von sich aus bereits eine spezielle Konkretisierung des Persönlichkeitsrechts betrifft, wie etwa den Schutz der Privatsphäre oder den Schutz der Ehre. Der ebenfalls vom allgemeinen Persönlichkeitsrecht erfasste Gedanke der Selbstbestimmung[1396] ist schon durch jede Datenverarbeitung berührt, eben weil dies für den Einzelnen so unabsehbare Konsequenzen hat. Die informationelle Selbstbestimmung liegt insofern quer zu den Sphären (Intim-, Privat- und Sozialsphäre) des allgemeinen Persönlichkeitsrechts.[1397]

1240 Dieser Begründung lassen sich auf individueller Ebene bereits zwei Schutzgewährleistungen entnehmen, die miteinander in engen Zusammenhang stehen. In erster Linie bezweckt der Schutz personenbezogener Daten den Schutz der Selbstbestimmung, die einen Wert an sich darstellt. Er kann aber auch als Vorfeldschutz gegen Eingriffe in spezielle Grundrechte wirken.[1398] Das Bundesverfassungsgericht nennt hier das Beispiel einer Ver-

---

1393 BVerfG v. 11.3.2008 – 1 BvR 2074/05, E 120, S. 378, 402 – *Kfz-Kennzeichenerfassung I*.
1394 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 43 – *Volkszählung*.
1395 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 42 – *Volkszählung*.
1396 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 41 – *Volkszählung*.
1397 BeckOK GG/*Lang*, Art. 2 GG, Rn. 38.
1398 BVerfG v. 13.6.2007 – 1 BvR 1550/03, E 118, S. 168, 184 – *Kontostammdaten*; BVerfG v. 27.2.2008 – 1 BvR 370, 595/07, E 120, S. 274, 312 – *Online-Durchsuchungen*; BVerfG v. 11.3.2008 – 1 BvR 2074/05, E 120, S. 378, 397 – *Kfz-Kennzeichenerfassung I; Bäcker* 2012, S. 26.

sammlung einer Bürgerinitiative, an der man möglicherweise nicht teilnähme, wen dies behördlich registriert würde. Der Datenschutz schützt in dem Sinne nicht nur die informationelle Selbstbestimmung, sondern auch die Versammlungs- und Vereinigungsfreiheit nach Art. 8 und 9 GG.

Schließlich kommt der informationellen Selbstbestimmung – wie allen Grundrechten – auch eine objektive Funktion zu. Sie ist Teil der Werteordnung, an der das einfache Recht ausgelegt werden muss. Das Bundesverfassungsgericht betont dies, wenn es feststellt, dass mit „dem Recht auf informationelle Selbstbestimmung […] eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar [wäre], in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß." Es ist darum nur konsequent, dass der einfache Datenschutz nach § 1 Abs. 1 S. 2 BDSG 2018 im Grundsatz auch zwischen Privaten gilt. 1241

3.5.3.2 Schutzbereich des Rechts auf informationelle Selbstbestimmung

Wie auch beim Recht auf Schutz personenbezogener Daten nach Art. 7, 8 GRC (siehe 3.2.3.3, S. 289) ist der Schutzbereich des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG denkbar weit gefasst. Es schützt die betroffene natürliche Person vor jedwedem Umgang mit personenbezogenen Daten, unabhängig von der Sensibilität[1399] der jeweiligen Information. Erfasst sind dabei sämtliche Formen der Verarbeitung.[1400] Obwohl das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung gerade mit den Möglichkeiten der automatisierten Datenverarbeitung begründet hat,[1401] erstreckte das Gericht den Schutzbereich dieses Rechts später unter Verweis auf dessen persönlichkeitsrechtliche Grundlage auf jede (staatliche) Erhebung und Verarbeitung personenbezogener Daten.[1402] 1242

1399 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 45 – *Volkszählung*; BVerfG v. 13.6.2007 – 1 BvR 1550/03, E 118, S. 168, 185 – *Kontostammdaten*; BVerfG v. 11.3.2008 – 1 BvR 2074/05, E 120, S. 378, 399 – *Kfz-Kennzeichenerfassung I;* BVerfG v. 18.12.2018 – 1 BvR 142/15, E 150, S. 244, Rn. 38 – *Kfz-Kennzeichenerfassung II*.

1400 BeckOK DSR/*Brink*, Syst. C., Rn. 70; *Di Fabio,* in: Maunz/Dürig 2015, Lfg. 39, Art. 2 GG, Rn. 176.

1401 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 42 – *Volkszählung*.

1402 BVerfG v. 9.3.1988 – 1 BvL 49/86, E 78, S. 77, 84 (=NJW 1988, S. 2031).

1243 Das Bundesverfassungsgericht bezog sich bei der Beschreibung des Schutzbereichs der informationellen Selbstbestimmung auf den bereits damals in § 2 Abs. 1 BDSG 1977[1403] legaldefinierten Begriff des personenbezogenen Datums als Einzelangabe über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person.[1404] Der verfassungsrechtliche Begriff des personenbezogenen Datums deckt sich folglich mit dem einfachgesetzlichen Begriff.[1405]

1244 Dieses Vorgehen ähnelt demjenigen zum Recht auf Schutz personenbezogener Daten nach Art. 8 GRC, zu dem in den Erläuterungen auf den sekundärrechtlichen Begriff in der Datenschutzrichtlinie verwiesen wird (siehe 3.2.3.3.1, S. 290). Insofern liegt es nahe, auch hier auf die Erörterungen zum einfachgesetzlichen Recht zu verweisen (siehe 3.3.1, S. 315). Dabei muss allerdings beachtet werden, dass die Diskussion über den einfachgesetzlichen Begriff des personenbezogenen Datums als Folge der in weiten Teilen notwendigen europarechtskonformen Auslegung des einfachen deutschen Rechts auch bereits vor dem Inkrafttreten der Datenschutz-Grundverordnung durch die Begriffsdefinition in der Datenschutzrichtlinie geprägt war.[1406]

1245 Daraus ergeben sich zwei grundlegende Einwände: Zum einen stammen das Volkszählungsurteil und § 2 Abs. 1 BDSG 1977 aus einer Zeit vor dem Inkrafttreten der Datenschutzrichtlinie 95/46/EG und der später einsetzenden intensiven Diskussion über den Begriff des personenbezogenen Datums. Das Bundesverfassungsgericht kann also bei der Festlegung des Schutzbereichs des Rechts auf informationelle Selbstbestimmung nicht die europäische Definition im Blick gehabt haben. Zum anderen werden die nationalen Grundrechte durch die europäischen Regeln nicht etwa inhaltlich beeinflusst, sie sind lediglich u.U. nicht anwendbar (siehe 3.2.2.1, S. 261).

1246 Trotz dieser grundsätzlichen Bedenken dürfte in der Sache kein Unterschied zwischen dem europäischen und deutsch-grundrechtlichen Begriff des personenbezogenen Datums bestehen. Beide Grundrechte fungieren angesichts ihres breiten Anwendungsbereichs als Vorfeldschutz für die selbstbestimmte Ausübung der übrigen Grundrechte. Die Verarbeitung personenbezogener Daten erfüllt damit zwar noch nicht zwingend einen

---

1403 BGBl. I 1977, S. 201.
1404 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 42 – *Volkszählung*.
1405 *Di Fabio*, in: Maunz/Dürig 2015, Lfg. 39, Art. 2 GG, Rn. 175.
1406 Siehe dazu den Überblick bei *Bergt*, ZD 2015, S. 365–371.

Verletzungs-, aber immerhin stets einen Gefährdungstatbestand.[1407] Ob personenbezogene Daten verarbeitet werden, ist darum nicht zuletzt danach zu bestimmen, ob aus der konkreten Datenverarbeitung eine Verletzung grundrechtlich geschützter Interessen folgen kann. Denn nur, wenn dies hinreichend wahrscheinlich ist, besteht eine grundrechtliche Gefährdungslage. Zumindest in der Sache kann also auf die Ausführungen zum sekundärrechtlichen Begriff des personenbezogenen Datums verwiesen werden (siehe 3.3.1, S. 315).

3.5.3.3 Notwendigkeit einer Ermächtigungsgrundlage

Private, nur mittelbar an die Grundrechte gebundene (siehe 2.2.1, S. 77) Akteure benötigen für die Verarbeitung personenbezogener Daten nach Maßgabe des Grundgesetzes keine Ermächtigungsnorm.[1408] Dies gilt für den (privaten, dazu 2.2, S. 76) Arbeitgeber ebenso wie für den Betriebsrat[1409], weil auch das Handeln als Betriebsparteien nicht zu einer unmittelbaren Bindung an die Grundrechte führt (siehe 2.2.1, S. 77). Etwas anderes könnte angesichts der ungeklärten Art der Grundrechtsbindung höchstens für Tarifvertragsparteien gelten. 1247

Abgesehen von den Konstellationen des § 26 Abs. 7 BDSG 2018[1410] spielt dies aber keine Rolle, weil sich im Anwendungsbereich der Datenschutz- 1248

1407 BeckOK DSR/*Brink*, Syst. C., Rn. 72; BVerfG v. 13.6.2007 – 1 BvR 1550/03, E 118, S. 168, 184 – *Kontostammdaten* „Gefährdungen und Verletzungen der Persönlichkeit".

1408 *Di Fabio,* in: Maunz/Dürig 2015, Lfg. 39, Art. 2 GG, Rn. 189.

1409 Es ist allerdings ohnehin bereits zweifelhaft, ob der Betriebsrat überhaupt als eigenständiger Verantwortlicher angesehen werden kann oder nicht vielmehr stets dem Arbeitgeber zuzuordnen ist. Zur bisher unklaren neuen Rechtslage *Brams/Möhle,* ZD 2018, S. 570–573; *Jung/Hansch,* ZD 2019, S. 143–148; *Wybitul,* NZA 2017, S. 1488, 1490. Unter der Geltung des alten Bundesdatenschutzgesetzes war der Betriebsrat dem Arbeitgeber als einheitlicher verantwortlicher Stelle zugeordnet BAG v. 12.8.2009 – 7 ABR 15/08, NZA 2009, S. 1218, 1221; BAG v. 7.2.2012 – 1 ABR 46/10, E 140, S. 350, Rn. 43 (=NZA 2012, S. 744); BAG v. 14.1.2014 – 1 ABR 54/12, NZA 2014, S. 738, Rn. 28; *Dammann,* in: Simitis 2014, § 3 BDSG, Rn. 240; dazu damals schon kritisch *Kort* 2012, S. 113 ff.; *Kort,* NZA 2015, S. 1345, 1347.

1410 Das neue Bundesdatenschutzgesetz regelt für die nicht automatisierte und nicht dateisystembezogene Verarbeitung personenbezogener Daten kein sog. Verbotsprinzip. Es ist aber davon auszugehen, dass der Gesetzgeber in § 26 Abs. 7 BDSG 2018 mit dem Verweis auf § 26 Abs. 1 bis 6 BDSG 2018 auch das den Normen zugrundeliegende sog. Verbotsprinzip in Art. 5 Abs. 1 lit. a

Grundverordnung nach Art. 2 Abs. 1 DS-GVO (siehe 3.3.2, S. 334) die Notwendigkeit einer Erlaubnisnorm ohnehin nur aus Art. 5 Abs. 1 lit. a DS-GVO und Art. 6 Abs. 1 UAbs. 1 DS-GVO ergeben kann. Ein Abweichen vom Grundsatz des sog. datenschutzrechtlichen Verbotsprinzips (siehe 3.4.1.6.1, S. 418) ist von der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO nicht gedeckt.[1411]

3.5.3.4 Abwägungsfestigkeit des Rechts auf informationelle Selbstbestimmung

1249 Bei der Datenverarbeitung durch selbst nicht grundrechtsgebundene Private handelt es sich nicht um rechtfertigungsbedürftige Grundrechtseingriffe, sondern vielmehr selbst um eine Form der Grundrechtsausübung. Dennoch geben die Rechtfertigungsanforderungen an staatliche Eingriffe – wie auch im Rahmen des Rechts auf Schutz personenbezogener Daten nach Art. 7, 8 GRC (siehe 3.2.3.4, S. 293) – einen Anhaltspunkt dafür, wie Abwägungsfest das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gegenüber anderen Grundrechten ausgestaltet ist.

1250 Ein Eingriff in das Recht auf informationelle Selbstbestimmung unterliegt einem einfachen Gesetzesvorbehalt, sowie sämtlichen allgemeinen Schranken-Schranken für Grundrechtseingriffe, von denen das Bundesverfassungsgericht einige hervorhebt.[1412]

3.5.3.4.1 Bestimmtheit

1251 Die Verarbeitung personenbezogener Daten setzt voraus, dass der Verwendungszweck in der Verarbeitungsgrundlage präzise bestimmt wird[1413] und

---

DS-GVO und Art. 6 Abs. 1 UAbs. 1 DS-GVO ebenso wie alle anderen allgemeinen Vorschriften auch auf diese Art der Verarbeitung erstrecken wollte, BeckOK DSR/*Riesenhuber*, § 26 BDSG, S. 41.

1411 *Hense,* in: Sydow 2018, Art. 88 DS-GVO, Rn. 7.

1412 Grundsätzlich BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 44 ff. – *Volkszählung*.

1413 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 46 – *Volkszählung*; BeckOK DSR/*Brink*, Syst. C., Rn. 96; *Di Fabio,* in: Maunz/Dürig 2015, Lfg. 39, Art. 2 GG, Rn. 182.

die Verwendung der Daten auf diesen bestimmten Zweck begrenzt[1414] bleibt. Daraus folgt, dass „die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken“[1415] nicht zulässig ist. Die Bestimmtheitsanforderungen steigen mit der Eingriffstiefe.[1416]

Diese verfassungsrechtlichen Vorgaben sind grundsätzlich auch für Kollektivvereinbarungen relevant, in denen die Verarbeitung von Beschäftigtendaten geregelt wird. Aufgrund der mittelbaren Bindung der Kollektivvertragsparteien an das Recht der Beschäftigten auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG müssen diese Vereinbarungen einen bestimmten Verarbeitungszweck angeben und die Verarbeitung im Weiteren grundsätzlich darauf beschränken. 1252

Es ist allerdings nicht erkennbar, inwieweit diese verfassungsrechtlichen Anforderungen an die Zweckbindung sich von jenen in Art. 5 Abs. 1 lit. b DS-GVO (siehe 3.4.1.2, S. 355) unterscheiden. Damit bleiben sie zwar im Rahmen der Öffnungsklausel in § 88 DS-GVO, spielen aber zumindest praktisch keine Rolle. 1253

3.5.3.4.2 Verfahrensrechtliche Schutzvorkehrungen

Neben dem Bestimmtheitsgebot werden für die Einschränkung des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG weitere verfahrensrechtliche Schutzvorkehrungen wie Aufklärungspflichten, Auskunftspflichten und Löschungspflichten[1417] sowie Kennzeichnungs- und Protokollierungspflichten[1418] verlangt. Gerade bei der besonders umfangreichen Verarbeitung personenbezogener Daten bedarf es festgelegter Maßnahmen zur Datensicherheit.[1419] 1254

1414 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 46 – *Volkszählung*; BeckOK DSR/*Brink*, Syst. C., Rn. 102 f.
1415 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 46 – *Volkszählung*.
1416 BeckOK DSR/*Brink*, Syst. C., Rn. 101; *Di Fabio,* in: Maunz/Dürig 2015, Lfg. 39, Art. 2 GG, Rn. 183; zur Verarbeitung von Telekommunikationsdaten BVerfG v. 2.3.2010 – 1 BvR 256/08, E 125, S. 260, 332 ff. – *Vorratsdatenspeicherung II*.
1417 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 46 – *Volkszählung*; BVerfG v. 20.4.2016 – 1 BvR 966/09, E 141, S. 220, 324 – *BKA-Gesetz*.
1418 BVerfG v. 20.4.2016 – 1 BvR 966/09, E 141, S. 220, 324 – *BKA-Gesetz*.
1419 Zur Verarbeitung von Telekommunikationsdaten BVerfG v. 2.3.2010 – 1 BvR 256/08, E 125, S. 260, 325 ff. – *Vorratsdatenspeicherung II*.

1255 Dies trägt dem Umstand Rechnung, dass sich die Grundrechtsbeeinträchtigung bei der Verarbeitung personenbezogener Daten nicht allein aus dem ergibt, was der Verantwortliche mit den Daten vorhat, sondern auch und gerade aus der Unsicherheit und dem Missbrauchspotenzial, dass mit der Datenverarbeitung verbunden ist.

3.5.3.4.3 Verhältnismäßigkeitsprinzip

1256 Wie bereits in der Abgrenzung der unionalen zu den nationalen Grundrechten erwähnt (siehe 3.2.2.3.3, S. 275) bildet das Verhältnismäßigkeitsprinzip den Kern der mitgliedstaatlichen Konkretisierungskompetenz im Beschäftigtendatenschutz.

3.5.3.4.3.1 Allgemeine Anforderungen

1257 Für Einschränkungen des Rechts auf informationelle Selbstbestimmung gilt lediglich eine absolute Grenze: Über die betroffene Person darf kein Persönlichkeitsprofil als Gesamtbild ihrer Persönlichkeit angelegt werden.[1420] Ansonsten ist die Verhältnismäßigkeitsprüfung stark einzelfallbezogen, auch weil sich die Eingriffstiefe nicht abstrakt, sondern nur im Verwendungszusammenhang[1421] ergibt.

1258 Staatliche Eingriffe in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sind grundsätzlich im überwiegenden Allgemeininteresse gerechtfertigt,[1422] unterliegen also einer eher niedrigen Eingriffsschwelle. Im Bereich der privaten Datenverarbeitung kann darum auch die (unternehmerische) Berufsfreiheit des Arbeitgebers nach Art. 12 Abs. 1 GG eine Beeinträchtigung der grundrechtlich geschützten Interessen des Arbeitnehmers rechtfertigen.

1420 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, Rn. 53 – *Volkszählung*; BeckOK DSR/*Brink*, Syst. C., Rn. 114.
1421 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, 45 – *Volkszählung*.
1422 BVerfG v. 15.12.1983 – 1 BvR 209/83, E 65, S. 1, Rn. 44 – *Volkszählung*.

3.5.3.4.3.2 Kriterien zur Abwägung der betroffenen Grundrechte

Insgesamt zeigen sich starke Ähnlichkeiten zur Einschätzung der Verhältnismäßigkeit bei den EU-Grundrechten (siehe 3.2.3.5, S. 299).[1423] So können für die Bestimmung der Eingriffstiefe vergleichbare Kriterien herangezogen werden: 1259

- Persönlichkeitsrelevanz: Wie schwer ein Eingriff in das Recht auf informationelle Selbstbestimmung wiegt, hängt u.a. vom Grad der Persönlichkeitsrelevanz ab, den die erfasste Information allein oder durch Verknüpfung mit anderen Informationen aufweist.[1424] Es bleibt zwar jede Verarbeitung personenbezogener Daten ein Eingriff, für die Rechtfertigungsanforderungen kann aber trotzdem auf die „Sphärentheorie" des Bundesverfassungsgerichts[1425] zurückgegriffen werden.
- Umfang der Verarbeitung: Je mehr Daten verarbeitet werden und je vielfältiger und umfangreicher der Datenbestand[1426] ist, desto detaillierter wird das Bild, dass sich der Verantwortliche über die Persönlichkeit des Betroffenen machen kann.
- Streubreite: Wenn eine Datenverarbeitung auf eine unbestimmte Vielzahl an Personen gerichtet ist, die hierfür keinen Anlass gegeben haben, erhöht die große Zahl an Verarbeitungen nicht nur das Risiko eines Missbrauchs. Weil sie im Grunde jeden treffen kann, führt dies auch zu einem – selbst schon grundrechtsgefährdenden – Gefühl des Überwachtwerdens.[1427]
- Mögliche Konsequenzen: Das Recht auf informationelle Selbstbestimmung macht bereits den Datenumgang zum Gefährdungstatbestand. Diese Gefährdung wiegt umso schwerer, je einschneidender die Nachteile für den Einzelnen sein können.[1428]

1423 Für die Übertragbarkeit der Leitlinien und zur Rechtsprechung im Folgenden *Thüsing,* in: Thüsing 2014, § 3, Rn. 40 ff.

1424 BVerfG v. 4.4.2006 – 1 BvR 518/02, E 115, S. 320, 348 – *Rasterfahndung II; Thüsing,* in: Thüsing 2014, § 3, Rn. 42.

1425 BVerfG v. 15.1.1970 – 1 BvR 13/68, E 27, S. 344, 351 – *Ehescheidungsakten*; BVerfG v. 19.7.1972 – 2 BvL 7/71, E 33, S. 367 ff. – *Zeugnisverweigerungsrecht für Sozialarbeiter*; dazu ausführlich *Di Fabio,* in: Maunz/Dürig 2015, Lfg. 39, Art. 2 GG, Rn. 158 ff., m.w.N.

1426 BVerfG v. 27.2.2008 – 1 BvR 370, 595/07, E 120, S. 274, 324 – *Online-Durchsuchungen*.

1427 BVerfG v. 11.3.2008 – 1 BvR 2074/05, E 120, S. 378, 402 – *Kfz-Kennzeichenerfassung I*.

1428 BVerfG v. 4.4.2006 – 1 BvR 518/02, E 115, S. 320, 351 – *Rasterfahndung II*.

– Heimlichkeit: Eine verdeckte Maßnahme macht es der betroffenen Person wesentlich schwerer, sie zu erkennen und dagegen Rechtsschutz zu suchen oder sich anderweitig zu wehren. Dies vertieft den Eingriff.[1429]

1260 Eine Datenverarbeitung mit einer gesteigerten Eingriffsintensität bedarf seitens des Arbeitgebers nicht nur eines seinerseits gesteigerten grundrechtlich geschützten Interesses. Solche Maßnahmen sind auch regelmäßig nur dann verhältnismäßig, wenn ein konkreter Anlass oder Verdacht vorliegt, dass dieses Interesse gefährdet sein kann.[1430]

3.5.3.5 Ergebnis

1261 Für die Anwendung des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG besteht ohnehin nur ein enger Rahmen, der durch die Öffnungsklausel in Art. 88 DS-GVO definiert wird. Die verfassungsrechtlichen Anforderungen können in weiten Teilen nur zur Konkretisierung der Anforderungen des europäischen Datenschutzrechts herangezogen werden.

1262 Dass eben dies geschieht, ist allerdings zweifelhaft. Es ist nicht erkennbar, dass die verfassungsrechtlichen Vorgaben zum Recht auf informationelle Selbstbestimmung in den hier relevanten Bereichen signifikant über die primär- und sekundärrechtlichen Vorgaben des europäischen Datenschutzrechts hinausgehen. Eine wesentliche Konkretisierung oder Abänderung ist darum nicht zu erwarten. Das ist stattdessen die Aufgabe derer, die spezifische Regelungen im Sinne der Öffnungsklausel in Art. 88 DS-GVO erlassen dürfen.

3.6 Folgen für das sekundär- und einfachgesetzlichen Datenschutzrecht

1263 Die Handhabung der grundlegenden Vorgaben der Datenschutz-Grundverordnung an die Verarbeitung personenbezogener Daten (siehe 3.4, S. 353) sowie der verfassungsrechtlichen Anforderungen (siehe 3.5, S. 471) unterscheidet sich zwar nicht in allen, aber doch in einigen Punkten je nach anwendbarem Erlaubnistatbestand voneinander. Das ist nicht zuletzt

---

1429 BVerfG v. 11.3.2008 – 1 BvR 2074/05, E 120, S. 378, 402 f. – *Kfz-Kennzeichenerfassung I*.

1430 Zur Verdachtsabhängigkeit bei staatlichen Maßnahmen BVerfG v. 4.4.2006 – 1 BvR 518/02, E 115, S. 320–381 – *Rasterfahndung II*.

dem Umstand geschuldet, dass jeder Erlaubnistatbestand auf andere Lebenssachverhalte hin zugeschnitten ist. Dies gilt insbesondere für die Reichweite der Zweckkonkretisierung und den Maßstab der Interessenabwägung.

Trotz dieser Differenzierung erweist sich ein Vorgehen nach Erlaubnistatbeständen noch als zu holzschnittartig. Abgesehen davon, dass es für die exakten Anforderungen ohnehin stets auf den Einzelfall ankommt, empfiehlt es sich darum, diese zumindest für die in der Industrie 4.0 typischen Verarbeitungssituationen (siehe 3.6.2, S. 525) zu ermitteln. 1264

3.6.1 Erlaubnistatbestände im Beschäftigtendatenschutz

Für den Umgang mit personenbezogenen Beschäftigtendaten kommen im Zusammenhang mit dem Einsatz von Assistenz- und Produktionssystemen verschiedene Erlaubnistatbestände in Betracht. Dies sind: 1265

- Die Verarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO bzw. – wenn man die hier vertretene Auffassung zur Unionswidrigkeit von § 26 Abs. 1 S. 1 BDSG 2018 (siehe 3.1.5.2, S. 248) nicht teilt – zur Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses nach § 26 Abs. 1 S. 1 BDSG 2018.
- Die Verarbeitung auf der Grundlage einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO, unter Berücksichtigung der Maßstäbe in § 26 Abs. 2 BDSG 2018.
- Die Verarbeitung auf der Grundlage einer Kollektivvereinbarung, Art. 88 Abs. 1 DS-GVO bzw. § 26 Abs. 4 BDSG 2018.
- Die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO.

3.6.1.1 Das Verhältnis der Erlaubnistatbestände untereinander

Nach Art. 6 Abs. 1 DS-GVO genügt es, wenn „mindestens" eine der nachfolgend genannten Bedingungen erfüllt ist. Zwischen den hier aufgezählten Alternativen besteht folglich kein Rangverhältnis, weshalb sie jeweils eigenständige, voneinander unabhängige Rechtsgrundlagen für den Um- 1266

gang mit Beschäftigtendaten bilden.[1431] Sie entfalten untereinander auch keine Sperrwirkung, dergestalt, dass etwa eine Maßnahme, die bereits auf die Vertragsdurchführung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO bzw. § 26 Abs. 1 S. 1 BDSG gestützt werden könnte, nicht auch mit der Wahrung berechtigter Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO begründet werden könnte.[1432] Für die hier aufgeworfenen Fragen lassen sich dennoch erhebliche Bedeutungsunterschiede erkennen.

3.6.1.1.1 Leitbildfunktion von Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO

1267 Der Datenschutz-Grundverordnung lässt sich an verschiedenen Stellen eine gewisse Leitbildfunktion des vertragsbezogenen Erlaubnistatbestands in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO entnehmen. Wird z.B. die Erfüllung eines Vertrags davon abhängig gemacht, dass die betroffene Person in die Verarbeitung ihrer Daten nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO einwilligt, muss gemäß Art. 7 Abs. 4 DS-GVO dem Umstand „in größtmöglichen Umfang Rechnung getragen werden", ob diese Datenverarbeitung zur Erfüllung des Vertrags erforderlich ist. Das Leitbild des Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO, demzufolge nur die für die Vertragserfüllung erforderlichen Daten verarbeitet werden dürfen, soll nicht durch eine Einwilligung konterkariert werden.

1268 Überschneidungen ergeben sich auch im Verhältnis der Datenverarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO und derjenigen zur Wahrung berechtigter Interessen nach Buchstabe f. Soweit es hier um die berechtigten Interessen des Vertragspartners und nicht des Dritten geht, ist nicht klar, inwiefern dem Erlaubnistatbestand in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO noch ein relevanter Anwendungsbereich bleibt. Gerade im Beschäftigungsverhältnis treffen die Parteien umfassende Rücksichtnahmepflichten nach § 241 Abs. 2 BGB, die ebenfalls Teil des zu erfüllenden Vertrags sind.[1433] Eine hierauf gerichtete Datenver-

---

1431 BeckOK DSR/*Albers/Veit*, Art. 6 DS-GVO, Rn. 18; *Buchner/Petri*, in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 22.

1432 Im diesem Sinne noch zur inhaltsgleichen Vorschrift des Art. 7 DSRL EuGH, ECLI:EU:C:2011:777, Rn. 31 ff. – *ASNEF*; so auch *Zöll*, in: Taeger/Gabel 2019, § 26 BDSG, Rn. 12.

1433 Zu § 26 Abs. 1 S. 1 BDSG 2018 *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 44; zu § 32 Abs. 1 S. 1 BDSG 2003 *Schmidt*, DuD 2010, S. 207, 209; allgemein zu Art. 6 Abs. 1 Uabs. 1 lit. b BeckOK DSR/*Albers/Veit*, Art. 6 DS-GVO, Rn. 31; *Buchner/Petri*, in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 33; *Gola*,

arbeitung verfolgt per se berechtigte Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO (siehe 3.4.1.3.4.2.1, S. 381).

Zumindest für eine Datenverarbeitung, die auf die Erfüllung der verschiedenen vertraglichen Pflichten gerichtet ist, sind darum keine berechtigten Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO denkbar, die nicht zugleich von Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO erfasst wären.[1434] Dies verbietet es zwar nicht, diese Interessen weiterhin im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zu Geltung zu bringen. Es gilt dabei aber zu beachten, dass außervertragliche Interessen, die im Zusammenhang mit dem Vertragsverhältnis stehen, hierdurch beeinflusst werden. Dieses Phänomen ist vor allem aus der Haftung für die Verletzung absoluter Rechte bekannt. Obwohl es sich dabei nicht um vertragliche, sondern gesetzliche Ansprüche handelt, werden etwaige Haftungserleichterungen – etwa für unentgeltlich Leistende wie den Entleiher nach § 599 BGB[1435] oder Arbeitnehmer[1436] – aus dem vertraglichen Bereich hierauf übertragen. 1269

Diese Ausstrahlungswirkung des Vertragsverhältnisses lässt darauf schließen, dass die maßgeblichen Interessen der Vertragsparteien aus dem Vertragsverhältnis abzuleiten sind, soweit sie mit diesem Verhältnis unmittelbar zusammenhängen. Dies gilt auch für Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Da zudem auch bei der Verarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO eine Angemessenheitsprüfung vorzunehmen ist (siehe 3.4.1.3.4.2.1, S. 381),[1437] dürften die Erlaubnistatbestände in Art. 6 Abs. 1 UAbs. 1 lit. b und f DS-GVO im unmittelbaren Zusammenhang mit dem Beschäftigungsverhältnis und in Bezug auf die Interessen des Arbeitgebers stets zum selben Ergebnis führen.[1438] Damit verbleibt letzterem in dieser Situation kein relevanter Anwendungsbereich. 1270

---

in: Gola 2018, Art. 6 DS-GVO, Rn. 28 A.A., d.h. für die Berücksichtigung lediglich der Hauptpflichten in § 32 Abs. 1 S. 1 BDSG 2003 *Joussen*, NZA 2010, S. 254, 258.

1434 So wohl auch *Maschmann*, in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 68; ähnlich *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 18.

1435 Siehe nur BeckOK BGB/*Wagner*, § 599 BGB, Rn. 3, m.w.N.

1436 BAG v. 30.8.1966 – 1 AZR 456/65, E 19, S. 66 (=NJW 1967, S. 269); BeckOGK/*Feuerborn*, § 619a BGB, Rn. 58.

1437 Speziell für den Beschäftigtendatenschutz *Gola*, BB 2017, S. 1462, 1464. Davon geht auch der deutsche Gesetzgeber in Bezug auf § 26 Abs. 1 S. 1 BDSG 2018 aus, BT-Drucks. 18/11325, S. 97.

1438 *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 18.

1271 Die zentrale Frage für die praktische Abgrenzung der Erlaubnistatbestände in Art. 6 Abs. 1 UAbs. 1 lit. b und f DS-GVO lautet darum, wie weit dieser unmittelbare Zusammenhang mit dem Vertragsverhältnis – hier: mit dem Beschäftigungsverhältnis – reicht. Diese Frage stellt sich allgemein vor allem im Hinblick auf Maßnahmen zur Überwachung der Arbeitnehmer, die durchgeführt wird, um Schaden vom Arbeitgeber oder seinen Vertragspartnern abzuwenden.[1439] Im Kontext von Assistenz- und Produktionssystemen geht es vor allem um den Austausch von Daten in Produktionsverbünden (siehe 3.6.1.3, S. 512).

3.6.1.1.2 Das Verhältnis von § 26 BDSG zu den Regelungen der DS-GVO

1272 Mit § 26 BDSG 2018 hat der deutsche Gesetzgeber gestützt auf die Öffnungsklausel in Art. 88 Abs. 1 DS-GVO umfassende Sonderregelungen für das Beschäftigungsverhältnis getroffen (siehe 3.1.4, S. 245). Ihr Verhältnis zur Datenschutz-Grundverordnung ist für die Darstellung jedoch nur teilweise von Belang bzw. unproblematisch:

- Die – unionsrechtskonformen (siehe 3.1.5, S. 246) – Regelungen über die Datenverarbeitung zur Ausübung der Rechte der Interessenvertretung nach § 26 Abs. 1 S. 1 Alt. 4 BDSG 2018 sowie die zur Verhinderung und Aufklärung von Straftaten nach § 26 Abs. 1 S. 2 BDSG 2018 betreffen keine Spezifika der Industrie 4.0 und bleiben hier darum außer Betracht.
- Die Regelungen zur Datenverarbeitung auf der Grundlage einer Kollektivvereinbarung in § 26 Abs. 4 BDSG 2018 wirken rein deklaratorisch. Nach anderer Meinung folgt die spezifisch datenschutzrechtliche Regelungsmacht erst aus § 26 Abs. 4 S. 1 BDSG 2018 (zu beidem näher 3.1.5, S. 246). In jedem Fall gehen die Regelungen in Kollektivvereinbarungen den Erlaubnistatbeständen in Art. 6 DS-GVO vor.
- Die Regelungen in § 26 Abs. 5 BDSG 2018 verpflichten den Verantwortlichen geeignete Maßnahmen zu ergreifen, um sicherzustellen, dass insbesondere die in Art. 5 DS-GVO dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Diese Regelung ist nicht von der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO gedeckt und darum weitgehend als Klarstellung zu Art. 5 Abs. 2, 24 Abs. 1

1439 *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 17 f.

DS-GVO anzusehen.[1440] Andernfalls wäre sie unionsrechtswidrig und dadurch unanwendbar. Der Gesetzgeber ist darüber hinaus der Ansicht, die Norm beinhalte auch geeignete Garantien und setze insofern die Anforderungen aus der Öffnungsklausel für die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten in Art. 10 DS-GVO um.[1441] Ob dem so ist,[1442] kann für diese Arbeit dahinstehen; die Verarbeitung der Daten nach Art. 10 DS-GVO spielt für Assistenzsysteme keine Rolle.

– Die Regelung in Art. 26 Abs. 8 BDSG 2018 weitet den Beschäftigtenbegriff gegenüber dem europäischen Begriffsverständnis insbesondere auch auf arbeitnehmerähnliche Selbständige und Beamte aus.[1443] Dies spielt im Rahmen dieser Arbeit aber keine Rolle. Der Einsatz von Assistenz- und Produktionssystemen in der Industrie 4.0 ist ein Phänomen, das in Deutschland hauptsächlich Arbeitnehmer in der privatwirtschaftlich organisierten Industrie betrifft. Die Beschäftigteneigenschaft dieser Personen, sowohl im Sinne des Art. 88 Abs. 1 DS-GVO als auch des § 26 Abs. 8 Nr. 1 BDSG 2018 steht außer Frage.

Die Abgrenzungsproblematik beschränkt sich für den Einsatz von Assistenz- und Produktionssystemen in der Industrie 4.0 darum auf die Generalklausel in § 26 Abs. 1 S. 1 Alt. 1 bis 3 BDSG 2018 sowie auf die Regelungen zur Einwilligung nach § 26 Abs. 2 BDSG 2018. 1273

3.6.1.1.2.1 Das Verhältnis der Generalklausel in § 26 Abs. 1 S. 1 BDSG 2018 zur DS-GVO

Die Abgrenzung der Erlaubnistatbestände in § 26 Abs. 1 S. 1 BDSG 2018 und Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO hängt davon ab, wie man erstere im Hinblick auf die Anforderungen in Art. 88 DS-GVO beurteilt (siehe 3.1.5.2, S. 248). 1274

Bewertete man die Regelung in § 26 Abs. 1 S. 1 BDSG mit der hier vertretenen Auffassung als europarechtswidrig, bleibt Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO unvermindert anwendbar (siehe 3.1.2, S. 241). Entsprechend des 1275

1440 In Bezug auf Art. 5 Abs. 2 DS-GVO für eine alleinige Klarstellungsfunktion BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 58; *Seifert*, in: Simitis et al. 2019, Art. 88 DS-GVO, Rn. 225.

1441 BT-Drucks. 18/11325, S. 97.

1442 Dafür wohl ErfK/*Franzen*, § 26 BDSG, Rn. 49.

1443 Dazu *Maschmann*, in: Kühling/Buchner 2018, Art. 88 DS-GVO, S. 65.

Anwendungsvorrangs des Unionsrechts bliebe § 26 Abs. 1 S. 1 BDSG 2018 dann nur ein nicht weiter relevanter Anwendungsbereich bei der nichtautomatisierten und auch nicht dateisystembezogenen Datenverarbeitung nach § 26 Abs. 7 BDSG 2018 (siehe 3.3.2, S. 334). Für die übrige Datenverarbeitung zur Erfüllung des Arbeitsvertrags wäre allein auf Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO abzustellen.

1276 Die herrschende Meinung hält § 26 Abs. 1 S. 1 BDSG 2018 dagegen für europarechtskonform. Aufgrund der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO wäre der Erlaubnistatbestand in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO im Anwendungsbereich des § 26 Abs. 1 S. 1 BDSG 2018 folglich selbst nicht anwendbar. Dies zieht Abgrenzungsschwierigkeiten nach sich: Für die Verarbeitung von Beschäftigtendaten – oder für diese Arbeit allein relevant: Arbeitnehmerdaten nach § 26 Abs. 8 Nr. 1 BDSG 2018 –, die für den Zweck des Beschäftigungsverhältnisses erfolgt, wäre somit allein auf § 26 Abs. 1 S. 1 BDSG 2018 abzustellen.[1444] Für die Verarbeitung von beschäftigungsfremden Zwecken, die dennoch auf einen Vertrag gestützt werden kann, bliebe Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO aber weiterhin anwendbar.[1445] Diese Zwecke liegen außerhalb sowohl der Öffnungsklausel nach Art. 88 Abs. 1 DS-GVO als auch des Anwendungsbereichs des § 26 Abs. 1 S. 1 BDSG 2018.

1444 BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 20; *Wybitul et al.*, ZD 2015, S. 559, 561. In Bezug auf präventive Compliance, die teilweise ebenfalls unter die Zwecke des Beschäftigungsverhältnisses fallen soll, *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 17. Die Regelung in § 26 Abs. 1 S. 1 BDSG 2018 führt die in § 32 Abs. 1 S. 1 BDSG 2003 fort, BT-Drucks. 18/11325, S. 96 f. Im Verhältnis von § 26 Abs. 1 S. 1 BDSG 2018 zu Art. 6 Abs. 1 Uabs. 1 lit. b DS-GVO gilt darum dasselbe wie im Verhältnis von § 32 Abs. 1 S. 1 zu § 28 Abs. 1 S. 1 Nr. 1 BDSG 2003 (dazu BT-Drucks. 16/13657, S. 20).

1445 Hierzu zählen die Abwicklung von Verträgen über Werkswohnungen oder ähnlichen Vergünstigungen, siehe nur *Buchner/Petri*, in: Kühling/Buchner 2018, Art. 6 DS-GVO, Rn. 51; *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 60; *Maschmann*, in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 18. Noch zum insofern identischen Verhältnis von § 32 Abs. 1 S. 1 BDSG 2003 zu § 28 Abs. 1 S. 1 Nr. 1 BDSG 2003: *Bierekoven*, CR 2010, S. 203, 205 f.; *Erfurth*, NJOZ 2009, S. 2914, 2922; *Schmitz* 2016, S. 183.

3.6.1.1.2.2 Das Verhältnis der Regelungen zur Einwilligung in DS-GVO und BDSG 2018

Die Regelung in § 26 Abs. 2 BDSG 2018 konkretisiert die Vorschriften zur Einwilligung in Art. 7 DS-GVO. Dabei kann sich der deutsche Gesetzgeber auf Art. 88 Abs. 1 DS-GVO berufen. Die Einwilligung wird in der Norm zwar nicht eigens erwähnt, die Aufzählung ist aber ausdrücklich nicht abschließend.[1446] Dass sie auch die Besonderheiten für die Einwilligung im Beschäftigungskontext abdeckt, kann man dem ErwG 155 entnehmen. 1277

Die für den Umgang mit Produktions- und Assistenzsystemen relevante Regelung in § 26 Abs. 2 S. 1 und 2 BDSG 2018 betrifft die Freiwilligkeit der Einwilligung (siehe 3.6.1.5, S. 523). Der deutsche Gesetzgeber spricht hier u.a. das Abhängigkeitsverhältnis im Beschäftigungskontext an. Was die Beurteilung dieses – aber ohnehin bereits in ErwG 43 angesprochenen[1447] – Kriteriums angeht, ist § 26 Abs. 2 S. 1 und 2 BDSG 2018 vorrangig anzuwenden. Gleiches gilt für das Formerfordernis in Satz 3 und die Informationspflichten in Satz 4 von § 26 Abs. 2 BDSG 2018. 1278

3.6.1.2 Die Datenverarbeitung zur Erfüllung des Arbeitsvertrags

Der Erlaubnistatbestand in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO für die Datenverarbeitung zur Erfüllung eines Vertrags bildet aufgrund seiner Leitbildfunktion (siehe 3.6.1.1.1, S. 486) die wichtigste Verarbeitungsgrundlage im Beschäftigungsverhältnis. Sie setzt den Maßstab, an dem sich insbesondere Kollektivvereinbarungen nach § 26 Abs. 4 BDSG orientieren (siehe 3.6.1.4.2, S. 519). Die Prüfung hier vermittelt darum einen recht zuverlässigen Einblick darüber, was insgesamt im Beschäftigungsverhältnis an Datenverarbeitung zulässig sein kann. 1279

3.6.1.2.1 Reichweite der Zwecksetzungsbefugnis

Das maßgebliche Element für die Konkretisierung datenschutzrechtlicher Anforderungen ist nach der hier vertretenen Auffassung die Zweckset- 1280

1446 *Seifert*, in: Simitis et al. 2019, Art. 88 DS-GVO, Rn. 215, i.E. auch *Maschmann*, in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 48; BeckOK DSR/*Riesenhuber*, Art. 88 DS-GVO, Rn. 76.

1447 *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 77.

zung. Bei der Verarbeitung zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO wird sie maßgeblich durch die Auslegung der vertraglichen Pflichten bestimmt. Steht einem Teil auf vertraglicher Ebene ein Leistungsbestimmungsrecht zu, ist dieses Recht auf der datenschutzrechtlichen Ebene als Zwecksetzungsbefugnis zu berücksichtigen (siehe 3.4.1.4.7, S. 403). Im Arbeitsverhältnis ist dies das Weisungsrecht des Arbeitgebers nach § 106 GewO. Die Zwecksetzungsbefugnis ist folglich kongruent mit der Reichweite des Weisungsrechts.

3.6.1.2.1.1 Das Weisungsrecht als Ausdruck unternehmerischer Freiheit

1281 Der Inhalt der Arbeitsleistung ergibt sich nicht unmittelbar aus dem Arbeitsvertrag, sondern bedarf der Konkretisierung durch Weisungen des Arbeitgebers (siehe 2.4, S. 189). Wie auch bei anderen Leistungsbestimmungsrechten[1448] steht dem Arbeitgeber als Bestimmungsberechtigten bei der Ausübung dieses Rechts ein gewisser Entscheidungsspielraum zu. Darin liegt der Unterschied zu einem rein faktischen Bestimmungsrecht[1449], wie es sich z.B. aus der Verwendung unbestimmter Begrifflichkeiten im Vertrag ergibt. Die Auslegung eines unbestimmten Rechtsbegriffs kann vom Gericht in vollem Maße nachgeprüft werden. Die Ausübung eines Leistungsbestimmungsrechts unterliegt demgegenüber lediglich der Billigkeitskontrolle nach § 315 BGB, die im Falle des Weisungsrechts des Arbeitgebers in § 106 S. 1 GewO spezialgesetzlich geregelt ist.

1282 Einer Weisung eines Arbeitgebers liegt in der Regel eine von ihm getroffenen unternehmerischen Entscheidung zugrunde. Der Entscheidungsspielraum, der ihm bei der Ausübung seines Weisungsrechts zusteht, beruht auf der eingeschränkten Überprüfbarkeit dieser unternehmerischen Entscheidung. Der Arbeitgeber unterliegt hier einer bloßen Willkürkontrolle (siehe 2.4.4.1, S. 193).

1283 Die Weisung selbst als konkrete Umsetzung der unternehmerischen Entscheidung ist unterdessen nicht mehr vom Entscheidungsspielraum des Arbeitgebers gedeckt und unterliegt folglich der uneingeschränkten Kontrolle durch die Gerichte. Die genaue Verortung der Grenze zwischen der

---

1448 Zu § 315 BGB BGH v. 10.10.1991 – III ZR 100/90, Z 115, S. 311, Rn. 29 (=NJW 1992, S. 171); BGH v. 18.10.2007 – III ZR 277/06, Z 174, S. 48, Rn. 20 (=NVwZ 2008, S. 110); daran anschließend BAG v. 13.6.2012 – 10 AZR 296/11, AP GewO § 106 Nr. 15, Rn. 28 (=NZA 2012, S. 1154).

1449 Zur Abgrenzung BeckOGK/*Netzer*, § 315 BGB, Rn. 57.

unternehmerischen Entscheidung auf der einen und ihrer Umsetzung auf der anderen Seite entscheidet damit maßgeblich über die Reichweite des Entscheidungsspielraums des Arbeitgebers (siehe 2.4.4.3, S. 195).

3.6.1.2.1.2 Konsequenzen für den Prüfungsaufbau und die Prüfdichte

Nach der hier gewählten Konzeption (3.2.2.5.2, S. 281) unterliegt die Verarbeitung von Beschäftigtendaten in weiten Teilen zwei Kontrollinstrumenten: der Ausübungskontrolle nach § 106 S. 1 GewO und der Erforderlichkeitsprüfung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO. Beide Instrumente betreffen unterschiedliche Prüfungspunkte und stehen insofern nebeneinander. Die Ausübungskontrolle formuliert Anforderungen an die Zwecksetzung, die Erforderlichkeitsprüfung knüpft an den so gesetzten Zweck an. Dabei zeigen sich dem ersten Anschein nach Überschneidungen. So müsste im Rahmen der Billigkeitskontrolle nach § 106 S. 1 GewO auch das Recht der Arbeitnehmer auf informationelle Selbstbestimmung nach Art. 2 Abs. 1, 1 Abs. 1 GG berücksichtigt werden. Für die Datenverarbeitung zur Vertragserfüllung ist diesbezüglich aber Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO vorrangig anzuwenden. In dessen Rahmen ist wiederum auf Arbeitnehmerseite allein deren unionales Grundrecht auf Schutz ihrer personenbezogenen Daten nach Art. 8 GRC relevant. Die Billigkeitskontrolle im engeren Sinne nach § 106 S. 1 GewO wird darum hinsichtlich ihrer datenschutzrechtlichen Aspekte völlig durch die Erforderlichkeitsprüfung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO verdrängt. 1284

Dies hat Konsequenzen für den Prüfungsaufbau und die Prüfdichte. Die datenschutzrechtliche Prüfung der Zwecksetzung entspricht der Prüfung der unternehmerischen Entscheidung nach § 106 S. 1 GewO. Hier sind die Wertungen des deutschen Arbeitsrechts entscheidend. Die anschließende Prüfung im Hinblick auf die Geeignetheit, Erforderlichkeit und Angemessenheit der Datenverarbeitung richtet sich nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO und insbesondere dem Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO. Hier sind die Wertungen des europäischen Datenschutzrechts entscheidend. 1285

3.6.1.2.1.2.1 Übereinstimmende Prüfdichte in beiden Kontrollinstrumenten

1286 Hinsichtlich der jeweiligen Prüfdichte lassen sich die beiden Kontrollinstrumente ohne Weiteres in Einklang bringen. Die Geeignetheit, Erforderlichkeit und Angemessenheit der Datenverarbeitung unterliegt wie die konkrete Weisung des Arbeitgebers der vollen gerichtlichen Kontrolle. Hier ist lediglich zu beachten, dass der Maßstab der Angemessenheitsprüfung vorrangig durch die gemeinsamen Vorstellungen der Parteien bestimmt wird.

1287 Bei der Zwecksetzungsbefugnis ist zwischen dem Inhalt dieses Rechts und seinen Grenzen zu unterscheiden. Die Grenzen ergeben sich zum einen aus der abstrakten Zweckvorgabe in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO, demzufolge die Datenverarbeitung nur auf diesen Erlaubnistatbestand gestützt werden kann, wenn der Zweck im unmittelbaren Zusammenhang mit dem Beschäftigungsverhältnis steht (siehe 3.6.1.1.1, S. 486). Hinzu kommen die inhärenten Beschränkungen des Weisungsrechts, das sich zum einen gemäß § 106 S. 1 GewO von vornherein nur auf den Inhalt, den Ort und die Zeit der Arbeitsleistung bezieht und zum anderen dort seine Grenze findet, wo die Arbeitsbedingungen u.a. bereits durch den Arbeitsvertrag oder gesetzliche Vorschriften festgelegt sind. Innerhalb dieser Grenzen ist die Ausübung der Zwecksetzungsbefugnis wie die unternehmerische Entscheidung nur auf Plausibilität und Willkürfreiheit zu überprüfen.

3.6.1.2.1.2.2 Gängiges Beispiel 1: Vertrauensarbeitszeit

1288 Um diese Entscheidungsfreiheit zu illustrieren wird auf zwei Beispiele verwiesen: die Auszahlung des Lohns (dazu 3.6.1.2.1.2.3, S. 496) und die Kontrolle der Arbeitszeit.[1450]

1289 Zum einen stehe es dem Arbeitgeber prinzipiell frei, Vertrauensarbeitszeit anzuordnen oder stattdessen die Einhaltung der Arbeitszeit zu kontrollieren. Diese Entscheidung müsse im Rahmen von Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO grundsätzlich akzeptiert werden. Eine auf diese Entscheidung gestützte Weisung des Arbeitgebers, die Arbeitszeit aufzuzeichnen und die

1450 BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 62; *Thüsing,* NZA 2009, S. 865, 867; *Zöll,* in: Taeger/Gabel 2019, § 26 BDSG, Rn. 43.

damit verbundene Erhebung und Verarbeitung von Beschäftigtendaten könne also nicht dahingehend überprüft werden, ob es überhaupt erforderlich sei, die Einhaltung der Arbeitszeit zu kontrollieren oder es nicht vielmehr ausreichend wäre, Vertrauensarbeitszeit anzuordnen.[1451]

Dieses Beispiel überzeugt nicht durchgehend. Unerwähnt bleibt zum einem, dass Vertrauensarbeitszeit einer entsprechenden vertraglichen Regelung bedarf und der Verzicht auf Arbeitszeitkontrollen in einem Beschäftigungsverhältnis mit festen Arbeitszeiten darum von vornherein kein geeignetes Mittel ist, die arbeitsvertraglichen Pflichten zu kontrollieren.[1452] Darüber hinaus ist der Arbeitgeber für die Einhaltung des Arbeitszeitgesetzes verantwortlich, das u.a. Regelungen zu Höchstarbeitszeiten, Ruhepausen und Ruhezeiten trifft. Der Arbeitgeber ist gemäß § 16 Abs. 2 S. 1 ArbZG verpflichtet, die Arbeitszeit aufzuzeichnen, die über die gesetzlich vorgegebenen acht Stunden hinausgeht. Bereits hier wird die Leitungs- und Organisationsmacht des Arbeitgebers – und damit auch seine Zwecksetzungsbefugnis als Verantwortlicher – gesetzlich begrenzt. 1290

Darüber hinaus ist er verpflichtet, seinen Betrieb so zu organisieren, dass auch die übrigen, d.h. von der gesetzlichen Aufzeichnungspflicht in § 16 Abs. 2 S. 1 ArbZG nicht erfassten Vorgaben eingehalten werden. Dazu musste er nach der – mittlerweile überholten; dazu sogleich – Auffassung des Bundesarbeitsgerichts z.B. den täglichen Beginn und das Ende der Arbeitszeit sowie die Pausen zwar nicht aufzeichnen aber zumindest wahrnehmen.[1453] Daraus folgte, dass außerhalb der Aufzeichnungspflicht nach § 16 Abs. 2 S. 1 ArbZG keine allgemeine[1454] Pflicht bestand, personenbezogene Daten über die Arbeitszeit zu erheben. Gestützt auf sein Leitungs- 1291

1451 BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 62; *Thüsing,* NZA 2009, S. 865, 867.

1452 *Forst,* in: Auernhammer 2020, § 26 BDSG, Rn. 110.

1453 BAG v. 6.5.2003 – 1 ABR 13/02, E 106, S. 111, Rn. 65 (=NZA 2003, S. 1348). Aus dieser Auffassung folgte nicht zwingend, dass der Arbeitgeber Daten über die Arbeitszeit erheben musste. Trotz der Ausweitung des Anwendungsbereichs in § 26 Abs. 7 BDSG 2018 auf nichtautomatisierte und nicht dateisystembezogene Datenverarbeitung muss es sich für eine Datenverarbeitung wenigstens um Informationen handeln, die auf einem Datenträger fixiert werden – und sei es nur ein Blatt Papier (siehe 3.3.1.3.1, S. 320). Seine allgemeine Kontrollpflicht in Bezug auf die gesetzlichen Vorgaben zur Arbeitszeit würde der Arbeitgeber aber auch erfüllen, wenn die Informationen hierüber nicht fixiert würden, sondern lediglich „im Kopf" des Arbeitgebers bzw. seiner leitenden Mitarbeiter existierte. Dies allein wäre aber keine Datenverarbeitung.

1454 Eine weitere gesetzliche Grenze der Zwecksetzungsbefugnis des Arbeitgebers kann sich schließlich auch aus seinen Unterrichtungspflichten gegenüber dem Betriebsrat nach § 80 Abs. 1 Nr. 1, Abs. 2 S. 1 BetrVG ergeben. Wenn der Be-

und Organisationsrecht konnte der Arbeitgeber dies als unternehmerische Entscheidung aber anordnen. Dazu musste er nur plausibel darlegen, warum er dies für seinen unternehmerischen Erfolg für erforderlich hält. Da zu vermuten ist, dass seine Erfolgsaussichten steigen, wenn seine Beschäftigten tatsächlich entsprechend der vereinbarten Arbeitszeit für ihn arbeiten, dürfte dies nicht allzu schwergefallen sein. Entsprechend weit reicht die Zwecksetzungsbefugnis des Arbeitgebers im datenschutzrechtlichen Sinne.

1292 Nach der Rechtsprechung des Europäischen Gerichtshofs zu der dem Arbeitszeitgesetz zugrunde liegenden Arbeitszeitrichtlinie RL 2003/88/EG stellt sich die Situation mittlerweile viel klarer dar. Die Richtlinie sei so auszulegen, dass der Arbeitgeber verpflichtet ist, „ein objektives, verlässliches und zugängliches System einzuführen, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann."[1455] Anders ließe sich nicht gewährleisten, dass die in Art. 3, 5 und 6 lit. b ArbZ-RL und Art. 31 Abs. 2 GRC verankerten Rechte auf eine Begrenzung der Höchstarbeitszeit sowie auf tägliche und wöchentliche Ruhezeiten tatsächlich beachtet würden.[1456] Folglich besteht nun eine Pflicht zur Verarbeitung personenbezogener Arbeitszeitdaten, die als Zwecksetzung der Erforderlichkeitsprüfung nach Art. 6 Abs. 1 UAbs. 1 lit. b und Art. 5 Abs. 1 lit. c DS-GVO vorangestellt ist. Der Arbeitgeber kann sich zudem auf seine gesetzliche Aufzeichnungspflicht nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO i.V.m. der – europarechtskonform ausgestalteten – Regelung in § 16 Abs. 2 S. 1 ArbZG berufen.

3.6.1.2.1.2.3 Gängiges Beispiel 2: Art der Auszahlung des Arbeitsentgelts

1293 Das zweite Beispiel betrifft die Art der Auszahlung des Arbeitsentgelts. Die unternehmerische Freiheit erstrecke sich auch hierauf. Der Arbeitgeber

triebsrat bestimmte für seine Überwachungsaufgaben notwendige Informationen über die Arbeitszeit der einzelnen Beschäftigten anfordert, genügt es nicht, diese Informationen nur wahrzunehmen. Sie müssten dann auch als Daten erhoben und an den Betriebsrat (intern) weitergegeben werden, BAG v. 6.5.2003 – 1 ABR 13/02, E 106, S. 111, Rn. 65 (=NZA 2003, S. 1348).

1455 EuGH, ECLI:EU:C:2019:402, Rn. 60 – *CCOO/Deutsche Bank SAE*; zur Übertragung ins deutsche Recht *Ulber,* NZA 2019, S. 677, 680.

1456 EuGH, ECLI:EU:C:2019:402, Rn. 58 f. – *CCOO/Deutsche Bank SAE*.

müsse den Lohn nicht bar auszahlen, um dadurch die Verarbeitung der Kontodaten der Arbeitnehmer zu vermeiden.[1457]

Dieses Beispiel ist gänzlich verfehlt. Wie eine Geldleistung zu erfüllen ist, richtet sich nach der Vereinbarung der Vertragsparteien. Grundsätzlich ist in bar zu zahlen (siehe 3.4.1.4.8.1, S. 404). Dies kann in einem Tarifvertag oder im Arbeitsvertrag abweichend geregelt werden.[1458] Womöglich wird man angesichts der wohl nahezu lückenlos verbreiteten Praxis der unbaren Lohnauszahlung davon ausgehen können, dass dies in Arbeitsverträgen auch stets konkludent so geregelt ist. Es ist aber jedenfalls keine Frage, die der Arbeitgeber unter Berufung auf seine unternehmerische Freiheit einseitig regeln könnte. 1294

Das Weisungsrecht nach § 106 S. 1 GewO bezieht sich nur auf Inhalt, Ort und Zeit der Arbeitsleistung, also lediglich auf die Leistungspflicht des Arbeitnehmers. Es ist zwar durchaus möglich, dass sich ein Leistungsbestimmungsrecht nach § 315 BGB auf die eigene Leistung bezieht, etwa wenn der Arbeitgeber Bonuszahlungen bestimmen kann.[1459] Jedenfalls das allgemeine Weisungsrecht bezieht sich aber nicht auf die Leistungspflicht des Arbeitgebers.[1460] Wie er den Lohn auszahlt, unterliegt folglich nicht seiner datenschutzrechtlichen Zwecksetzungsbefugnis. 1295

3.6.1.2.1.3 Personelle Einzelmaßnahmen als Anhaltspunkt

Die genaue Reichweite der unternehmerischen Entscheidung und das Ausmaß ihrer gerichtlichen Kontrolle bei der Gestaltung datenschutzrelevanter Systeme im Beschäftigungsverhältnis wurden von der Rechtsprechung und der Literatur bislang nicht eingehend behandelt. Sie spielen aber auch in anderen Bereichen des Direktionsrechts eine entscheidende Rolle. Besonders intensiv sind diese Fragen für den Bereich personeller Einzelmaßnahmen diskutiert worden.[1461] Die Erkenntnisse aus dieser Diskussion sol- 1296

1457 BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 62; *Thüsing,* NZA 2009, S. 865, 866 f.
1458 *Hromadka/Maschmann* 2015, § 7 Rn. 12.
1459 Dazu z.B. BAG v. 19.3.2014 – 10 AZR 622/13, E 147, S. 332–341 (=NZA 2014, S. 595).
1460 *Hromadka/Maschmann* 2015, § 6 Rn. 7.
1461 Z.B. *Bayreuther,* NZA-Beil. 2006, S. 3–13; *Franzen,* NZA 2001, S. 805–812; *Preis,* NZA 1995, S. 241–250; *Quecke,* NZA 1999, S. 1247–1251.

len darum für die Bestimmung der Reichweite der unternehmerischen Entscheidung im Beschäftigtendatenschutz als Anhaltspunkte dienen.

3.6.1.2.1.3.1 Betriebliche Gründe

1297 Ähnlich wie bei der betriebsbedingten Kündigung nach § 1 Abs. 2 KSchG lässt sich die Prüfung einer personellen Einzelmaßnahme wie z.B. eine Versetzung in mehrere Phasen aufteilen. Am Beginn der Maßnahme stehen betriebliche Gründe, die den Arbeitgeber dazu veranlassen, eine Änderung der Organisation der Arbeit vorzunehmen. Beispiele hierfür sind der Wunsch nach einer Rationalisierung (innerbetrieblich) oder die Veränderung auf einem Absatzmarkt (außerbetrieblich).[1462]

1298 Für den Bereich der Assistenz- und Produktionssysteme könnte dies z.B. das Ziel sein, die Produktion zu flexibilisieren oder auf anspruchsvollere Kundenwünsche zu reagieren.

3.6.1.2.1.3.2 Unternehmerische Entscheidung

1299 Darauf folgt eine unternehmerische Entscheidung, wie auf diese betrieblichen Gründe im Einzelnen reagiert werden soll. Diese Entscheidungen beeinflussen als Teil der „Unternehmenspolitik“[1463] maßgeblich den wirtschaftlichen Erfolg des Unternehmens und sind insofern mit einem erheblichen Maß an Unsicherheit verbunden. Sie betreffen Fragen, „ob, was, wieviel, wo und mit welchen Methoden produziert wird“[1464], also auch die Einführung neuer Fertigungsmethoden oder organisatorischer Veränderungen.[1465]

1300 Bei solchen risikobehafteten Entscheidungen ist demjenigen ein Spielraum zuzugestehen, der das Risiko der Fehlentscheidung tragen muss – dem Arbeitgeber.[1466] Die unternehmerische Entscheidung kann darum vom Gericht nicht auf ihre sachliche Rechtfertigung oder ihre Zweckmäßigkeit

---

1462 BAG v. 7.12.1978 – 2 AZR 155/77, E 31, S. 157, Rn. 13 (=NJW 1979, S. 1902).
1463 BAG v. 19.5.1993 – 2 AZR 584/92, E 73, S. 151, Rn. 31 (=NZA 1993, S. 1075).
1464 *Hromadka/Maschmann* 2015, § 10 Rn. 194.
1465 *Hoyningen-Huene*, NZA 1994, S. 1009, 1010.
1466 BAG v. 21.6.1995 – 2 ABR 28/94, E 80, S. 185, Rn. 19 (=NZA 1995, S. 1157); BAG v. 17.6.1999 – 2 AZR 522/98, E 92, S. 61, Rn. 17 (=NZA 1999, S. 1095); BAG v. 26.9.2002 – 2 AZR 636/01, E 103, S. 31, Rn. 18 (=NZA 2003, S. 549).

überprüft werden, sondern nur darauf, ob sie offenbar unsachlich, unvernünftig oder willkürlich ist.[1467] Im Grunde beschränkt sich diese Kontrolle darauf, ob wirklich eine unternehmerische Entscheidung vorliegt oder die angeführten Gründe nicht vielmehr vorgeschoben sind,[1468] um eine umstrittene Maßnahme durchzusetzen. Wurde die Entscheidung tatsächlich umgesetzt, spricht eine Vermutung dafür, dass sie aus sachlichen Gründen getroffen wurde.[1469]

Im Vorfeld personeller Einzelmaßnahmen werden typischerweise unternehmerische Entscheidungen getroffen, die dazu führen, dass Arbeit nicht mehr in demselben Maße, am selben Ort oder in derselben Form wie bisher benötigt wird. So können etwa die Produktion gedrosselt oder die Arbeit intern neu organisiert und verdichtet oder an Dritte ausgelagert werden. Denkbar ist auch, dass ganze Qualifikationsebenen infolge der steigenden Automation wegfallen oder ausgedünnt werden. 1301

Nach diesen Grundsätzen steht es dem Arbeitgeber bis zur Grenze der Willkür auch frei, ob und welche Assistenzsysteme er in seinem Betrieb einsetzt. Die unternehmerische Entscheidung besteht hier darin, die Funktionen zu definieren, über die das Assistenzsystem verfügen soll, um die betrieblichen Ziele zu erreichen. Ob diese Funktionen zweckmäßig oder sachlich gerechtfertigt sind, kann das Gericht nicht kontrollieren. 1302

Bei den im ersten Kapitel angeführten Assistenzsystemen (siehe 1.3.2, S. 71) wäre dies z.B. die Fähigkeit, Mitarbeitern nur die im jeweiligen Kontext relevanten Informationen über die Produktion anzuzeigen oder die Möglichkeit, notwendige Arbeiten (z.B. die Reparatur an einer Maschine) automatisch zu erkennen und den dafür jeweils am besten geeigneten Mitarbeiter auszuwählen. 1303

3.6.1.2.1.3.3 Umsetzung der unternehmerischen Entscheidung

Wird die unternehmerische Entscheidung umgesetzt, führt sie dazu, dass die Beschäftigungsmöglichkeit insgesamt bzw. in der bisherigen Form oder am bisherigen Ort nicht mehr länger möglich ist. In einem Kündi- 1304

1467 BAG v. 21.9.2000 – 2 AZR 440/99, E 95, S. 350, Rn. 22 (=NZA 2001, S. 255); BAG v. 21.9.2006 – 2 AZR 607/05, NZA 2007, S. 431, 433 m.w.N.

1468 BAG v. 22.4.2004 – 2 AZR 385/03, E 110, S. 188, Rn. 19 (=NZA 2004, S. 1158); *Hromadka/Maschmann* 2015, § 10 Rn. 194a.

1469 BAG v. 20.6.2013 – 2 AZR 379/12, E 145, S. 265, Rn. 20 (=NZA 2014, S. 139).

gungsschutzprozess muss der Arbeitgeber diesen Effekt darlegen.[1470] Er muss also zeigen, dass z.B. infolge der Drosselung der Produktion, der Neuorganisation der Arbeit oder der Einführung neuer Fertigungsmethoden mehr Arbeitskräfte als (für sie geeignete) Arbeit vorhanden sind.

1305 Es genügt darum nicht, wenn sich der Arbeitgeber lediglich dazu entschlossen hat, Personal abzubauen. Die Kündigung ist selbst keine nur eingeschränkt überprüfbare unternehmerische Entscheidung, sondern kann nur die Folge einer solchen Entscheidung sein. Andernfalls würde die Vorgabe des § 1 KSchG leerlaufen, wonach es eines dringenden betrieblichen Erfordernisses bedarf, das einer Weiterbeschäftigung des Arbeitnehmers im Betrieb entgegensteht.[1471]

1306 Gleiches gilt für Organisationsentscheidungen, die wie z.B. die Auflösung einer Hierarchieebene, ohne nähere Konkretisierung nicht vom Kündigungsentschluss getrennt werden können. Werden abstrakte Organisationsstrukturen geändert, ohne dass damit eine Änderung der realen Abläufe einhergeht, weckt dies den Verdacht, dass hierdurch lediglich die Arbeitsbedingungen zum Nachteil des Arbeitgebers geändert werden sollen.[1472] Die Vermutung, dass eine durchgeführte unternehmerische Entscheidung aus sachlichen Gründen getroffen wurde, gilt hier nicht von vornherein. Der Arbeitgeber muss den Missbrauchsverdacht erst ausräumen, indem er seine Entscheidung so weit konkretisiert, dass der oben genannte Effekt – der Wegfall der Beschäftigungsmöglichkeit – nachgeprüft werden kann. Dazu müsste er z.B. darlegen, wer die Aufgaben, die in der nunmehr gestrichenen Hierarchieebene angesiedelt waren, übernimmt und wie dieser Aufgabenzuwachs bewältigt werden soll.[1473] Die Änderung der abstrakten Stellenstruktur muss mit anderen Worten notwendig sein,

---

1470 BAG v. 7.12.1978 – 2 AZR 155/77, E 31, S. 157, Rn. 17 f. (=NJW 1979, S. 1902); BAG v. 15.6.1989 – 2 AZR 600/88, NZA 1990, S. 65; vergleichbare Darlegungspflichten bestehen auch bei der Versetzung BAG v. 21.7.2009 – 9 AZR 404/08, NZA 2009, S. 1369, 1371 f.

1471 BAG v. 20.2.1986 – 2 AZR 212/85, NZA 1986, S. 822, 824; BAG v. 20.3.1986 – 2 AZR 294/85, NZA 1986, S. 824, 825; BAG v. 26.9.2002 – 2 AZR 636/01, E 103, S. 31, Rn. 20 (=NZA 2003, S. 549).

1472 BAG v. 26.9.2002 – 2 AZR 636/01, E 103, S. 31, Rn. 22 (=NZA 2003, S. 549); BAG v. 22.4.2004 – 2 AZR 385/03, E 110, S. 188, Rn. 18 (=NZA 2004, S. 1158).

1473 BAG v. 17.6.1999 – 2 AZR 522/98, E 92, S. 61, Rn. 20 (=NZA 1999, S. 1095); BAG v. 26.9.2002 – 2 AZR 636/01, E 103, S. 31, Rn. 20 (=NZA 2003, S. 549); BAG v. 13.2.2008 – 2 AZR 1041/06, NZA 2008, S. 819, 820.

um die realen Ablaufänderungen abzubilden. Was den Arbeitgeber zu dieser Ablaufänderung bewogen hat, ist dagegen unerheblich.[1474]

3.6.1.2.1.4 Strenger Ansatz zur Abgrenzung bei Assistenzsystemen

Dieser Ansatz zur Reichweite der unternehmerischen Entscheidung ließe sich prinzipiell auch auf den Beschäftigtendatenschutz übertragen. Demnach wäre der Entschluss allein, personenbezogene Beschäftigtendaten zu verarbeiten, unerheblich und könnte einen entsprechenden Datenumgang nicht rechtfertigen. Um zu dieser Erkenntnis zu gelangen, bedürfte es jedoch keiner Parallelerwägungen aus dem Kündigungsschutzrecht, sie ergibt sich bereits unmittelbar aus Grundsätzen des Datenschutzes selbst. Andernfalls würde nämlich das Erforderlichkeitsprinzip leerlaufen (siehe 3.4.1.4.2.3, S. 394). 1307

3.6.1.2.1.4.1 Ansatz zur Missbrauchskontrolle

Weit weniger klar ist, wie mit Entscheidungen umzugehen ist, die zwar für sich genommen eine Organisationsentscheidung darstellen, praktisch aber mit dem Entschluss zum Datenumgang zusammenfallen. Fraglich ist also, ob es auch im Beschäftigtendatenschutzrecht eines dem Kündigungsschutzrecht vergleichbaren Mechanismus zur Missbrauchskontrolle bedarf. 1308

Befürwortete man dies, müsste zwischen den Funktionen eines Assistenzsystems in zwei Kategorien unterschieden werden, mit denen eine jeweils andere Darlegungslast verbunden wäre. Zur ersten Kategorie zählten die Funktionen eines Assistenzsystems, die sich unmittelbar auf die tatsächlichen Abläufe im Betrieb auswirkten, etwa, weil mit ihnen die Arbeit durchgeführt oder organisiert wird. Für sie gälte die Vermutung, aus sachlichen Gründen getroffen worden zu sein. 1309

Zur zweiten Kategorie zählten datenschutzrelevante Funktionen wie die Personalisierbarkeit eines Systems, die sich nur mittelbar auf die tatsächlichen Abläufe im Betrieb auswirkten, weil sie die unmittelbar wirkenden Funktionen nur verbessern sollen. Sie wären von der Vermutung ausge- 1310

1474 *Franzen*, NZA 2001, S. 805, 810 f., der den Ansatz, die Prüfung an der Sachlichkeit der Entscheidung festzumachen jedoch für verfehlt hält. Die unternehmerische Entscheidung sei nicht die Änderung der Organisationsstruktur, sondern die der tatsächlichen Abläufe; so auch *Quecke*, NZA 1999, S. 1247, 1249.

nommen, weil der Entschluss, sie einzuführen, einer Entscheidung über den Umgang mit personenbezogenen Beschäftigtendaten gleichkäme. Der Arbeitgeber müsste stattdessen darlegen, inwiefern diese nur mittelbar wirkenden Funktionen mit einer tatsächlichen Änderung der betrieblichen Abläufe hinterlegt sind, inwiefern die mittelbar wirkenden Funktionen also notwendig sind, um die unmittelbar wirkenden Funktionen zu ermöglichen. Ob diese erste Kategorie an Funktionen wiederum erforderlich ist, um die betrieblichen Ziele zu erreichen, würde hingegen nicht geprüft. Eine Zweckmäßigkeitskontrolle dieser unternehmerischen Entscheidung findet (siehe 3.6.1.2.1.3.2, S. 498) gerade nicht statt.

3.6.1.2.1.4.2 Beispiele

1311 Um die Konsequenzen dieser Auslegung zu verdeutlichen, sollen die oben erwähnten Beispiele (siehe 3.4.1.4.1.2, S. 390) wieder aufgegriffen werden.

- Bei einem System, das Arbeitnehmern kontextsensitiv die relevanten Informationen zur Produktion einblenden soll, kommt es maßgeblich darauf an, anhand welcher Merkmale der Kontext bestimmt wird. Um zu diesen Merkmalen auch Informationen über den Beschäftigten mit hinzuzunehmen – etwa seine räumliche Position in der Fabrik, sein bisheriger Erfahrungs- und Wissensstand, seine Nutzungspräferenzen oder die Aufträge, die er als nächstes zu erledigen hat – genügte es nicht, dass der Arbeitgeber dies für sinnvoll erachtet. Er müsste vielmehr darlegen, dass die Einbeziehung einer personenbezogenen Komponente in den Kontext notwendig ist, um die von ihm gewünschte situative Passgenauigkeit und Qualität der Information zu erreichen.
- Bei einem System, welches automatisch Arbeitsaufträge (z.B. die Reparatur eines Defekts einer Maschine) ermittelt und sie unter den Beschäftigten in der Fabrik verteilt, ist es durchaus denkbar, Informationen über die einzelnen Mitarbeiter in die Entscheidung einfließen zu lassen, wem von ihnen der Auftrag erteilt wird. Dies können z.B. seine zeitliche Verfügbarkeit oder die zurückzulegende Wegstrecke zum Einsatzort sein oder die Güte und Schnelligkeit, mit der er bisher vergleichbare Aufgaben erfüllt hat. Die Aufgabe könnte aber auch schlicht an den nächsten freien Mitarbeiter vergeben werden – unabhängig davon, wo er sich befindet und als wie kompetent er sich in der Vergangenheit erwiesen hat. Auch hier müsste der Arbeitgeber darlegen, inwiefern die Berücksichtigung der personenbezogenen Angaben erforderlich ist, um die gewünschte Qualität der Auswahl der für eine Auf-

gabe in Frage kommenden Mitarbeiter zu erreichen. Dass dies durchaus plausibel erscheint, würde insofern nicht ausreichen.

– Bei einem Leichtbauroboter, der direkt mit dem Beschäftigten interagiert und ihm schwere Lasten abnimmt oder diese besser positioniert, kann es darauf ankommen, Daten über den mit dem Roboter interagierenden Beschäftigten zu verarbeiten, etwa seine Körpergröße oder seine Position zur Maschine im Raum. Hier ist fraglich, ob sich die damit intendierte Senkung der körperlichen Belastung und die Optimierung des Produktionsablaufs nicht auch durch herkömmliche Methoden wie den Einsatz manuell bedienter Hebebühnen oder am Körper getragener „passiver" Exoskelette, die statt sensorgesteuerter Motorik nur Federmechanismen einsetzen, erreicht werden kann.[1475] Da bei diesen alternativen Methoden keine Beschäftigtendaten verarbeitet würden, müsste der Arbeitgeber darlegen, inwiefern durch den Einsatz des Leichtbauroboters die physische Belastung der Mitarbeiter erheblich gesenkt und das arbeitstechnische Ziel besser oder unter effizienter erreicht werden kann.

3.6.1.2.1.5 Eingeschränkte Übertragbarkeit der Missbrauchskontrolle

Es sprechen jedoch auch gute Gründe gegen eine solch umfangreiche Kontrolle der unternehmerischen Entscheidung. 1312

So enthält das Datenschutzrecht eigene Instrumente zur Missbrauchsbekämpfung. Anders als bei einer Kündigung handelt es sich beim Umgang mit Beschäftigtendaten nicht um eine einmalige Maßnahme. Wäre eine Kündigung aus vorgeschobenen Motiven wirksam, hätte der Arbeitgeber sein Ziel, sich von dem Arbeitnehmer zu trennen, bereits erreicht. Dagegen müsste er – selbst, wenn es ihm gelänge, unter Angabe vorgeschobener Zwecke personenbezogene Beschäftigtendaten zu erheben und zu speichern – diese Daten noch zu seinen eigentlichen Zwecken auswerten. 1313

1475 Eine solche Prüfung nehmen *Martini/Botta*, NZA 2018, S. 625, 630 vor. In ihrem Beispiel „aktiver", d.h. mit Sensorik ausgestattete Exoskelette, kommt zwar noch hinzu, dass diese aktiven Systeme vor allem Gesundheitsdaten der Beschäftigten nach Art. 9 Abs. 1 DS-GVO verarbeiten, etwa um sich der Belastung ihrer Bediener anzupassen. Sowohl nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO als auch nach Art. 9 Abs. 2 lit. b DS-GVO i.V.m. § 26 Abs. 3 BDSG 2018 kommt es für die Zulässigkeit der Datenverarbeitung aber im Kern darauf an, ob sie zur Erfüllung vertraglicher Pflichten aus dem Arbeitsvertrag erforderlich ist.

Hieran wäre er durch das Prinzip der Zweckbindung (siehe 3.4.1.2, S. 355) gehindert. Dies mag für einen auf eine solche Weise vorgehenden Arbeitgeber keine unüberwindbare Hürde sein und es rechtfertigte auch nicht, die Zulässigkeit der Datenerhebung praktisch ins Belieben des Arbeitgebers zu stellen. Es stellt aber nichtsdestotrotz einen nicht unerheblichen Unterschied zur Situation bei Kündigung eines Arbeitnehmers dar.

1314 Vor allem aber sind die Rahmenbedingungen in beiden Fällen nicht vergleichbar. Die Einführung von Assistenzsystemen betrifft das Direktionsrecht des Arbeitgebers. Anders als im Kündigungsrecht versucht er bei der Ausübung seines Direktionsrechts nicht, die vertragliche Grundlage der Zusammenarbeit mit dem Arbeitnehmer aufzulösen oder – im Falle der Änderungskündigung – einseitig zu seinen Gunsten zu ändern. Er bewegt sich vielmehr im Bereich des gemeinsam Vereinbarten und nimmt darin sein dem Arbeitsverhältnis inhärentes Leistungsbestimmungsrecht wahr.[1476]

1315 Nach der Rechtsprechung des Bundesarbeitsgerichts können die Grundsätze der Missbrauchskontrolle darum nicht auf die einer Weisung zugrundeliegende unternehmerische Entscheidung ausgedehnt werden.[1477] Der konkrete Fall betraf eine Versetzung an einem bestimmten Standort einer Fluggesellschaft, der notwendig wurde, weil die bisherige Station geschlossen wurde. Da die unternehmerische Entscheidung zur Stationsschließung deckungsgleich mit der Versetzung der dort bisher stationierten Mitarbeiter war, verlangte die Vorinstanz vom Arbeitgeber, die Nachhaltigkeit und Dauerhaftigkeit dieser Entscheidung durch weiteren Tatsachenvortrag zu verdeutlichen. Damit sollte sichergestellt werden, dass der Arbeitgeber nicht lediglich auf vorübergehende Marktschwankungen reagiert und dieses – grundsätzlich von ihm zu tragende – Risiko auf dem Arbeitnehmer verschiebt.[1478] Nach der Ansicht des Bundesarbeitsgerichts genügt es für die Sachlichkeit der Entscheidung dagegen, dass die Stationierungsentscheidung durch die Versetzung mehrerer anderer Mitarbeiter bereits umgesetzt wurde. Einen besonderen Beleg für die Nachhaltigkeit dieser Entscheidung verlangte es nicht.

1476 BAG v. 26.9.2012 – 10 AZR 412/11, AP GewO § 106 Nr. 22, Rn. 37 (=NJOZ 2013, S. 457); anders davor LAG Hessen v. 28.3.2011 – 17 Sa 1033/10, Rn. 67.

1477 BAG v. 26.9.2012 – 10 AZR 412/11, AP GewO § 106 Nr. 22, Rn. 37 (=NJOZ 2013, S. 457); ähnlich auch schon *Bayreuther,* NZA-Beil. 2006, S. 3, 7 f. anders davor LAG Hessen v. 28.3.2011 – 17 Sa 1033/10, Rn. 67.

1478 LAG Hessen v. 28.3.2011 – 17 Sa 1033/10, Rn. 67 ff.

Innerhalb seines Direktionsrechts ist dem Arbeitgeber demnach ein besonders weitreichender Spielraum hinsichtlich seiner unternehmerischen Entscheidungen zuzugestehen. Eine Missbrauchskontrolle ähnlich der im Kündigungsrecht findet nicht statt. Der Arbeitnehmer räumt dem Arbeitgeber durch die arbeitsvertragliche Vereinbarung einen größeren Zugriff auf grundrechtlich geschützte Positionen ein, als dies außerhalb dieses Rahmens möglich wäre.[1479] Entsprechend gilt der Entscheidungsspielraum auch dann, wenn die unternehmerische Entscheidung die grundrechtsbeeinträchtigende Maßnahme bereits im Grundsatz vorwegnimmt. 1316

3.6.1.2.1.6 Ergebnis: Weiter Ansatz zur Abgrenzung bei Assistenzsystemen

Spiegelt man diese Entscheidung auf die Gestaltung von Assistenzsystemen, lässt sich die eben angeregte Kategorienbildung (siehe 3.6.1.2.1.4.1, S. 501) nicht halten. Der Arbeitgeber kann zwar nicht einfach beschließen, personenbezogene Beschäftigtendaten zu erheben oder zu verwenden. Die unternehmerische Entscheidung betrifft nicht den Datenumgang selbst; er ist nur zulässig, soweit dies für die Umsetzung der unternehmerischen Entscheidung erforderlich ist. Der Arbeitgeber kann dem Assistenzsystem aber Funktionen hinzufügen, die – wie z.B. die Personalisierbarkeit des Systems – auf den Umgang mit personenbezogenen Beschäftigtendaten hinauslaufen.[1480] Die Definition solcher Funktionen selbst unterliegt nicht dem strengen Erforderlichkeitsprinzip, sondern ist lediglich auf Plausibilität und Willkürfreiheit zu prüfen (siehe 2.4.4.1, S. 193). 1317

An den oben (3.6.1.2.1.4, S. 501) genannten Beispielen kann dieser Ansatz wie folgt verdeutlicht werden: 1318

– Bei einem System zur Einblendung kontextsensitiver Informationen umfasst der Entscheidungsspielraum des Arbeitgebers auch die Frage, ob bei der Bestimmung des Kontexts Informationen über den Arbeitnehmer berücksichtigt werden sollen. Soweit dies in dem konkreten Fall plausibel erscheint, könnte er also z.B. auch den Standort des Beschäftigten, dessen bisherigen Erfahrungs- und Wissenstand, dessen

1479 Zur Bedeutung der Grundrechte im Kündigungsrecht, BAG v. 26.9.2002 – 2 AZR 636/01, E 103, S. 31, Rn. 19 (=NZA 2003, S. 549); *Preis,* NZA 1995, S. 241, 242; *Reuter,* RdA 2004, S. 161, 163 ff., m.w.N.; zur Wirkung im Beschäftigungsverhältnis allgemein, siehe 2.4.6.2, S. 204.

1480 In Bezug auf Maßnahmen zum Arbeitsschutz *Thüsing* 2014, S. 58 f.

Nutzungspräferenzen oder noch zu erledigenden Aufträge miteinbeziehen.
- Bei einem System zur automatischen Erfassung und Verteilung von Aufträgen könnte der Arbeitgeber auch Informationen über den einzelnen Mitarbeiter in die Entscheidung miteinfließen lassen. Plausibilität im konkreten Fall vorausgesetzt, könnte er also auch dessen zeitliche Verfügbarkeit, die bis zum konkreten Arbeitsort zurückzulegende Strecke oder das Niveau der einschlägigen Fähigkeiten des Beschäftigten berücksichtigen.
- Bei dem Leichtbauroboter könnte der Arbeitgeber dessen Fähigkeit zur unmittelbaren Interaktion mit dem unterstützten Beschäftigten als notwendige Funktion definieren. Es muss nur plausibel sein, dass hierdurch die Arbeit weniger belastend und effizienter gestaltet werden kann. Systeme, die über diese Funktionalität nicht verfügen, sind schon von vornherein nicht gleich geeignet und damit in der Erforderlichkeitsprüfung i.e.S. nicht zu berücksichtigen.[1481]

1319 Dieser Ansatz deckt sich auch mit den wenigen bisher genannten Beispielen für den Entscheidungsspielraum des Arbeitgebers. Hierfür wird z.B. die Frage angeführt, ob Mitarbeiter als Ausweis besonderer Kundenfreundlichkeit Namensschilder tragen sollen.[1482] Gern genannt wird auch die Frage, ob die Arbeitszeit der Beschäftigten kontrolliert oder vielmehr auf Vertrauensarbeit gesetzt werden sollte (siehe 3.6.1.2.1.2.2, S. 494). Diese unternehmerischen Entscheidungen nehmen den Datenumgang in Grundsatz bereits vorweg. Der Arbeitgeber muss aber trotzdem nicht im Einzelnen darlegen, inwiefern das Tragen von Namensschildern für die Erreichung seines Ziels, Kundenfreundlichkeit zu demonstrieren, erforderlich ist, und ob er nicht ebenso gut ohne diese Maßnahme am Markt bestehen könnte. Das Gleiche gilt für die Kontrolle der Arbeitszeit, bei der der Arbeitgeber nicht darauf verwiesen werden kann, seine unternehmerischen Ziele durch Vertrauensarbeit zu erreichen.

3.6.1.2.2 Konkrete Umsetzung nach dem Erforderlichkeitsprinzip

1320 Die Analyse hat gezeigt, dass die Festlegung der Funktionalität eines Assistenz- und Produktionssystems zur nur eingeschränkt kontrollierbaren Zwecksetzungsbefugnis des Arbeitgebers zählt. In diesem Rahmen kann er

1481 A.A. *Martini/Botta,* NZA 2018, S. 625, 630.
1482 *Deutsch/Diller,* DB 2009, S. 1462, 1463.

sich auf seine unternehmerische Freiheit berufen und muss lediglich plausibel darlegen, dass diese Funktionen zum Unternehmenserfolg beitragen.

Für die konkrete Umsetzung dieser Funktionen ist dem Arbeitgeber hingegen kein Spielraum mehr zu gewähren. Es ist darauf zu achten, dass sich die Gestaltung eines datenschutzrelevanten Systems an dem mit ihrem Einsatz verfolgten Zweck sowie den betrieblichen Gegebenheiten ausrichtet – und nicht umgekehrt. Die Zwecksetzungsbefugnis des Arbeitgebers reicht nicht so weit, dass er den Zweck z.B. auf die Arbeitszeitkontrolle mit einem bestimmten Zeiterfassungssystem oder einer bestimmten Methode konkretisieren dürfte.[1483] Andernfalls würden Beschäftigtendaten nicht deswegen erhoben, verarbeitet und genutzt, weil dies zur Zweckerreichung erforderlich ist, sondern weil es in der konkreten Systemgestaltung so vorgesehen ist (siehe 3.4.1.4.2.3, S. 394). Eine solch weitreichende Zweckkonkretisierung würde den Datenumgang zum Selbstzweck erklären und das Erforderlichkeitsprinzip aushebeln. 1321

Die Reichweite der Zwecksetzungsbefugnis endet bei Assistenzsystemen demnach bei der Festlegung der – u.U. auch datenschutzrelevanten – Funktionen, über die es zur Erreichung der unternehmerischen Ziele verfügen soll. Wie diese Funktion konkret umgesetzt wird, insbesondere in welchem Umfang dafür personenbezogenen Daten erhoben werden, wie lange sie gespeichert bleiben und wer darauf Zugriff hat, richtet sich nach dem Erforderlichkeitsprinzip. Auch technische Gestaltungsansätze wie z.B., ob für eine bestimmte Funktion die Daten permanent oder anlassbezogen erfasst werden oder ob dies bei einer zentralen Instanz oder dezentral durch die (mobilen) Geräte der Mitarbeiter geschieht, zählen zu den Umsetzungsfragen. 1322

Von der Zwecksetzungsbefugnis ebenfalls nicht mehr erfasst ist die Frage, ob der Datenumgang unter Einsatz von Datenverarbeitungsanlagen stattfindet.[1484] Beim Einsatz von Assistenzsystemen dürfte ihr jedoch keine praktische Bedeutung zukommen, weil sich die vom Arbeitgeber angestrebten Funktionen auf eine „analoge“ Weise nicht realisieren lassen dürften. Der Hinweis auf hergebrachte Methoden verfängt darum – wenn überhaupt – nur in den wenigsten Situationen.[1485] Das Bundesarbeitsgericht hat es jedenfalls in den Fällen, in denen der Arbeitgeber technische Hilfsmittel zum Datenumgang verwendet hat, bei solch allgemeinen Aus- 1323

1483 *Erfurth,* NJOZ 2009, S. 2914, 2918.
1484 So auch *Schmitz* 2016, S. 199.
1485 So aber *Steidle,* MMR 2009, S. 167, 170.

sagen zu deren besserer Eignung belassen und die Gleichwertigkeit einer „analogen" Methode nicht ernsthaft in Erwägung gezogen (siehe auch 3.4.1.3.3.2, S. 377).[1486] Insofern hat der Arbeitgeber hier ebenfalls einen – wenn auch rein faktischen – Entscheidungsspielraum.

3.6.1.2.3 Angemessenheit der Datenverarbeitung

1324 Die Angemessenheit der Datenverarbeitung ist – im Beschäftigtendatenschutz nicht anders als im sonstigen Datenschutzrecht – stark einzelfallbezogen zu bewerten, sodass nur wenige generalisierende Aussagen getroffen werden können. Vieles hängt vom konkreten Schutzbedarf der Daten und der spezifischen Bedrohungslage für die Rechte des Betroffenen ab. Im weiteren Verlauf der Untersuchung soll die Prüfung darum anhand von spezifischen Verarbeitungssituationen typisiert werden (dazu 3.6.2, S. 525). Unabhängig von diesen Kriterien lassen sich aber einige Leitlinien und Grenzen erkennen, die in allen Situationen gelten. Eine herausgehobene Bedeutung kommt dabei der Art des Zwecks zu, zu dem die Daten in der jeweiligen Situation verarbeitet werden sollen.

3.6.1.2.3.1 Unterscheidung nach der Art des Zwecks

1325 Die verschiedenen Zwecke, die sich mit Assistenz- und Produktionssystemen der Industrie 4.0 verfolgen lassen, können grob in die *Einsichtnahme* zur Organisation betrieblicher Abläufe einerseits und die *Kontrolle* von Leistung oder Verhalten andererseits eingeteilt werden.[1487]

3.6.1.2.3.1.1 Einsichtnahme

1326 Die Einsichtnahme in die Tätigkeit des Arbeitnehmers durch den Arbeitgeber ist der arbeitsteiligen Organisation des Betriebs geschuldet und insofern ein Phänomen, das so gut wie jeder Arbeit innewohnt. Die Industrie 4.0 hebt sich hier nur insofern ab, dass die Datenverarbeitung deutlich feingranularer und umfangreicher erfolgen kann. Die Datenverarbeitung

---

1486 BAG v. 11.3.1986 – 1 ABR 12/84, E 51, S. 217, Rn. 37 (=NZA 1986, S. 526); BAG v. 22.10.1986 – 5 AZR 660/85, E 53, S. 226, Rn. 37 (=NZA 1987, S. 415).

1487 Mit dieser Einteilung auch *Steidle* 2005, S. 258.

wird hier in der Regel durch fachlich nahestehende Mitarbeiter durchgeführt und dient dazu, die betrieblichen Abläufe zu organisieren und die jeweilige Arbeitsaufgabe zu erfüllen. Die Verarbeitung seiner Daten hat für den einzelnen Beschäftigten allenfalls zur Folge, dass ihm eine bestimmte Tätigkeit zugewiesen wird oder er an einer Schulung teilnehmen muss.[1488]

1327 Nach den oben erörterten Kriterien (siehe 3.2.3.5, S. 299) greifen Maßnahmen zur Einsichtnahme in der Regel nicht sonderlich tief in die Rechte der Beschäftigten ein. Es ist zwar anzunehmen, dass viele Beschäftigte von solchen Maßnahmen betroffen sein werden (siehe 3.2.3.5.4, S. 304). Für den Beschäftigten ergeben sich aus der Datenverarbeitung aber keine wirtschaftlichen Folgen, die sich gravierend auf andere Grundrechte und Lebensbereiche auswirken könnten (siehe 3.2.3.5.6, S. 306). Die Eingriffstiefe ist darum in der Terminologie der Risikoanalyse, wie sie z.B. in Art. 25 Abs. 1 DS-GVO vorgenommen werden muss (siehe 3.4.2.2.4.4, S. 443) als grundsätzlich normal einzustufen. Hinzu kommt, dass hinter der besseren Organisation der Arbeit ein starkes und darüber hinaus unmittelbar einsichtiges wirtschaftliches Interesse des Arbeitgebers steht.[1489] Die Abwägung dürfte darum hier für den Verarbeiter tendenziell positiv ausgehen.

3.6.1.2.3.1.2 Kontrolle

1328 Bei der Kontrolle werden die Daten der Beschäftigten mit dem Ziel verarbeitet, daraus arbeitsrechtliche Konsequenzen abzuleiten, also etwa eine Kündigung auszusprechen, eine Versetzung anzuweisen, aber auch eine Beförderung anzubieten. Dabei können die Kontrollmaßnahmen sowohl die Leistung des einzelnen Beschäftigten als auch sein Verhalten betreffen. Durchgeführt wird die Datenverarbeitung in der Regel in der Personalabteilung und zumindest von Stellen, die über die genannten arbeitsrechtlichen Kompetenzen verfügen.

1329 Maßnahmen zur Kontrolle der Arbeitnehmer greifen im Vergleich zu solchen zur Einsichtnahme tiefer in deren Rechte nach Art. 1 Abs. 2 DS-GVO

1488 So i.E. BAG v. 17.11.2016 – 2 AZR 730/15, NZA 2017, S. 394, Rn. 35 Bei der Entscheidung wird u.a. berücksichtigt, dass die Daten nur für Schulungsmaßnahmen, nicht aber z.B. für Kündigungen herangezogen werden dürfen.

1489 Zur Kraftstoffersparnis und zum Komfortgewinn für die Fahrgäste bei einem Assistenzsystem für Busfahrer BAG v. 17.11.2016 – 2 AZR 730/15, NZA 2017, S. 394, Rn. 32. Zur Nachvollziehbarkeit bei Datenbankeingaben LAG Köln v. 29.9.2014 – 2 Sa 181/14, NZA-RR 2015, S. 128, 130.

ein. Dies ergibt sich bereits aus den möglichen arbeitsrechtlichen Konsequenzen, welche jedenfalls die Berufsfreiheit der Arbeitnehmer betreffen und deren wirtschaftliche Existenz gefährden kann, was wiederum auf andere Lebensbereiche ausstrahlt (siehe 3.2.3.5.6, S. 306). Bezogen auf die Risikoanalyse (siehe 3.4.2.2.4.4, S. 443) kann ein Kontrollzweck darum dazu beitragen, dass der Eingriff als schwerwiegend und das Risiko entsprechend als hoch einzustufen ist.

1330 Das Interesse des Arbeitgebers an Leistungs- und Verhaltenskontrollen ist nicht per se geringer als dasjenige an der Organisation der Arbeit zu bewerten. Als Gläubiger der Leistungspflicht ist der Arbeitgeber berechtigt, deren Erbringung zu überwachen (siehe 2.4.6.2, S. 204).[1490] Hinzu kommt, dass sich der Arbeitgeber im Rahmen der Personalplanung in regelmäßigen Abständen ein Bild vom Leistungsstand der Beschäftigten verschaffen muss. Es kann ihm folglich nicht bereits prinzipiell verwehrt werden, Daten zu erheben, anhand derer er die Leistung des einzelnen Beschäftigten beurteilen kann.[1491] Das kann sowohl die Leistungsfähigkeit als auch die Leistungsbereitschaft[1492] betreffen.

3.6.1.2.3.2 Kontrollfreie Räume

1331 Als letzte allgemeine Anforderung muss die Datenverarbeitung den Beschäftigten kontrollfreie Räume lassen. Dies gilt sowohl im wörtlichen Sinne, weil sich die Verarbeitung nicht auf geschützte Lebensbereiche beziehen darf, als auch im übertragenen Sinne, weil die Verarbeitung auch außerhalb dieser speziell geschützten Bereiche nicht umfassend sein darf.

1332 Zu den geschützten Räumen der Beschäftigten zählt zuallererst deren Privatleben, also private Räume oder Gegenstände, aber auch sämtliches Verhalten außerhalb des Beschäftigungsverhältnisses.[1493] Der Arbeitgeber

---

1490 BAG v. 27.5.1986 – 1 ABR 48/84, E 52, S. 88, Rn. 50 (=NZA 1986, S. 643); BAG v. 13.1.1987 – 1 AZR 267/85, E 54, S. 67, Rn. 46 (=NZA 1987, S. 515).

1491 Allgemein BAG v. 28.3.1979 – 5 AZR 80/77, AP BPersVG § 75 Nr. 3 (=DB 1979, S. 1703); BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 117. Zur Mithören bei Callcenter-Mitarbeitern während der Probezeit BAG v. 30.8.1995 – 1 ABR 4/95, NZA 1996, S. 218, 221.

1492 Zur Speicherung unentschuldigter Fehlzeiten BAG v. 11.3.1986 – 1 ABR 12/84, E 51, S. 217, Rn. 39 ff. (=NZA 1986, S. 526).

1493 BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 120; zur Ortung *Forst,* in: Auernhammer 2020, § 26 BDSG, Rn. 112; *Gola,* NZA 2007, S. 1139, 1144; *Gola,* ZD 2012, S. 308, 310; *Göpfert/Papst,* DB 2016, S. 1015, 1018.

kann hier allenfalls zur Sicherung seines Eigentums[1494] sowie zur Aufdeckung massiver Pflichtverletzungen[1495] vorgehen, also im Grunde kaum anders als jeder andere Geschädigte auch.[1496] Da die zulässigen Verarbeitungsmöglichkeiten hier äußerst begrenzt sind, ergeben sich keine Besonderheiten für die Industrie 4.0. Darüber hinaus müssen auch Räume auf dem Betriebsgelände des Arbeitgebers, die besonders geschützten Lebensbereichen gewidmet sind (z.B. Pausen-, Sanitär- oder private Räume), von jeglicher Überwachung ausgenommen werden.[1497] Mobile Assistenzsysteme, welche nicht nur die Interaktion mit dem betroffenen Beschäftigten – die er selbst unterlassen kann –, sondern auch seine Umgebung aufzeichnen, dürfen in diesen Räumen nicht aktiv sein.

Der Schutz vor umfassender Datenverarbeitung ist überdies inhaltlich gegen eine lückenlose Totalüberwachung gerichtet[1498] und bezieht sich auch auf Parameter, die der Arbeitgeber einzeln im Wesentlichen ohne Weiteres verarbeiten dürfte.[1499] Die besondere Beeinträchtigung des Beschäftigten ergibt sich hier nicht aus der Qualität, sondern aus der Quantität der Daten.[1500] Selbst die Datenerhebung über die Arbeitsleistung und das Arbeitsverhalten können unter diesen Umständen einen erheblichen Anpassungs- 1333

1494 Zu Taschenkontrollen BAG v. 15.4.2014 – 1 ABR 2/13 (B), E 148, S. 26, Rn. 44 ff. (=NZA 2014, S. 551) Handelsübliche mobile Endgeräte dürften jedoch in der Regel nicht wertvoll genug sein, um eine Überwachung zu rechtfertigen, *Forst,* in: Auernhammer 2020, § 26 BDSG, S. 113.

1495 Zum Detektiveinsatz bei vorgetäuschter Arbeitsunfähigkeit und unerlaubter Konkurrenztätigkeit, BAG v. 29.6.2017 – 2 AZR 597/16, E 159, S. 278, Rn. 30 ff. (=NZA 2017, S. 1179).

1496 Zum Detektiveinsatz allgemein BGH v. 4.6.2013 – 1 StR 32/13, St 58, S. 268, Rn. 92 (=NJW 2013, S. 2530).

1497 Zur Videoüberwachung *Däubler,* NZA 2017, S. 1481, 1484; zur Ortung *Forst,* in: Auernhammer 2020, § 26 BDSG, Rn. 113; *Roßnagel, et al.* 2006, S. 107 f.

1498 *Kort,* RdA 2018, S. 24, 25; *Wedde,* in: Däubler et al. 2020, § 26 BDSG, Rn. 119; *Weichert,* NZA 2017, 565–570, 567; in Bezug auf die Ortung von Beschäftigten *Dehmel/Diekmann,* PinG 2016, S. 141, 144; *Gola,* ZD 2012, S. 308, 310; *Hofmann/Hornung* 2018, S. 242.

1499 BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 37 (=NZA 2017, S. 1205); BAG v. 27.7.2017 – 2 AZR 681/16, E 159, S. 380, Rn. 29 ff. (=NZA 2017, S. 1327); ArbG Berlin, ECLI:DE:ARBGBE:2017:0810.41CA12115.16.00, Rn. 112 ff. *Hofmann,* ZD 2016, S. 12, 16 In die Richtung auch *Martini/Botta,* NZA 2018, S. 625, 630.

1500 BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 32 (=NZA 2017, S. 1205); BAG v. 27.7.2017 – 2 AZR 681/16, E 159, S. 380, Rn. 33 (=NZA 2017, S. 1327). Das Bundesarbeitsgericht zieht seine Rechtsprechung zur Videoüberwachung (BAG v. 26.8.2008 – 1 ABR 16/07, E 127, S. 276–297 (=NZA 2008, S. 1187);

druck erzeugen, der den Beschäftigten übermäßig in seiner Entfaltungsfreiheit einschränkt.[1501]

3.6.1.3 Datenverarbeitung zur Wahrung berechtigter Interessen

1334 Eine Datenverarbeitung kann nur auf Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO gestützt werden, wenn sich ihr Zweck aus den vertraglichen Pflichten des Beschäftigungsverhältnisses ergibt. Diese Norm entfaltet für das Verhältnis von Arbeitgeber zu Beschäftigten aber keine abschließende Wirkung (siehe 3.6.1.1, S. 485), sodass sich der Arbeitgeber für andere Zwecke auch auf die übrigen Erlaubnistatbestände in Art. 6 Abs. 1 UAbs. 1 DS-GVO stützen kann, insbesondere auf die Generalklausel in Buchstabe f.

3.6.1.3.1 Abgrenzung

1335 Die Generalklausel in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO wird durch die speziellen Erlaubnistatbestände in deren Anwendungsbereich zwar nicht ausgeschlossen, aber praktisch vollkommen überlagert. Bei der Verarbeitung zur Erfüllung des Beschäftigungsverhältnisses ist dies der Fall, wenn ein unmittelbarer Zusammenhang mit dem Beschäftigungsverhältnis besteht (siehe 3.6.1.1.1, S. 486).[1502] Außerhalb dieses Bereichs, in dem gar kein oder lediglich ein mittelbarer Zusammenhang mit dem Beschäftigungsverhältnis besteht, hat die Generalklausel dagegen auch praktische Bedeutung.

1336 Die Abgrenzung der beiden Erlaubnistatbestände ist kein neues Problem, sodass hierfür Anleihen aus anderen Bereichen genommen werden können. Bei der Aufdeckung und Bekämpfung von Straftaten wird bspw. danach differenziert, ob dies präventiv oder repressiv geschieht. Letzteres ist auf arbeitsrechtliche Konsequenzen gerichtet und darum auf § 26 Abs. 1 S. 2 BDSG 2018 zu stützen. Ersteres ist dagegen lediglich Ausdruck der Pflichten der Geschäftsleitung gegenüber der Gesellschaft und lässt sich nicht aus den vertraglichen Pflichten des Beschäftigungsverhältnisses ablei-

---

BAG v. 20.10.2016 – 2 AZR 395/15, E 157, S. 69–83 (=NZA 2017, S. 443), siehe Fn. 1250) heran, obwohl es „lediglich" um die Aufzeichnung des Arbeitsverhaltens bzw. von Tastatureingaben und Screenshots geht.

1501 BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 32 (=NZA 2017, S. 1205).

1502 So i.E. auch *Varadinek, et al.* 2018, S. 24 ff.

ten. Hier muss folglich auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zurückgegriffen werden.[1503]

Für die Kontrolle von Beschäftigten lässt sich diese Abgrenzung direkt übernehmen. Für die Einsichtnahme, die ja im weitesten Sinne auf die Organisation des Betriebsablaufs gerichtet ist, rückt die Erteilung von Weisungen zur Arbeitsausführung an die Stelle der arbeitsrechtlichen Maßnahme.[1504] Die Datenverarbeitung, die letztlich hierauf zielt, ist an Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO zu messen. Geht es dem Arbeitgeber dagegen primär um das eigene Geschäft, hat das zwar u.U. ebenfalls Auswirkungen auf die Arbeit der Beschäftigten. Für den von der Datenverarbeitung betroffenen Beschäftigten sind diese Konsequenzen aber nur mittelbar spürbar. Weisungen zur Arbeitstätigkeit oder arbeitsrechtliche Maßnahmen sind nur ein Nebenprodukt; die Datenverarbeitung ist nicht darauf ausgerichtet. 1337

3.6.1.3.2 Legitime Interessen

Damit die Zulässigkeit einer Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO überhaupt in Betracht kommt, muss der Verantwortliche – in diesem Fall der Arbeitgeber – zur Wahrung seiner berechtigten Interessen oder denen eines Dritten handeln. Die Verordnung selbst gibt diesem Begriff keine weiteren Konturen. Ein allgemeiner Hinweis findet sich lediglich in ErwG 47 S. 2, wonach eine „maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen" ein berechtigtes Interesse begründet. Die danach genannten Beispiele einer Kunden- und Dienstbeziehung erfassen zwar immerhin die hier diskutierten Fälle, greifen aber angesichts der vielfältigen grundrechtlichen Positionen des Verantwortlichen insgesamt deutlich zu kurz. 1338

Als berechtigte Interessen kommen prinzipiell sämtliche grundrechtlich fundierten Interessen des Verantwortlichen in Betracht.[1505] Insofern besteht ein Gleichlauf mit den Anforderungen an die Legitimität des Zwecks im Rahmen der Zweckbindung (siehe 3.4.1.2.1.2, S. 357). Mit der prinzipiellen Anerkennung des Zwecks ist jedoch noch keine Bewertung verbun- 1339

1503 *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 17 f.; *Wedde*, in: Däubler et al. 2020, § 26 BDSG, Rn. 161.
1504 So auch *Varadinek, et al.* 2018, S. 27 f.
1505 BeckOK DSR/*Albers/Veit*, Art. 6 DS-GVO, Rn. 49.

den. Welches Gewicht dem Interesse beizumessen ist, bestimmt sich in der Interessenabwägung.

1340 Zu den anerkannten Interessen des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zählt insbesondere die unternehmerische Freiheit des Arbeitgebers nach Art. 16 GRC (siehe 3.2.4, S. 307). Dies gilt umso mehr, als hier die in ErwG 47 S. 2 erwähnte Beziehung besteht. Die (unternehmerische) Berufsfreiheit des Arbeitgebers nach Art. 12 Abs. 1 GG ist hier dagegen nicht anwendbar. Anders als im Rahmen von Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO muss der Zweck der Datenverarbeitung bei Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO nicht eigens durch eine – zumeist nach mitgliedstaatlichen Maßstäben – vorzunehmende Vertragsauslegung bestimmt werden. Die nationalen Grundrechte kommen aber nur in Rahmen dieser Zweckbestimmung zur Anwendung (3.2.2.5.2, S. 281).

1341 Ohne sein Leistungsbestimmungsrecht nach § 106 S. 1 GewO, mit dem er die arbeitsvertraglichen Pflichten der Arbeitnehmer konkretisieren kann, steht dem Arbeitgeber auch bei der Konkretisierung des datenschutzrechtlichen Zwecks kein Spielraum zu. Anders als bei Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO (siehe 3.4.1.4.4, S. 395) ist der Zweck in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO darum ausschließlich nach objektiven Kriterien zu bestimmen. Insbesondere was die Überprüfung wirtschaftlicher Erwägungen angeht, die hinter der Datenverarbeitung stehen, kann sich der Arbeitgeber darum nicht auf seine unternehmerische Entscheidungsfreiheit zurückziehen.

3.6.1.3.3 Erforderlichkeit und Interessenabwägung

1342 Die Erforderlichkeitsprüfung und Interessenabwägung laufen in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO nicht grundlegend anders ab als dies für § 26 Abs. 1 S. 1 BDSG 2018 bzw. Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO erörtert wurde. Der einzige augenfällige Unterschied betrifft den Maßstab der Angemessenheit. Für die Datenverarbeitung zur Erfüllung eines Vertrags gilt ein übereinstimmend subjektiver Maßstab (siehe 3.4.1.3.4.2.1, S. 381). Für die Interessenabwägung wird in ErwG 47 S. 1 dagegen hervorgehoben, dass hier die vernünftigen Erwartungen der betroffenen Person zu berücksichtigen sind, die auf ihrer Beziehung zu dem Verantwortlichen beruhen. In den Bereichen von Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO, die nicht durch einen unmittelbaren Zusammenhang mit dem Vertragsverhältnis von diesem determiniert werden, kommt es darum stärker auf die objektivierte Sicht der betroffenen Person an.

Praktisch wirkt sich dieser Unterschied so aus, dass der Erlaubnistatbestand in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO in der Regel eine geringere Legitimationswirkung entfaltet. Eine Datenverarbeitung aus Anlass des Beschäftigungsverhältnisses ist zwar nicht völlig ungewöhnlich, aber dennoch nicht in dem Maße selbstverständlich wie eine Verarbeitung aufgrund des Beschäftigungsverhältnisses. Im Kontext der Industrie 4.0 wird sich der Erwartungshorizont hier zwar womöglich etwas erweitern.[1506] An der grundsätzlichen Verschiedenheit der Konstellationen ändert dies aber nichts. Die Interessen sind darum – wie es ErwG 47 S. 3 ausdrückt – besonders sorgfältig abzuwägen. 1343

3.6.1.4 Mitbestimmung

Der zentrale Mitbestimmungstatbestand im Datenschutzrecht ist § 87 Abs. 1 Nr. 6 BetrVG, der die Einrichtung und Anwendung von technischen Einrichtungen erfasst, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Diese Norm betrifft weite Teile der automatisierten Verarbeitung von Beschäftigtendaten durch den Arbeitgeber. Übt der Betriebsrat sein Mitbestimmungsrecht aus, mündet dies in der Regel in eine Betriebsvereinbarung nach § 77 BetrVG, die ihrerseits einen Erlaubnistatbestand für die Datenverarbeitung darstellt. 1344

Für den Beschäftigtendatenschutz im Umgang mit Assistenzsystemen der Industrie 4.0 stellen sich im Hinblick auf die Mitbestimmung zwei Fragen: Erstens, welche Systemgestaltung der Mitbestimmungstatbestand erfasst und zweitens, welche Spielräume den Betriebsparteien im Vergleich zu einem auf das Weisungsrecht gestützten Vorgehen des Arbeitgebers zu gewähren sind. 1345

3.6.1.4.1 Die Reichweite des Mitbestimmungstatbestands

Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG hat einen gegenüber dem Beschäftigtendatenschutzrecht eigenständigen Anwendungsbereich, der sich jedoch in den meisten Fällen mit diesem überschneidet. 1346

1506 *Varadinek, et al.* 2018, S. 38.

3.6.1.4.1.1 Technische Einrichtung mit eigenständiger Überwachungswirkung

1347 Erfasst wird zunächst nur die Überwachung mit technischen Einrichtungen. Dieser Regelung liegt die Annahme zugrunde, dass gerade der Einsatz technischer Kontrolleinrichtungen zu einer anonymen Überwachung führt, in dem Sinne, dass der Überwacher aus der Sicht des überwachten Arbeitnehmers kein Gesicht zeigt und die Überwachung darum weder erkannt noch abgewendet werden kann.[1507] Dieser Regelungsgedanke stimmt nicht mit dem der automatisierten oder dateisystembezogenen Datenverarbeitung in Art. 2 Abs. 1 DS-GVO überein, bei dem es maßgeblich um die bessere Verarbeitungsmöglichkeit geht.

1348 Um als technische Einrichtung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG zu gelten, muss das eingesetzte Gerät eine eigenständige Überwachungswirkung haben und nicht nur Hilfsmittel personell durchgeführter Überwachung sein.[1508] Anders als nach Art. 2 Abs. 1 DS-GVO fallen damit z.B. auch reine Kamera-Monitor-Verfahren in den Mitbestimmungstatbestand des § 87 Abs. 1 Nr. 6 BetrVG,[1509] da sie den Überwachungsdruck gegenüber einer direkten und dadurch in der Regel offenen Beobachtung durch einen Menschen erhöhen. Dieser Unterschied spielte z.B. in der Einordnung von Kamerasystemen ohne automatisierte Erkennungsfähigkeiten („dumme Videoüberwachung", siehe 3.3.4.7.2.1, S. 347) eine Rolle, wird aber durch die Ausweitung des Anwendungsbereichs des Beschäftigtendatenschutzes auf nicht automatisierte Datenverarbeitung ohne Dateisystembezug in § 26 Abs. 7 BDSG 2018 gänzlich eingeebnet.

1349 Nach diesem weiten Begriffsverständnis sind Produktions- und Assistenzsysteme der Industrie 4.0, mit denen Arbeitnehmer in irgendeiner Form interagieren, als technische Einrichtungen im Sinne von § 87 Abs. 1 Nr. 6 BetrVG einzustufen. Damit steht aber lediglich fest, dass ein Mitbestimmungsrecht des Betriebsrats in Frage kommt. Ob es tatsächlich besteht, richtet sich nach der konkreten Verwendung des Systems.

1507 BAG v. 9.9.1975 – 1 ABR 20/74, E 27, S. 256, Rn. 25 (=NJW 1976, S. 261); BeckOK ArbR/*Werner*, § 87 BetrVG, Rn. 89.

1508 LAG Berlin-Brandenburg v. 22.3.2017 – 23 TaBVGa 292/17, ZD, S. 579–580*Richardi*, in: Richardi 2018, § 87 BetrVG, S. 515; BeckOK ArbR/*Werner*, § 87 BetrVG, Rn. 92.

1509 BAG v. 26.1.2016 – 1 ABR 68/13, NZA 2016, S. 498, 500; *Kreuder/Matthiessen-Kreuder*, in: Däubler et al. 2017, § 611a BGB, Rn. 530.

3.6.1.4.1.2 Konkrete Eignung zur Überwachung

Der Mitbestimmungstatbestand in § 87 Abs. 1 Nr. 6 BetrVG erfasst nach seinem Wortlaut nur Systeme, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Wendete man die Unterscheidung zwischen Einsichtnahme und Kontrolle (3.6.1.2.3.1, S. 508) auch hier an, würde nur letzteres die Mitbestimmung des Betriebsrats auslösen. Das Bundesarbeitsgericht interpretiert die Norm allerdings in ständiger Rechtsprechung so, dass es bereits ausreicht, wenn die Einrichtung aufgrund ihrer technischen Gegebenheiten und der konkreten Art ihrer Verwendung zur Überwachung der Arbeitnehmer objektiv geeignet ist.[1510] 1350

Die Auslegung ist durch den Schutzgedanken der Norm gedeckt, Eingriffe in das Persönlichkeitsrecht durch technische Kontrolleinrichtungen nur bei gleichberechtigter Mitbestimmung des Betriebsrats zuzulassen. Da der für den Eingriff maßgebliche Überwachungsdruck bereits mit der Datenerhebung einsetzt, unabhängig davon, ob die Überwachung bezweckt wird oder die Daten überhaupt ausgewertet werden, muss auch das Mitbestimmungsrecht in dieser frühen Phase greifen.[1511] 1351

Da es nach diesem weiten Ansatz auf den Zweck der technischen Einrichtung gerade nicht ankommt, ist die Unterscheidung zwischen Überwachung und Einsichtnahme für das Bestehen eines Mitbestimmungsrechts nicht von Belang. Was der Einsichtnahme dient, kann prinzipiell auch zur Kontrolle der Mitarbeiter eingesetzt werden. Insofern ergeben sich Parallelen zum Anwendungsbereich des Datenschutzrechts. 1352

Dieser Effekt zeigte sich schon in dem Sachverhalt, der dem richtungsweisenden Urteil des Bundesarbeitsgerichts zu § 87 Abs. 1 Nr. 6 BetrVG im Jahre 1975 zugrunde lag.[1512] Hier verfügten Drehbänke über einen sog. Produktographen (Nutzungsschreiber), den die Mitarbeiter zu bedienen 1353

1510 Grundlegend BAG v. 9.9.1975 – 1 ABR 20/74, E 27, S. 256, Rn. 25 (=NJW 1976, S. 261); in die Richtung bereits BAG v. 14.5.1974 – 1 ABR 45/73, AP BetrVG 1972 § 87 Überwachung Nr. 1 (=NJW 1974, S. 2053); zuletzt z.B. BAG v. 27.1.2004 – 1 ABR 7/03, E 109, S. 235, Rn. 27 (=NZA 2004, S. 556); BAG v. 13.12.2016 – 1 ABR 7/15, E 157, S. 220, Rn. 22 (=NZA 2017, S. 657) Diese Auffassung wird in der Literatur – zumindest mittlerweile – nicht in Zweifel gezogen, siehe nur *Richardi,* in: Richardi 2018, § 87 BetrVG, Rn. 513; *Thüsing/Granetzny,* in: Thüsing 2014, § 20, Rn. 34 m.w.N.

1511 So sinngemäß BAG v. 9.9.1975 – 1 ABR 20/74, E 27, S. 256, Rn. 25 (=NJW 1976, S. 261); zustimmend *Richardi,* in: Richardi 2018, § 87 BetrVG, Rn. 492; *Thüsing/Granetzny,* in: Thüsing 2014, § 20, Rn. 34.

1512 BAG v. 9.9.1975 – 1 ABR 20/74, E 27, S. 256–263 (=NJW 1976, S. 261).

hatten. Damit erfasste der Arbeitgeber, wie die Maschine in Bezug auf jedes Arbeitsstück tatsächlich genutzt wurde, konkret ob es repariert oder gereinigt wurde, ob es zu Werkzeugbruch oder zu Wartezeiten kam. Ziel war es, Störungen zu erkennen und zu beseitigen. Das Bundesarbeitsgericht hat die Frage nach der konkreten Eignung zur Überwachung in dem Fall mangels hinreichender Sachverhaltsaufklärung offengelassen. Die Tatsache, dass das System allenfalls der Einsichtnahme in Arbeitsprozesse diente, hat es für das Bestehen des Mitbestimmungsrechts aber jedenfalls nicht als maßgeblich betrachtet.

3.6.1.4.1.3 Maßgeblichkeit der Systemgestaltung

1354 Eine wichtige Einschränkung erfährt das Mitbestimmungsrecht des Betriebsrats durch das Anknüpfen an die konkrete Art, in der die technische Einrichtung verwendet wird. Auch Systeme, die für sich genommen prinzipiell geeignet sind, personenbezogene Daten zu verarbeiten, können demnach im konkreten Fall so eingesetzt werden, dass das Mitbestimmungsrecht nicht berührt ist. Dafür genügt es aber nicht, dass das System aktuell keine Arbeitnehmer überwacht. Die Überwachung muss bereits nach der konkreten Systemgestaltung praktisch ausgeschlossen sein.

1355 Ein simples Beispiel für eine solche Systemgestaltung wäre eine Videokamera, die in einem Bereich eingesetzt wird, in dem sich keine Menschen aufhalten können. Der für § 87 Abs. 1 Nr. 6 BetrVG maßgebliche Überwachungsdruck fehlt aber auch, wenn die Systeme menschliches Verhalten zwar erfassen, dabei aber keine personenbezogenen Daten verarbeiten.[1513] Systeme ohne interne Identifizierungsleistung oder Schnittstellen nach außen (siehe 3.3.4.7.2.4, S. 351) oder solche, die lediglich anonyme Daten verarbeiten (siehe 3.3.4.4, S. 341) fallen darum nicht unter das Mitbestimmungsrecht des Betriebsrats.

1356 Die konkrete Eignung zur Überwachung schließt alle Szenarien mit ein, in denen der Arbeitnehmer die technische Einrichtung ohne größeren Aufwand, d.h. allein abhängig von seinem Willen zur Überwachung einsetzen

---

1513 BAG v. 18.2.1986 – 1 ABR 21/84, E 51, S. 143, Rn. 26 ff. (=NZA 1986, S. 488); BAG v. 26.7.1994 – 1 ABR 6/94, E 77, S. 262, Rn. 25 (=NZA 1995, S. 185); BAG v. 13.12.2016 – 1 ABR 7/15, E 157, S. 220, Rn. 27 (=NZA 2017, S. 657); *Richardi,* in: Richardi 2018, § 87 BetrVG, S. 511; BeckOK ArbR/*Werner*, § 87 BetrVG, Rn. 94.

könnte.[1514] Ließe sich z.B. die Videokamera in Bereiche schwenken, in denen sich Menschen aufhalten, wären die Schnittstellen doch zu öffnen oder ließe sich die Anonymität aufheben, wäre das Mitbestimmungsrecht einschlägig. Ob eine Schutzmaßnahme überwunden werden kann, entscheidet sich wie bei der Anwendbarkeit des Datenschutzrechts danach, ob der Arbeitgeber den dazu erforderlichen Aufwand realistischerweise betreiben würde, also letztlich anhand einer kursorischen Risikoanalyse (siehe 3.3.1.2.2, S. 318).

Dabei ist allerdings zu beachten, dass die Mitbestimmung nicht nur sicher- 1357
stellen soll, dass Leistung und Verhalten der Arbeitnehmer richtig beurteilt werden. Es geht auch darum, den Überwachungsdruck möglichst gering zu halten und ihn z.B. mit Schutzmaßnahmen dort zu vermeiden, wo er nicht notwendig ist. Dazu ist der Betriebsrat bereits bei der Vorbereitung der Anwendung zu beteiligen.[1515] Dies deckt sich mit dem Anwendungsbereich von Art. 25 Abs. 1 DS-GVO, demzufolge technische und organisatorische Maßnahmen bereits bei der Festlegung der Mittel für die Verarbeitung getroffen werden müssen. Insbesondere Maßnahmen, die der technischen Einrichtung nicht immanent sind, sondern in der Vorbereitungsphase erst auf sie angewendet werden müssen, sind darum kritisch zu bewerten. Das Mitbestimmungsrecht entfällt nur, wenn bereits in der mitbestimmungsfreien Planungsphase[1516] ausgeschlossen werden kann, dass personenbezogene Daten verarbeitet werden.

3.6.1.4.2 Der Spielraum der Betriebsparteien

Eine Betriebsvereinbarung wirkt nach Art. 77 Abs. 4 BetrVG unmittelbar 1358
und zwingend auf das Rechtsverhältnis zwischen Arbeitgeber und Arbeitnehmer und bildet darum gemäß Art. 88 Abs. 1 DS-GVO – nach anderer Auffassung gemäß § 26 Abs. 4 BDSG 2018 (siehe 3.6.1.1.2, S. 488) – einen eigenständigen Erlaubnistatbestand für die Datenverarbeitung. Inhaltlich sind die Betriebsparteien jedoch weiterhin dazu verpflichtet, die Persönlichkeit der Arbeitnehmer zu schützen. Das zeigt sich schon an der origi-

1514 BAG v. 14.5.1974 – 1 ABR 45/73, AP BetrVG 1972 § 87 Überwachung Nr. 1 (=NJW 1974, S. 2053).
1515 BeckOK ArbR/*Werner*, § 87 BetrVG, Rn. 97.
1516 *Richardi*, in: Richardi 2018, § 87 BetrVG, Rn. 526; BeckOK ArbR/*Werner*, § 87 BetrVG, Rn. 97.

när betriebsverfassungsrechtlichen Pflicht nach § 75 Abs. 2 BetrVG, die freie Entfaltung der Persönlichkeit der Beschäftigten zu fördern.[1517]

1359 Darüber hinaus gibt auch das Datenschutzrecht einen gewissen Rahmen vor. Kollektivvereinbarungen werden in der Datenschutz-Grundverordnung nicht großzügiger gehandhabt als die übrigen Erlaubnistatbestände nach Art. 6 Abs. 1 UAbs. 1 DS-GVO. Das Gegenteil ist der Fall: Gemäß Art. 88 Abs. 2 DS-GVO bzw. § 26 Abs. 4 S. 2 BDSG 2018 müssen Kollektivvereinbarungen, welche spezifische Vorschriften nach Art. 88 Abs. 1 DS-GVO enthalten, umfassend geeignete und besondere Maßnahmen zur Wahrung der Rechte der betroffenen Personen enthalten. Darüber hinaus sind auch die allgemeinen Grundsätze des Datenschutzrechts nach Art. 5 DS-GVO (siehe 3.4.1, S. 354) zu beachten.[1518]

1360 So deutlich der Umstand hervortritt, dass die Betriebsparteien bei ihren Entscheidungen die Grundsätze des Datenschutzes beachten müssen, so unklar bleibt gleichzeitig, wie eng die Bindung an die Standards der Datenschutz-Grundverordnung ausfällt. Dies gilt insbesondere für die Frage, wie weit der Spielraum im Hinblick auf den Interessenausgleich oder die Risikoabwägung beim technischen Datenschutz ausfällt.[1519] Denkbar wäre aber auch, dass die Betriebsparteien bei vergleichsweise detailliert geregelten Schutzinstrumenten wie den Transparenzpflichten oder den Betroffenenrechten abweichen dürfen.

3.6.1.4.2.1 Europarechtlicher und mitgliedstaatlicher Handlungsrahmen

1361 Die Frage stellt sich im Grunde sogar doppelt, auf europarechtlicher und nationaler Ebene. Unabhängig davon, ob man die Regelungskompetenz der Betriebsparteien als eine originäre oder von der der Mitgliedstaaten abgeleitete betrachtet, ist klar, dass die Betriebsparteien bei der Normierung spezifischer Vorschriften nach Art. 88 Abs. 1 DS-GVO jedenfalls keinen größeren Spielraum haben als die Mitgliedstaaten (dazu 3.1.3, S. 242)

1517 BAG v. 27.5.1986 – 1 ABR 48/84, E 52, S. 88, Rn. 49 (=NZA 1986, S. 643); BAG v. 29.6.2004 – 1 ABR 21/03, E 111, S. 173, Rn. 13 (=NZA 2004, S. 1278); BAG v. 15.4.2014 – 1 ABR 2/13 (B), E 148, S. 26, Rn. 40 (=NZA 2014, S. 551); BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 13 (=NZA 2017, S. 1205).

1518 BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 55.

1519 Für eine generelle Abweichungskompetenz nach oben *Wedde,* in: Däubler et al. 2020, § 26 BDSG, Rn. 249; für eine umfassende Abweichungskompetenz, auch nach unten BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 54.

selbst. Der Streit betrifft im Grunde nur die Frage, ob der deutsche Gesetzgeber die Betriebsparteien bereits durch § 77 Abs. 4 BetrVG oder erst durch § 26 Abs. 4 BDSG 2018 ermächtigt hat, innerhalb der Öffnungsklausel zu agieren, nicht aber, ob die Betriebsparteien allein auf Art. 88 Abs. 1 DS-GVO gestützt neben den Mitgliedstaaten Regelungen treffen können.[1520] Den ersten Handlungsrahmen bildet demnach Art. 88 DS-GVO.

Wird dieser europarechtliche Handlungsrahmen eingehalten, gelten nur deutsche Grundrechte. Die europäischen Grundrechte gelten lediglich im Hinblick auf die Frage, ob die Grenzen der Öffnungsklausel eingehalten wurden (siehe 3.2.2.2.2.1, S. 267). Innerhalb des europäischen Rahmens spannt sich so ein zweiter, mitgliedstaatlicher Handlungsrahmen auf. 1362

3.6.1.4.2.2 Bisherige Rechtsprechungslinie zum nationalen Handlungsrahmen

Das Bundesarbeitsgericht hatte zur alten Rechtslage die Auffassung vertreten, dass Kollektivvereinbarungen andere Rechtsvorschriften nach § 4 Abs. 1 BDSG 2003 darstellen und darum hinsichtlich ihres Inhalts nicht an die Vorschriften des Bundesdatenschutzgesetzes gebunden seien, die dortigen Standards also auch unterschreiten könnten. Der datenschutzrechtliche Mindeststandard ergebe sich stattdessen aus den grundgesetzlichen Wertungen, die etwa über § 75 Abs. 2 BetrVG zum Tragen kämen.[1521] Schon damals war allerdings unklar, inwiefern sich die Standards z.B. des § 32 BDSG 2003 und § 75 Abs. 2 BetrVG angesichts der identischen grundrechtlichen Fundierung voneinander unterschieden.[1522] Eine Unterschreitung des Schutzstandards wäre darum wohl nur dann zulässig gewesen, wenn gleichzeitig kompensatorische Maßnahmen vorgesehen worden wären.[1523] 1363

1520 So aber BeckOK DSR/*Riesenhuber*, Art. 88 DS-GVO, Rn. 49.

1521 BAG v. 27.5.1986 – 1 ABR 48/84, E 52, S. 88, Rn. 44 ff. (=NZA 1986, S. 643); so auch *Thüsing,* NZA 2011, S. 16, 18; a.A. *Arnold* 2010, S. 69 f.; *Seifert,* in: Simitis 2014, § 32 BDSG, Rn. 167.

1522 *Franzen,* RdA 2010, S. 257, 260 spricht von seltenen Fällen, in denen eine Abweichung möglich wäre. *Gola/Wronka* 2013, S. 336 hielten eine zulässige Abweichung für „kaum denkbar".

1523 *Seifert,* in: Simitis 2014, § 32 BDSG, Rn. 167; *Thüsing/Granetzny,* in: Thüsing 2014, § 4, Rn. 17; a.A. *Nink/Müller,* ZD 2012, S. 505, 508.

1364 Diese auf das Subsidiaritätsprinzip des alten Bundesdatenschutzgesetzes gestützte Argumentation lässt sich zumindest anhand des nationalen Handlungsrahmens auch im neuen Recht fortführen. Das allgemeine Subsidiaritätsprinzip in § 1 Abs. 2 BDSG 2018 gilt zwar nur für Rechtsvorschriften des Bundes, die Öffnungsklausel in § 26 Abs. 4 S. 1 BDSG 2018 kann dafür aber als spezielles Subsidiaritätsprinzip verstanden werden. In diesem Fall käme es auch nicht darauf an, ob die Parteien der Kollektivvereinbarung nach den für sie geltenden Grundsätzen Rechtspositionen des Einzelnen verschlechtern dürfen. Die fraglichen datenschutzrechtlichen Rechtspositionen gälten dann nämlich nicht mehr.

1365 Der nationale Handlungsrahmen ergibt sich damit weiterhin ausschließlich aus § 75 Abs. 2 BetrVG und nicht aus dem Bundesdatenschutzgesetz. Letzterem können damit auch weiterhin keine Mindeststandards entnommen werden.

3.6.1.4.2.3 Veränderungen aufgrund des europäischen Handlungsrahmens

1366 Im Gegensatz zur bisherigen Rechtslage regeln Art. 88 Abs. 2 DS-GVO bzw. die deutsche Verweisnorm in § 26 Abs. 4 S. 2 BDSG 2018 allerdings nun einen explizit datenschutzrechtlichen Mindeststandard, der in der Kollektivvereinbarung nicht unterboten werden darf. Dabei lässt sich der Wortlaut, geeignete und besondere Maßnahmen zur Wahrung der Rechte der betroffenen Person zu treffen, noch so interpretieren, dass die spezifische Regelung nach Art. 88 Abs. 1 DS-GVO nur einen gleichwertigen, nicht aber einen gleichartigen Schutz gewährleisten muss. Dies entspräche weitgehend der alten Rechtslage, in der die Vorgaben z.B. von § 75 Abs. 2 BetrVG an die Stelle der Vorgaben des Bundesdatenschutzgesetzes traten, sodass dessen Schutzstandards nicht beliebig unterschritten werden konnten.[1524]

1367 Aufgrund des wenigstens mindestharmonisierenden Charakters der Datenschutz-Grundverordnung (siehe 3.1.3, S. 242) dürfen deren Schutzstandards aber nicht unterschritten werden.[1525] Sie dürfen allenfalls verbessert

1524 Für einen inhaltlichen Gleichlauf von Art. 88 Abs. 2 DS-GVO und § 75 Abs. 2 BetrVG auch *Maschmann*, in: Kühling/Buchner 2018, Art. 88 DS-GVO, Rn. 84.

1525 So auch *Klösel/Mahnhold*, NZA 2017, S. 1428, 1430 f.; *Maier*, DuD 2017, S. 169, 172 f.; *Pötters*, in: Gola 2018, Art. 88 DS-GVO, Rn. 26; *Varadinek, et al.* 2018, S. 42 f.; *Wedde*, in: Däubler et al. 2020, § 26 BDSG, Rn. 249, die aber nicht zwischen einzelnen Vorgaben der Datenschutz-Grundverordnung differenzieren.

werden. Die Linie des Bundesarbeitsgerichts lässt sich unter dem neuen Recht folglich nicht fortführen. In wichtigen Bereichen wie dem des Interessenausgleichs im Rahmen der Angemessenheit ist die Verordnung sogar vollharmonisierend. Hier kann eine Kollektivvereinbarung die Pflichten lediglich unter Berücksichtigung der Vorgaben der Datenschutz-Grundverordnung konkretisieren.[1526]

Dabei ist jedoch zu beachten, dass die Vorgaben der Verordnung im höchsten Maße unbestimmt sind. Ähnlich der Zwecksetzungsbefugnis des Arbeitgebers (siehe 3.6.1.2.1, S. 491) wird man den Betriebsparteien darum eine gewisse Einschätzungsprärogative zubilligen müssen.[1527] 1368

3.6.1.5 Einwilligung

Wie die Regelung in § 26 Abs. 2 BDSG 2018 zeigt, kann auch die Verarbeitung von Beschäftigtendaten auf eine Einwilligung der betroffenen Person gestützt werden.[1528] Im Hinblick auf das konstituierende Merkmal der Freiwilligkeit unterliegt dieses Instrument aber empfindlichen Einschränkungen, welche es im Umgang mit Produktions- und Assistenzsystemen der Industrie 4.0 als nicht praktikabel erscheinen lassen. 1369

Die erste Einschränkung betrifft die Leitbildfunktion des Erlaubnistatbestands der Erfüllung des Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO (siehe 3.6.1.1.2.2, S. 491). Sie führt dazu, dass man bei der Datenverarbeitung, die im unmittelbaren Zusammenhang mit der Vertragserfüllung steht, bereits daran zweifeln kann, ob die Einwilligung einzuholen überhaupt einen relevanten Mehrwert erzeugt. Dies gilt umso mehr, als der Verantwortliche eine Datenverarbeitung nicht auf die Einwilligung stützen darf, wenn er sie ebenso gut auf der Basis eines gesetzlichen Erlaubnistatbestands in Art. 6 Abs. 1 UAbs. 1 lit. b bis f DS-GOV rechtfertigen könnte (siehe 3.4.1.6.1, S. 418). Die Bereiche, die auf die Einwilligung gestützt 1370

Für eine Unterschreitungskompetenz dagegen BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 54.

1526 So auch *Martini/Botta,* NZA 2018, S. 625, 633; *Maschmann,* NZA-Beil. 2018, S. 115, Rn. 116 f., jedoch ohne die hier angeregte Differenzierung. A.A. *Zöll,* in: Taeger/Gabel 2019, Art. 88 DS-GVO, Rn. 25.

1527 *Klösel/Mahnhold,* NZA 2017, S. 1428, 1431, die ebenfalls auf eine Willkürkontrolle abstellen.

1528 Dies war nach altem Recht umstritten, siehe nur *Bausewein* 2012. Zur verfassungsrechtlichen Dimension *Bäcker* 2012, S. 36.

werden sollen, müssten darum wenigstens klar von denen abgegrenzt werden, die zur Vertragserfüllung notwendig sind.

1371 Die zweite Einschränkung folgt aus § 26 Abs. 2 S. 1 BDSG 2018, demzufolge bei Einwilligungen im Beschäftigungsverhältnis u.a. die bestehende Abhängigkeit der beschäftigten Person zu berücksichtigen ist. Freiwilligkeit kann gemäß § 26 Abs. 4 S. 2 BDSG 2018 vorliegen, wenn die betroffene Person einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder Arbeitgeber und Beschäftigter gleichgerichtete Interessen verfolgen. Da hiermit kaum das übliche Austauschverhältnis und das allgemeine Interesse am wirtschaftlichen Erfolg des Betriebs gemeint sein kann, wird man die Einwilligung nur in ausgewählten Situationen zulassen dürfen.[1529]

1372 Als Beispiele werden in der Gesetzesbegründung und der Literatur Situationen genannt, in denen der Arbeitgeber Leistungen anbietet, die über das zur Durchführung des Beschäftigungsverhältnisses notwendige Maß hinausgehen, etwa die private Nutzung betrieblicher IT.[1530] Da dem Beschäftigten durch die Verweigerung der Einwilligung hier keine Nachteile entstünden,[1531] gebe es keinen Grund, an der Freiwilligkeit zu zweifeln. Für den Umgang mit Produktions- und Assistenzsystemen bedeutet dies, dass erstens deren Benutzung nicht verpflichtend sein darf und zweitens der Beschäftigte auch bei Wahlfreiheit die ihm gestellten Aufgaben auch mit einem datensparsameren System erledigen können muss.[1532] Dies würde auf ein paralleles Angebot herkömmlicher und neuartiger Arbeitsplätze hinauslaufen[1533] und damit den Anreiz zur Einführung von Produktions- und Assistenzsystemen der Industrie 4.0 beträchtlich mindern.[1534]

1373 Darüber hinaus kann die Einwilligung aufgrund ihrer nunmehr in Art. 7 Abs. 3 S. 1 DS-GVO explizit normierten Widerruflichkeit keine Planungssicherheit bieten. Eine Einwilligungslösung ist darum für den Einsatz von Assistenzsystemen aller Voraussicht nach nicht praktikabel.[1535]

1529 *Martini/Botta,* NZA 2018, S. 625, 629 erwähnen den Fall eines Exoskeletts und dessen Analysetools als Teil eines betrieblichen Gesundheitsmanagementsystems.

1530 BT-Drucks. 18/11325, S. 97; *Forst,* in: Auernhammer 2020, § 26 BDSG, Rn. 77.

1531 Für diesen Maßstab *Art. 29-Grp.,* WP 48, S. 23.

1532 So auch *Martini/Botta,* NZA 2018, S. 625, 628 f.

1533 *Hofmann,* ZD 2016, S. 12, 14.

1534 Auch *Varadinek, et al.* 2018, S. 52 gehen davon aus, dass die Einwilligung in Ermangelung echter Wahlfreiheit nicht praktikabel wäre.

1535 So auch *Martini/Botta,* NZA 2018, S. 625, 629; *Maschmann,* NZA-Beil. 2018, S. 115, Rn. 116.

3.6.2 Spezifische Verarbeitungssituationen

Die Prüfung der Erforderlichkeit und Angemessenheit folgt zwar allgemeinen Regeln, lässt sich aber aufgrund der starken Einzelfallbezogenheit dieser Regeln nicht generell, sondern allenfalls typisiert für verbreitete Verarbeitungssituationen vornehmen. Der deutsche Gesetzgeber hat die Öffnungsklausel in Art. 88 Abs. 1 DS-GVO trotz entsprechender Vorschläge im Reformprozess[1536] nicht dazu genutzt, speziellere Regelungen für solche Verarbeitungsformen zu erlassen. Die Prüfung muss darum anhand der bereits erörterten Grundsätze des Datenschutzrechts sowie der für die jeweilige Situation bestehenden Rechtsprechung und Literatur erfolgen. 1374

3.6.2.1 Videoüberwachung

Kamerabasierte Systeme zur Überwachung der Beschäftigten fallen nicht zwingend in den Anwendungsbereich des Datenschutzrechts nach Art. 2 Abs. 1 DS-GVO und § 26 Abs. 7 BDSG 2018. Gerade Systeme zur reinen Objekterkennung verarbeiten nach der hier vertretenen Auffassung (3.3.4.7, S. 345) keine personenbezogenen Daten, wenn sie weder über eine Schnittstelle zum Auslesen der Aufnahmen noch über die Fähigkeit zur automatisierten Personenidentifikation verfügen. 1375

3.6.2.1.1 Erlaubnistatbestände für die Videoüberwachung

Für anderweitig gestaltete Systeme gelten dagegen die allgemeinen Grundsätze des Datenschutzrechts. Die Rechtmäßigkeit der Datenverarbeitung bestimmt sich hier anhand der Erlaubnistatbestände in Art. 6 Abs. 1 UAbs. 1 DS-GVO, wobei für die Videoüberwachung durch den Arbeitgeber vor allem die Verarbeitung zur Erfüllung des Vertrags nach lit. b sowie die zur Wahrung berechtigter Interessen in Buchstabe f in Betracht kommen. 1376

Andere Erlaubnistatbestände spielen für die spezifischen Verarbeitungssituationen in der Industrie 4.0 dagegen keine Rolle. So ist zwar durchaus vorstellbar, dass in Videosystemen auch besonderen Kategorien personenbezogener Daten verarbeitet werden, sodass Art. 9 Abs. 2 lit. b i.V.m. § 26 1377

1536 *Körner* 2017, S. 72 f.

Abs. 3 DS-GVO Anwendung fände. Dies ist aber nur bei entsprechender Auswertungsabsicht oder beim Einsatz biometrischer Gesichtserkennung der Fall.[1537] Beides betrifft keine Spezifika der Industrie 4.0.

1378 Für die Videoüberwachung öffentlich zugänglicher Räume hat der Gesetzgeber in § 4 BDSG 2018 zudem eine spezielle Regelung getroffen. Bei diesen Räumen kann es sich auch um Arbeitsräume handeln, etwa bei Verkaufsflächen im Einzelhandel, die für den Publikumsverkehr geöffnet sind.[1538] Die Verarbeitung der personenbezogenen Daten der dort tätigen Beschäftigten würde sich aber wohl dennoch nach Art. 6 Abs. 1 UAbs. 1 lit. b oder f DS-GVO richten. Dies zeigt ein Blick auf die Rechtslage zur Vorgängernorm in § 6b BDSG 2003, welche der Gesetzgeber lediglich mit § 4 BDSG 2018 fortschreiben wollte[1539].

1379 Der Gesetzgeber hatte zumindest nicht-öffentliche Räume gerade im Hinblick auf die spezielle Interessenlage im Beschäftigungsverhältnis bei der Einführung von § 6b BDSG 2003 bewusst ausgenommen.[1540] Die Interessenlage der Beschäftigten weicht nämlich erheblich von der in § 4b BDSG 2018 bzw. § 6b BDSG 2003 ab. Anders als Kunden in einem Geschäft sind Beschäftigte dem Arbeitgeber als für die Videoüberwachung Verantwortlichen bekannt und halten sich dort auch nicht nur vorübergehend, sondern beinahe täglich und für längere Zeit auf.[1541] Der Überwachungsdruck für Beschäftigte ist also ungleich höher. Dies gilt unabhängig davon, ob der Arbeitsplatz in einem öffentlichen oder in einem nicht-öffentlichen Raum liegt.[1542]

1380 Es spricht folglich viel dafür, dass sich die Videoüberwachung auch in beiden Fällen nach Art. 6 UAbs. 1 UAbs. 1 lit. b oder f DS-GVO richtet und nicht nach § 4 BDSG 2018.[1543] Im Übrigen dürfte diese Situation für die Industrie 4.0 aber ohnehin nicht von Belang sein. Die Arbeitsräume sind

---

1537 Dazu ausführlich *Schneider/Schindler*, ZD 2018, S. 463–469.
1538 *Wedde*, in: Däubler et al. 2020, § 26 BDSG, Rn. 120.
1539 BT-Drucks. 18/11325, S. 81.
1540 BT-Drucks. 14/4329, S. 38; BAG v. 29.6.2004 – 1 ABR 21/03, E 111, S. 173, Rn. 27 (=NZA 2004, S. 1278).
1541 BAG v. 29.6.2004 – 1 ABR 21/03, E 111, S. 173, Rn. 27 (=NZA 2004, S. 1278).
1542 BAG v. 22.9.2016 – 2 AZR 848/15, E 156, S. 370, Rn. 43 (=NZA 2017, S. 112).
1543 Für das Verhältnis von § 32 Abs. 1 S. 1 BDSG 2003 und § 6b BDSG 2003 BAG v. 22.9.2016 – 2 AZR 848/15, E 156, S. 370, Rn. 43 (=NZA 2017, S. 112); für das Verhältnis von § 4 zu § 26 Abs. 1 S. 1 BDSG 2018 *Forst*, in: Auernhammer 2020, § 26 BDSG, Rn. 147. Ablehnend zu dieser Sonderregelung für das Beschäftigungsverhältnis nach altem Recht dagegen *Jerchel/Schubert*, DuD 2015, S. 151, 152.

hier in der Regel nur den Betriebsangehörigen zugänglich und damit nicht öffentlich. § 4 BDSG 2018 käme damit auch nicht zur Anwendung, wenn man die weitgehende Sonderrolle des Beschäftigungsverhältnisses ablehnt.

Aus dem Verhältnis der Erlaubnistatbestände wird schließlich auch klar, dass man für die Interessenabwägung in Art. 6 Abs. 1 UAbs. 1 lit. b (dazu 3.4.1.3.4.2.1, S. 381) oder f DS-GVO aus § 4 BDSG keine Schlüsse ziehen kann. Es gilt also insbesondere nicht, dass eine Videoüberwachung, die in öffentlich zugänglichen Räumen unzulässig wäre, mit großer Wahrscheinlichkeit auch in nicht öffentlich zugänglichen Räumen rechtswidrig wäre.[1544] Die Regelung in § 4 BDSG ist für kamerabasierte Assistenzsysteme darum ohne Belang. 1381

3.6.2.1.2 Die Zulässigkeit der Verarbeitung

Bild- und besonders Videoaufnahmen eines Menschen enthalten in der Regel viele Informationen über die abgebildete Person. Sie geben Aufschluss über das Alter, das Geschlecht und die ethnische Herkunft sowie ggf. über den emotionalen Zustand, die gesundheitliche Verfassung und zentrale Charaktereigenschaften des Abgebildeten.[1545] Der Mensch ist von Kindheit an geradezu darauf trainiert, den anderen anhand optischer Eindrücke zu beurteilen und einzuordnen.[1546] Die Videoüberwachung stellt darum einen schwerwiegenden Eingriff[1547] (siehe 3.2.3.5.2, S. 301) in das Recht am eigenen Bild dar, das als spezielle Ausprägung des Rechts auf Schutz personenbezogener Daten nach Art. 7 und 8 GRC angesehen werden kann. 1382

3.6.2.1.2.1 Videoüberwachung zu Kontrollzwecken

Eine Videoüberwachung zu Kontrollzwecken wird oft heimlich durchgeführt. Angesichts des schwerwiegenden Eingriffs, der mit Videoaufnahmen allgemein verbunden ist, gelten hier verschärfte Anforderungen. Nur die Aufdeckung von Straftaten nach § 26 Abs. 1 S. 2 BDSG 2018 kann eine 1383

1544 So aber noch *Hofmann,* ZD 2016, S. 12, 16; und wohl auch *Däubler,* NZA 2017, S. 1481, 1484.
1545 *Schneider/Schindler,* ZD 2018, S. 463, 466 f.
1546 *Rose,* ZD 2017, S. 64, 66 m.w.N.
1547 Zu den Kriterien für die Eingriffstiefe *Pötters/Traut,* RDV 2013, S. 132, 135.

verdecke Videoüberwachung rechtfertigen. Im Übrigen lassen sich die Informationspflichten nach Art. 13 Abs. 1 und 2 DS-GVO nicht beschränken (siehe 3.4.1.5.3, S. 410). Zu Kontrollzwecken ist eine verdeckte Videoüberwachung ausgeschlossen.

1384 Für eine nur teilweise verdeckte Videoüberwachung, bei der offen auf die Kameras hingewiesen wird, es aber nicht zu erkennen ist, ob sie angeschaltet sind, gelten ähnlich strenge Anforderungen. Da hier aber nicht einzelne Beschäftigte,[1548] sondern in der Regel ein bestimmter Bereich überwacht werden soll, muss sich der Verdacht auf den ganzen Bereich beziehen.[1549]

1385 Den Grundsätzen der Rechtsprechung lässt sich entnehmen, dass auch der mit einer offenen Videoüberwachung verbundene Überwachungsdruck nur bei konkreten Anhaltspunkten für eine starke Beeinträchtigung der Interessen des Arbeitgebers zu rechtfertigen ist.[1550] Das bloße Interesse an der Kontrolle der Erfüllung der arbeitsvertraglichen Leistungspflicht reicht dazu grundsätzlich nicht aus. Eine Ausnahme könnte allenfalls dann gemacht werden, wenn der Überwachungsdruck erheblich gesenkt werden würde, etwa wenn sich die Videoüberwachung auf einzelne eng umgrenzte Bereiche beschränkte, die – vergleichbar mit der Situation in Callcentern (siehe 3.4.1.5.3.4, S. 414) – andernfalls gar nicht kontrolliert werden könnten. Im Kontext der Industrie 4.0 ist aber kein solcher Einsatzbereich ersichtlich. Videoüberwachung zur Kontrollzwecken ist darum in aller Regel unzulässig.[1551]

3.6.2.1.2.2 Videoüberwachung zur Einsichtnahme

1386 Auch die Einsichtnahme ist nur in engen Grenzen möglich. Dies zeigt sich z.B. bei dem eingangs erwähnten System zur Kollisionsvermeidung (siehe

---

1548 Dies schließt nicht aus, dass Zufallsfunde verwertet werden dürfen, die bei Personen gemacht wurden, gegen die kein konkreter Verdacht bestand, solange die Maßnahme an sich auf einem konkreten Verdacht gegen eine hinreichend abgegrenzte Gruppe basierte, siehe BAG v. 22.9.2016 – 2 AZR 848/15, E 156, S. 370, Rn. 30 (=NZA 2017, S. 112).

1549 BAG v. 14.12.2004 – 1 ABR 34/03, AP § 87 BetrVG 1972 Überwachung Nr. 42 (=RDV 2005, S. 216); BAG v. 22.9.2016 – 2 AZR 848/15, E 156, S. 370, Rn. 41 (=NZA 2017, S. 112).

1550 So auch *Däubler,* NZA 2017, S. 1481, 1484; *Maschmann,* NZA-Beil. 2018, S. 115, 120.

1551 *Däubler* 2019, Rn. 312; *Jerchel/Schubert,* DuD 2015, S. 151, 154.

1.3.3, S. 72). Der Zweck dieser Anlagen, Kollisionen zu vermeiden, erfordert es nicht, die zu schützende Person zu identifizieren. Die Fähigkeit des Systems zur Erkennung identifizierender Merkmale ist entsprechend zu begrenzen. Gelingt dies, sind lediglich die Videoaufnahmen selbst noch problematisch. Da sie nur für die in Echtzeit ablaufende Objekterkennung benötigt werden, ist es nicht erforderlich, die Aufnahmen aufzuzeichnen oder auszuspielen. Soweit die Funktion kamerabasierter Systeme realisiert werden kann, ohne dass personenbezogene Daten erhoben werden, ist dies auch so umzusetzen.

Die Videoaufnahmen könnten über den eigentlichen Einsatzzweck aber auch zur Beweissicherung eingesetzt werden, um z.B. später Regressansprüche geltend zu machen. Die Tatsache, dass dieses Vorgehen zumindest bei permanenter und anlassloser Aufzeichnung nach Ansicht des Bundesgerichtshofs im Falle des Einsatzes so genannter Dashcams im öffentlichen Raum unzulässig ist,[1552] schließt es im Beschäftigungsverhältnis zwar nicht aus (siehe 3.6.2.1.1, S. 525). Arbeitnehmer genießen aber nach den Grundsätzen des innerbetrieblichen Schadensausgleichs[1553] eine Haftungsbegrenzung, die eine persönliche Haftung weitgehend ausschließt. Wenn sich folglich aber ohnehin kein relevanter Regress nehmen lässt, ist es wohl nicht erforderlich, zumindest aber unangemessen, die Aufnahmen längerfristig personenbezogen zu speichern.[1554] Dem Arbeitgeber bliebe allerdings die Möglichkeit, die personenbezogenen Merkmale in den Aufnahmen automatisiert unkenntlich zu machen.[1555] 1387

Außerhalb der genannten Beispiele für kamerabasierte Assistenzsysteme mögen dennoch Situationen bestehen, in denen der Einsatz von Videoüberwachung zur Produktionssteuerung im engeren Sinne erforderlich ist. In diesen Fällen ist die Datenverarbeitung nur zulässig, wenn das Recht der Beschäftigten auf Schutz ihrer personenbezogenen Daten nur marginal betroffen ist.[1556] Dies wurde z.B. für das Monitoring von Standbildern ohne Zoomfunktion bejaht, weil der Personenbezug hier angesichts der geringen Bildauflösung von niedriger Qualität (siehe 3.2.3.5.3, S. 302) und die Kontrolldichte so gering war (siehe 3.2.3.5.2, S. 301), dass eine ernst- 1388

1552 BGH v. 15.5.2018 – VI ZR 233/17, Z 218, S. 348, Rn. 19 (=NJW 2018, S. 2883).
1553 BAG v. 30.8.1966 – 1 AZR 456/65, E 19, S. 66 (=NJW 1967, S. 269); BeckOGK/*Feuerborn*, § 619a BGB, Rn. 58.
1554 So auch *Bäcker* 2012, S. 40 f., der eine Videoüberwachung auch im Räumen mit Schadensdisposition ablehnt.
1555 S. die Funktion bei YouTube *Förster,* Heise Online, 19.7.2012.
1556 *Däubler* 2019, Rn. 312.

hafte Beeinträchtigung der Interessen der Beschäftigten unwahrscheinlich erschien.[1557]

3.6.2.2 Verarbeitung von Standortdaten

1389 Die Verarbeitung von Standortdaten weist im Hinblick auf den Personenbezug und die Erlaubnistatbestände einige Besonderheiten auf. So wird erstens genau genommen oftmals nicht der Mitarbeiter, sondern lediglich das Assistenzsystem selbst geortet. Ein Personenbezug könnte insofern nur indirekt hergestellt werden, entweder, weil der Arbeitgeber positiv weiß, dass sich der Mitarbeiter in der Nähe des Systems aufhält oder auch nur, weil er das System typischerweise mit dem Mitarbeiter verbindet.[1558] Solange ein Zweckelement vorliegt, ist aber unproblematisch von einem Personenbezug auszugehen (siehe 3.3.1.2.2, S. 318).

1390 Die zweite Besonderheit besteht darin, dass Standortdaten nicht nur dann anfallen, wenn eine Person von anderen geortet wird, sondern auch dann, wenn sie – also wiederum genau genommen das Gerät – sich selbst ortet. Wenn das Gerät die Positionsdaten nicht übermittelt, kann dies dazu führen, dass der Tatbestand des Erhebens durch den Verantwortlichen als Teil der Verarbeitung nach Art. 4 Nr. 2 DS-GVO entfällt.[1559] Dies setzt allerdings voraus, dass der Verantwortliche keinen Zugriff auf die fragliche Information hat und ihm auch die rechtlichen Mittel fehlen, sich diesen Zugriff zu verschaffen. Das wäre nur der Fall, wenn die Information nur vorübergehend auf dem Gerät zwischengespeichert würde. Die Kenntnisnahme durch den Arbeitgeber wäre hier so unwahrscheinlich, dass ausnahmsweise keine personenbezogenen Daten verarbeitet würden (siehe 3.3.4.6, S. 344).

1391 Bei sämtlichen längerfristig gespeicherten Informationen ist dagegen zu beachten, dass sich der Arbeitgeber Zugriff auf den Gerätespeicher verschaffen kann und darf. In diesen Fällen ist darum von einem Personenbezug auszugehen.[1560]

1557 LAG Schleswig-Holstein v. 29.8.2013 – 5 TaBV 6/13, NZA-RR 2013, S. 577, 582.
1558 *Göpfert/Papst,* DB 2016, S. 1015, 1017.
1559 *Schnabel* 2009, S. 255. Zur technischen Umsetzung siehe *Lucke, et al.* 2008.
1560 A.A. noch *Hofmann,* ZD 2016, S. 12, 16.

3.6.2.2.1 Die Zulässigkeit der Verarbeitung im Allgemeinen

Personenbezogene Standortdaten geben keinen derart unmittelbaren und intuitiv erfassbaren Einblick in die Persönlichkeit der betroffenen Person, wie dies bei Bild- und Videoaufnahmen der Fall ist. Sie erlauben aber demjenigen, der den Kontext des jeweiligen Standorts kennt, Rückschlüsse auf das Verhalten und die sozialen Beziehungen des Betroffenen zu ziehen.[1561] Wer sich wann wie lange mit wem trifft, wird im Beschäftigungsverhältnis zwar wesentlich von den Notwendigkeiten des Arbeitsalltags bestimmt. Da dieser Alltag aber nicht allein von roboterhafter Pflichterfüllung, sondern auch von sozialer Interaktion geprägt ist, können Standortdaten eine hohe Persönlichkeitsrelevanz aufweisen. Dies gilt besonders, wenn sie zu detaillierten Bewegungsprofilen zusammengesetzt werden, weil dann über die Person auch solche Aussagen getroffen werden können, die keinen direkten Bezug mehr zum Arbeitsverhältnis aufweisen. 1392

Die Verarbeitung von Standortdaten unterliegt den allgemeinen Grenzen der Angemessenheit (siehe 3.6.1.2.3, S. 508), was sich hier besonders im Hinblick auf kontrollfreie Räume im wörtlichen Sinne bemerkbar macht (siehe 3.6.1.2.3.2, S. 510). Im übertragenen Sinne wirkt dieses Verbot hier dagegen nicht absolut, weil der Aufenthaltsort einer Person zwar wesentliche, aber bei Weitem nicht alle Aspekte ihres Verhaltens betrifft. Unter engen Voraussetzungen sind Ausnahmen darum durchaus möglich. In der Literatur anerkannt sind Konstellationen, in denen die abschnittsweise auch längere Ortung der Sicherheit dient, wobei sowohl die Sicherheit hoher Vermögenswerte des Arbeitgebers oder seiner Partner[1562] als auch die Sicherheit des Beschäftigten[1563] in Frage kommt. Das Anlegen ganzer Bewegungsprofile ist aber auch in diesen Fällen unzulässig.[1564] 1393

In Konstellationen, welche die zeitweise permanente Ortung nicht rechtfertigen, ist die Datenerhebung auf den konkreten Informationsbedarf zu beschränken. Dies läuft in der Regel auf eine anlassbezogene Ortung hi- 1394

1561 *Scholz, et al.* 2013.
1562 *Kopp/Sokoll,* NZA 2015, S. 1352, 1355; *Seifert,* in: Simitis 2014, § 32 BDSG, Rn. 82 f.; *Wedde,* in: Däubler et al. 2020, § 26 BDSG, Rn. 131.
1563 *Gola,* NZA 2007, S. 1139, 1142; *Kort,* RdA 2018, S. 24, 28; *Varadinek, et al.* 2018, S. 31; *Wedde,* in: Däubler et al. 2020, § 26 BDSG, Rn. 133.
1564 *Däubler,* NZA 2017, S. 1481, 1486; *Kopp/Sokoll,* NZA 2015, S. 1352, 1355; *Kort,* RdA 2018, S. 24, 27 f.

naus.[1565] Für weitergehende Einschränkungen findet sich im Gesetz keine Stütze.[1566]

3.6.2.2.2 Ortung zu Kontrollzwecken

1395 Ähnlich wie bei der Verarbeitung von Bild- und Videodaten bestehen gegen die Verwendung von Standortdaten für Leistungs- und Verhaltenskontrollen bereits grundsätzliche Bedenken. In begründeten Ausnahmefällen wird man aber auch hier eine Datenverarbeitung zu Kontrollzwecken zulassen müssen. Der Eingriff ist zwar ebenfalls erheblich, in seiner Intensität aber nur bei sehr umfassender Datenverarbeitung mit dem Eingriff bei Bild- und Videoaufnahmen zu vergleichen.[1567] Eine Kontrolle kann darum jedenfalls unter denselben Voraussetzungen wie eine Videoüberwachung gerechtfertigt sein, also bei konkreten Anhaltspunkten für eine starke Beeinträchtigung der Interessen des Arbeitgebers.

1396 Die Erfassung von Standortdaten unterhalb des Aussagegehalts von Bewegungsprofilen muss entsprechend des geringeren Überwachungsdrucks[1568] nicht in demselben Maße gerechtfertigt werden. Die Anforderungen an die beeinträchtigten Interessen des Verantwortlichen sind hier niedriger anzusetzen.[1569] Einen Anhaltspunkt hierfür gibt ein Vergleich mit § 26 Abs. 1 S. 2 BDSG 2018. Diese Norm kann selbst eine verdeckte Videoüber-

---

1565 *Gola*, ZD 2012, S. 308, 310; *Hofmann/Hornung* 2018, S. 246; BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 164. Zu ähnlichen Problemen beim eCall-System *Pohle/Zoch*, CR 2014, S. 409, 412 ff.

1566 A.A. *Steidle* 2005, S. 308 f.; *Steidle*, MMR 2009, S. 167, 170, der § 28 Abs. 1 Satz 1 Nr. 1 BDSG (nach alter Rechtslage; auf § 26 Abs. 1 Satz 1 BSDG 2018 übertragbar) als Erlaubnistatbestand für untauglich hält. Hierfür bemüht er die Wertung der § 98 Abs. 1 TKG und Art. 9 EK-DSRL, welche nach Art. 95 DS-GVO neben der Datenschutz-Grundverordnung weiterhin gilt. Diese Regelungen betreffen die Ortung durch den Mobilfunkanbieter und erfordern stets die Einwilligung des Teilnehmers, selbst, wenn die Ortung im Rahmen des für den gewählten Dienstes mit Zusatznutzen erforderlich sind. Diese Wertung kann aber auf das Arbeitsverhältnis schon deswegen nicht übertragen werden, weil dem Mobilfunkanbieter keine berechtigten Interessen zustehen, die denen des Arbeitgebers vergleichbar wären.

1567 *Göpfert/Papst*, DB 2016, S. 1015, 1017.

1568 Zur GPS-Technik BVerfG v. 12.4.2005 – 2 BvR 581/01, E 112, S. 304, 317 – *GPS-Observation*. Zum Vergleich der Ortung zur Telekommunikationsüberwachung EGMR v. 2.9.2010 – 35623/05, NJW 2011, S. 1333, Rn. 66 – *Uzun/Deutschland*.

1569 *Beckschulze*, DB 2009, S. 2097, 2099; a.A. *Kort*, RdA 2018, S. 24, 27.

wachung rechtfertigen (siehe 3.4.1.5.3.4, S. 414 und 3.6.2.1.2.1, S. 527) benötigt hierfür aber auf der Seite der beeinträchtigten Interessen des Arbeitgebers eine Straftat im Beschäftigungsverhältnis. Für die Standortdatenverarbeitung könnte eine Stufe niedriger auf das Kündigungsschutzrecht abgestellt werden. Denkbar wäre, Verfehlungen genügen zu lassen, die eine verhaltensbedingte Kündigung rechtfertigten.

Eine routinemäßige, d.h. nicht durch konkrete Anhaltspunkte für eine Interessenbeeinträchtigung veranlasste Datenerhebung wird man aber auch hier ablehnen müssen. Insgesamt ergeben sich also nur graduelle, aber keine grundlegend konzeptionellen Unterschiede zur Videoüberwachung. Sowohl die Videoüberwachung als auch die Ortung verlangen beide konkrete Anhaltspunkte für eine Beeinträchtigung. Diese Beeinträchtigung muss bei der Ortung aber nicht so stark ausfallen. 1397

Eine Verschärfung der Anforderungen an die beeinträchtigten Interessen des Arbeitgebers bis auf das Niveau der Videoüberwachung ist hingegen wieder geboten, wenn Daten, die zur Einsichtnahme gewonnen wurden, zur Kontrollzwecken zweckentfremdet werden sollen. Dieser Kontextwechsel ist im Rahmen der Vereinbarkeitsprüfung eingriffsvertiefend zu werten. Entsprechend müssen auch die Rechtfertigungsanforderungen erhöht werden.[1570] 1398

3.6.2.2.3 Ortung zur Einsichtnahme

Die Verarbeitung personenbezogener Standortdaten zur Organisation der Arbeit ist angesichts der erheblichen Eingriffstiefe zwar voraussetzungsvoll, aber nicht grundlegend und insbesondere auch nicht[1571] für die Zwecke der Koordinierung der Arbeit abzulehnen.[1572] Der Schwerpunkt der Prüfung liegt bei der Erforderlichkeit im engeren Sinne. Dabei kann der Zweck nicht auf die Ortung von Mitarbeitern konkretisiert werden. Ent- 1399

1570 So i.E. auch *Wedde*, in: Däubler et al. 2020, § 26 BDSG, Rn. 131.

1571 A.A. *Zöll*, in: Taeger/Gabel 2019, § 26 BDSG, Rn. 57, der die Ortung ohne nähere Begründung nur zum Schutz des Arbeitnehmers oder wertvoller Gegenstände des Arbeitgebers erlauben will. Vgl. zur Verarbeitung – noch sensiblerer – Gesundheitsdaten zum Schutz der Beschäftigten, *Roßnagel, et al.* 2012, S. 86 f.

1572 *Gola*, ZD 2012, S. 308, 310; BeckOK DSR/*Riesenhuber*, § 26 BDSG, Rn. 164; *ULD*, LTSH-Drucks. 17/210, 6; a.A. wohl *Däubler*, NZA 2017, S. 1481, 1485; *Meyer*, K&R 2009, S. 14, 18; *Wedde*, in: Däubler et al. 2020, § 26 BDSG, Rn. 131 ff.

scheidend ist vielmehr, welche konkrete Funktionalität das Assistenzsystem haben soll (siehe 3.6.1.2.1.6, S. 505).[1573] Für sie muss der Standort des Mitarbeiters eine relevante Information darstellen.

1400 Eine mögliche Funktionalität könnte die Koordinierung der Arbeit sein,[1574] dergestalt, dass z.B. Wartungsaufträge an denjenigen Mitarbeiter vergeben werden, der sie am schnellsten erledigen kann. Auch hier ist die Erforderlichkeit der Datenverarbeitung aber situationsbezogen genau zu ermitteln. Steht schon anderweitig fest, welcher Arbeiter adressiert werden soll, genügt es, dass dieser Mitarbeiter über das Kommunikationssystem erreichbar ist.[1575] In diesem Fall muss überhaupt niemand geortet werden. Steht fest, dass ein bestimmter Mitarbeiter überhaupt nicht verfügbar ist, kann zumindest bei ihm auf die Ortung verzichtet werden. Ist eine Ortung an sich erforderlich, hat sie nur anlassbezogen zu erfolgen.[1576] Auch eine Speicherung der Daten über den Zeitpunkt des konkreten Bedarfs hinaus dürfte in den meisten Fällen nicht notwendig sein.[1577] Die weitere Auswertung kann schließlich anonymisiert erfolgen.

1401 Eine Funktionalität wie die eben beschriebene kann aber u.U. auch komplett ohne die Verarbeitung personenbezogener Standortdaten realisiert werden. Statt auf mobilen Endgeräten, die den Beschäftigten persönlich zugeordnet sind und die im Fall einer Anfrage geortet werden, basiert ein datenschutzfreundlicher Ansatz darauf, im Betriebsgelände Terminals zu verteilen, die diese Funktion übernehmen.[1578] Die Reparaturanfrage eines Geräts wird an die Terminals gesendet, von denen die Arbeiter die Aufgaben einsehen und „abholen", d.h. zur eigenen Erledigung markieren können. In diesem Fall wird allenfalls der Standort des abholenden Mitarbeiters ermittelt, nicht aller potenziell für die Aufgabe in Betracht kommenden Mitarbeiter. In der Folge wird nicht der Mitarbeiter selbst, sondern nur die Aufgabe und das dafür benötigte – ihm nicht exklusiv zugeordne-

---

1573 Das übersieht *Meyer,* K&R 2009, S. 14, 18, wenn er die Ortung allenfalls auf die Wahrung berechtigter Interessen stützen will.

1574 Vgl. *Arning/Born,* in: Forgó et al. 2019, Teil XI Kapitel 2, Rn. 37; *Däubler* 2019, 322; *Gola,* ZD 2012, S. 308, 310; *Gola, et al.* 2016, 1258 Vgl. zur Verarbeitung von Gesundheitsdaten zur Einsatzkoordinierung bei Feuerwehrleuten *Roßnagel, et al.* 2012, S. 95 f.

1575 So ähnlich bei *Wieland, et al.* 2009, S. 17. Zu Außendienstmitarbeitern VG Lüneburg v. 19.3.2019 – 4 A 12/19, CR 2019, S. 367, Rn. 43; *Däubler,* NZA 2017, S. 1481, 1485.

1576 *Hallaschka/Jandt,* MMR 2006, S. 436, 439.

1577 *Gola,* ZD 2012, S. 308, 310; *ULD,* LTSH-Drucks. 17/210, S. 98 f.

1578 *Wieland, et al.* 2009, S. 18 ff.

te – Werkzeug getrackt. So können einzelne Aufgabenteile trotzdem von anderen Mitarbeitern übernommen werden.

Ob eine solche datenschutzfreundliche standortbasierte Verteilung von Aufgaben als Rechtspflicht zu bevorzugen ist, bestimmt sich anhand der gleichen Eignung der Methode. Hier spielen in erster Linie die Kosten und der Unterhaltungsaufwand für die Terminals bzw. die mobilen Endgeräte eine Rolle. Sie sind nach dem hier gewählten Prüfungsschema objektiv zu bestimmen (siehe 3.4.1.3.3.2, S. 377), sodass der Arbeitgeber hier keinen Entscheidungsspielraum genießt. Denkbar ist aber, dass sich Synergieeffekte ergeben, weil der Arbeitgeber z.B. ohnehin plant, die Mitarbeiter mit mobilen Endgeräten auszustatten, etwa um die Kommunikation zu erleichtern. Insofern könnte eine unternehmerische Entscheidung doch den Ausschlag in der Erforderlichkeitsprüfung geben. 1402

Wo eine Form der Ortung für die konkrete Funktionalität letztlich notwendig ist, bestehen verschiedene Ansätze, die damit verbundene Eingriffsintensität zu verringern. So könnten z.B. solche Geräte eingesetzt werden, die sich selbst orten und ihre Positionsdaten ggf. einer autorisierten Stelle – z.B. einer wartungsbedürftigen Maschine oder einem hilfesuchenden Mitarbeiter – nur auf Anfrage mitteilen. Denkbar wäre auch, es dem Mitarbeiter zu ermöglichen, seine Ortung zeitweilig zu unterbinden.[1579] Und schließlich könnten statt zentraler Instanzen dezentrale, auf P2P-Verbindungen aufbauende Systeme eingesetzt werden.[1580] 1403

Welcher dieser Ansätze einer datenschutzfreundlichen Technikgestaltung im Sinne des Art. 25 Abs. 1 DS-GVO schließlich gewählt werden muss, bemisst sich nach den oben dargelegten Grundsätzen (3.4.2.2.5.6, S. 457) für die Höhe des Risikos, den Schutzstandard der Technik und den konkreten Kosten für die Umsetzung des Systems. Die Ortung von Beschäftigten zu Zwecken der Einsichtnahme ist im Zweifel mit einem hohen Risiko verbunden. Zwar ist der Zweck hier eher unverfänglich; Standortdaten sind aber vergleichsweise sensible Informationen und insofern anfällig für Missbrauch. 1404

1579 *ULD*, LTSH-Drucks. 17/210, S. 99.
1580 Zum Ganzen *Steidle* 2005, S. 367 ff.

3.6.2.3 Verarbeitung von Betriebsdaten

1405 Der Begriff der Betriebsdaten soll hier als Auffangtatbestand für sämtliche anderweitig in der Smart Factory anfallenden personenbezogenen Daten verwendet werden. Darunter fallen Daten über die Art und Weise, wie ein Mitarbeiter mit einem Produktions- oder Assistenzsystem interagiert, welche Einstellungen er an einer Maschine vorgenommen hat oder wie lange er für die Bearbeitung eines Auftrags benötigt hat.

1406 Bei Betriebsdaten dürfte noch häufiger als bei Video- und Standortdaten in Frage stehen, ob sie einen Personenbezug aufweisen. Gerade in Bereichen, in denen eine personenbezogene Verwendung der Daten nicht bezweckt ist, gilt es das Ergebniselement sorgsam zu untersuchen. Nicht jede abstrakt mögliche Zuordnung der Informationen zu einer Person führt dazu, dass die Identifizierung der Person auch hinreichend wahrscheinlich ist. Ein handhabbares Kriterium stellt hierfür die Unterscheidung zwischen der ungezielten Verarbeitung und Daten ohne gezieltem Personenbezug dar (siehe 3.3.4.3, S. 338).

3.6.2.3.1 Zulässigkeit der Verarbeitung im Allgemeinen

1407 Einzelne personenbezogene Betriebsdaten weisen im Gegensatz zu Video- und Standortdaten für sich genommen kaum je eine signifikante Persönlichkeitsrelevanz auf. Hier kommt die Grundannahme des Datenschutzes zum Tragen, der zufolge nicht das einzelne Datum für sich, sondern der Verarbeitungskontext über die Grundrechtsbeeinträchtigung entscheidet (siehe 3.2.3.5, S. 299). Anders als bei der Videoüberwachung und der Verarbeitung von Standortdaten kann die Verarbeitung von Betriebsdaten darum das volle Spektrum der Eingriffstiefe bedienen.

1408 Das Verbot der Totalüberwachung gilt auch für die Verarbeitung von Betriebsdaten. Was als Totalüberwachung zu bewerten ist, hängt aber wesentlich von der Gestalt des Assistenzsystems ab. Assistenzsysteme, die nur eine begrenzte Anzahl an Parametern erfassen, können auch dann nicht als Totalüberwachung eingeordnet werden, wenn sie permanent sämtliche Interaktionen des Beschäftigten erfassen oder gar aufzeichnen. Solche Systeme bilden von vornherein nur einen Ausschnitt des Arbeitsverhaltens des Beschäftigten ab. Dies gilt umso mehr, wenn die betreffenden Werte nicht dauerhaft gespeichert, sondern nur zur Ermittlung von Durchschnittswer-

ten herangezogen werden.[1581] Die Grenze zur unter allen Umständen verbotenen Totalüberwachung wäre also nur erreicht, wenn das komplette Arbeitsverhalten des Beschäftigten erfasst würde.[1582]

3.6.2.3.2 Verarbeitung von Betriebsdaten zur Kontrollzwecken

Leistungs- und Verhaltenskontrollen auf der Grundlage von Betriebsdaten sind zwar nicht voraussetzungslos, angesichts der vergleichsweise geringen Persönlichkeitsrelevanz dieser Parameter aber mit den geringsten Anforderungen verbunden. Aus dem Beschäftigungsverhältnis, insbesondere aus der Personalplanung, ergibt sich unmittelbar die Notwendigkeit, die Tätigkeit der Beschäftigten von Zeit zu Zeit zu beurteilen (siehe 3.6.1.2.3.1.2, S. 509). Die Kontrolle der Leistung oder des Verhaltens muss aber nicht zwingend mit der systematischen Erfassung von Betriebsdaten einhergehen. Der Arbeitgeber kann sich z.B. auf die Beobachtungen und Einschätzungen seiner Führungskräfte verlassen und sich dabei auf die Kontrolle des Arbeitsergebnisses beschränken. 1409

Daran zeigt sich der Maßstab der datenschutzrechtlichen Prüfung: Ob der Arbeitnehmer Kontrollen durchführt, unterliegt seiner unternehmerischen Entscheidungsfreiheit, die sich insofern in seiner Zwecksetzungsbefugnis äußert. Im Hinblick auf die genaue Ausgestaltung der Kontrollen unterliegt der Arbeitgeber dagegen der vollen gerichtlichen Kontrolle nach dem Erforderlichkeitsprinzip. 1410

3.6.2.3.2.1 Bezugspunkt der Erforderlichkeitsprüfung

Die Entscheidung, die systematische Erfassung und Auswertung von Betriebsdaten überhaupt als Kontrollinstrument einzusetzen, wird in der Regel kaum zu hinterfragen sein. Es ist unmittelbar einsichtig, dass komplexe Tatbestände – in diesem Fall die Leistung und/oder das Verhalten des Beschäftigten – besser eingeschätzt werden können, wenn dies auf der Grundlage einer objektiven Datenbasis geschieht. Die Werte könnten zwar u.U. auch manuell erfasst, aufgezeichnet und ausgewertet werden. Diese Methode ist aber zumindest aufwändiger und folglich weniger geeignet 1411

1581 BAG v. 17.11.2016 – 2 AZR 730/15, NZA 2017, S. 394, Rn. 35.

1582 BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 30 ff. (=NZA 2017, S. 1205); *Wächter* 2014, Rn. 221.

(siehe 3.6.1.2.2, S. 506). Problematisch sind insofern nur jene Fälle, in denen die gewählten Parameter zu wenig aussagekräftig und deshalb ungeeignet sind.[1583]

1412 Der Bezugspunkt der Erforderlichkeitsprüfung ist weniger in der Art, als vielmehr im Umfang der Datenverarbeitung zu sehen. Der Arbeitgeber muss zwar spätestens auf der Ebene der Angemessenheit einen der Totalüberwachung auch nur ähnlichen Überwachungsdruck vermeiden. In der Regel wird eine durchgehende und umfassende Verarbeitung von Betriebsdaten aber auch nicht erforderlich sein. Eine gängige Methode, um den Überwachungsdruck auf ein notwendiges bzw. angemessenes Maß zu senken, besteht darin, die Datenverarbeitung auf die Fälle zu beschränken, in denen ein konkreter Verdacht für eine Pflichtverletzung besteht. Nach diesem Prinzip ist auch die Verarbeitung von Video- oder Standortdaten (siehe 3.6.2.1.2.1, S. 527 und 3.6.2.2.1, S. 531) zulässig. Für Betriebsdaten ergeben sich aber einige Besonderheiten.

1413 Die Verarbeitung von Video- oder Standortdaten ist per se ein erheblicher Eingriff in das Recht der Beschäftigten auf Schutz ihrer personenbezogenen Daten. Entsprechend ist eine von vornherein auf Kontrolle angelegte Verarbeitung dieser Daten unzulässig. Der legitimierende Verdacht muss sich aus anderweitig erlangten Erkenntnissen ergeben. Die Verarbeitung von Betriebsdaten ist dagegen nicht zwingend in verstärktem Maße persönlichkeitsrelevant, sodass der Überwachungsdruck hier auch durch eine Einschränkung der Verarbeitung gesenkt werden kann.

3.6.2.3.2.2 Maßnahmen zur Senkung des Überwachungsdrucks

1414 Eine Möglichkeit, den Überwachungsdruck zu senken, besteht darin, die Verarbeitung von Betriebsdaten auf stichprobenartige Kontrollen zu beschränken, wie dies z.B. bei solch persönlichkeitsrelevanten Instrumenten wie der Tor- und Taschenkontrolle anerkannt ist.[1584] Soll die Kontrolle dagegen permanent erfolgen, ist die Datenverarbeitung auf wenige abstrakte Kriterien zu beschränken, sodass insbesondere kein Beschäftigter beson-

---

1583 BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 26 (=NZA 2017, S. 1205).

1584 Zur Verarbeitung von Betriebsdaten BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 27 (=NZA 2017, S. 1205); BAG v. 27.7.2017 – 2 AZR 681/16, E 159, S. 380, Rn. 31 (=NZA 2017, S. 1327). So wohl auch *Däubler*, CR 1994, S. 101, 108. Zur Torkontrolle BAG v. 15.4.2014 – 1 ABR 2/13 (B), E 148, S. 26, Rn. 47 (=NZA 2014, S. 551).

ders unter Verdacht gestellt wird. Ergibt sich auf der Grundlage dieser Daten ein Verdacht, kann die Kontrolle für den einzelnen Beschäftigten dann auch breitflächiger erfolgen.[1585]

Damit sie aber eine breit angelegte Kontrolle rechtfertigen kann, muss die Verdachtsermittlung selbst einigen Voraussetzungen genügen. Neben der Beschränkung der verarbeiteten Parameter und der Speicherdauer dieser Daten[1586] muss vor allem das Verfahren transparent gestaltet sein. So hat das Bundesarbeitsgericht in einem – vordergründig zwar auf Einsichtnahme angelegten[1587] – Fall bemängelt, dass die Sollwerte, die zu verfehlen einen Verdacht auslöste, vom Arbeitgeber nicht absolut und statisch bestimmt wurden, sondern sich dynamisch relativ zur Durchschnittsleistung einer Gruppe ergaben. Der Beschäftigte weiß in diesen Fällen nicht, welche Werte er zu erreichen hat und wie diese zu Stande kommen. Dies schafft ein Gefühl des Ausgeliefertseins und erhöht den Überwachungsdruck.[1588] 1415

3.6.2.3.3 Verarbeitung von Betriebsdaten zur Einsichtnahme

Hinsichtlich der Verarbeitung von Betriebsdaten zur Einsichtnahme ist dem Arbeitgeber oder den Betriebsparteien schließlich im Vergleich zu den anderen hier diskutierten Konstellationen der weiteste Entscheidungsspielraum zu gewähren. Dies drückt sich darin aus, dass die Festlegung der Funktionalität eines Assistenzsystems nur einer eingeschränkten, auf Willkürfreiheit und Plausibilität ausgelegten Kontrolle unterliegt (siehe 3.6.1.2.2, S. 506). 1416

Die eigentliche Prüfung der Erforderlichkeit und Angemessenheit verläuft nach allgemeinen Maßstäben. Ähnlich wie bei der Verarbeitung von Standortdaten lautet die Frage darum in erster Linie, ob die gewählte Funktionalität nicht auch mit anonymisierten Personendaten oder sogar nur mit reinen Maschinendaten zu bewältigen wäre. 1417

1585 BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 38 (=NZA 2017, S. 1205).

1586 BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 29 ff. (=NZA 2017, S. 1205) Für eine sofortige Löschung *Däubler*, CR 1994, S. 101, 108. Der Arbeitgeber muss aber einen Zeitraum wählen dürfen, in dem aussagekräftige Datenmengen erfasst werden können.

1587 BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 26 (=NZA 2017, S. 1205).

1588 BAG v. 25.4.2017 – 1 ABR 46/15, E 159, S. 49, Rn. 33 f. (=NZA 2017, S. 1205).

3.6.2.3.3.1 Technische Schutzmaßnahmen als Prüfungsschwerpunkt

1418 Anders als bei der Datenverarbeitung zu Kontrollzwecken, die auf individuelle arbeitsrechtliche Maßnahmen hinauslaufen, müssen Systeme zur Einsichtnahme nicht von vornherein so angelegt werden, dass die handelnden Personen ohne Weiteres rückverfolgbar bleiben. Dies eröffnet die Möglichkeit, Anonymisierungs- oder wenigstens (externe) Pseudonymisierungsmethoden einzuführen. Soweit der Einsatz solcher Maßnahmen dem Stand der Technik entspricht, ist der Arbeitgeber hierzu gemäß Art. 25 Abs. 1 DS-GVO auch grundsätzlich verpflichtet. Etwas anderes gilt nur, wenn das Risiko für die Rechte der betroffenen Beschäftigten nicht als hoch einzustufen ist, die technische oder organisatorische Schutzmaßnahme dafür aber den wirtschaftlichen Nutzen des Assistenzsystems in Frage stellen würde (siehe 3.4.2.2.6, S. 459).

1419 An dieser Stelle zeigen sich Überschneidungen zwischen der Pflicht zum Einsatz technischer oder organisatorischer Maßnahmen nach Art. 25 Abs. 1 DS-GVO und der Angemessenheitsprüfung. Wenn die Abwägung in Art. 25 Abs. 1 DS-GVO ergibt, dass der Arbeitgeber trotz hoher Kosten für Schutzmaßnahmen an dem Stand der Technik festhalten muss, wird dies in der Regel auch die einzige Möglichkeit sein, die abschließende Angemessenheitsprüfung zu bestehen, ohne die Funktionalität des Assistenzsystems beschneiden zu müssen. Geht die Risikoabwägung dagegen zugunsten des Arbeitgebers aus, darf dies in der Angemessenheitsprüfung nicht mehr konterkariert werden.

1420 Die Datenverarbeitung zur Einsichtnahme ist nicht per se als riskant einzustufen. Dies wäre nur der Fall, wenn andere Kriterien zu einer Risikoerhöhung beitrügen, etwa wenn besonders viele Daten erhoben würden, viele Personen darauf Zugriff erhielten oder lange Speicherfristen gewählt würden. Es ist demnach ziemlich wahrscheinlich, dass sich der Arbeitgeber außerhalb dieser Risikosituationen gemäß Art. 25 Abs. 1 DS-GVO auf vergleichsweise einfache Schutzmaßnahmen nach den anerkannten Regeln der Technik beschränken darf. Nicht selten dürften demnach eine nur interne Pseudonymisierung und eine – im Grunde ohnehin stets verpflichtende – Zugriffsbeschränkung auf die jeweilige Fachabteilung[1589] ausreichen.

1589 *Däubler* 2019, Rn. 407 ff.; *Wächter* 2014, Rn. 211.

3.6.2.3.3.2 Einzelne Funktionalitäten

Indessen kann nicht immer auf die Pseudonymisierung der Nutzer gesetzt werden. In Assistenzsystemen kann es eine Vielzahl von Funktionalitäten geben, die – vorausgesetzt, es werden wenigstens Schutzmaßnahmen nach den allgemeinen Regeln der Technik ergriffen – die Verarbeitung offen personenbezogener Beschäftigtendaten legitimieren können. 1421

3.6.2.3.3.2.1 Dokumentation und Analyse von Arbeitsvorgängen

Hierzu zählt z.B. die Dokumentation von Arbeitsvorgängen und -ergebnissen. Sollen die Mitarbeiter in der Lage sein, bspw. die Einstellungen an einer Maschine nachvollziehen und ggf. Rücksprache mit dem verantwortlichen Kollegen halten zu können, kann es notwendig sein festzuhalten, wer wann welche Einstellungen oder Reparaturen an einer Maschine vorgenommen hat.[1590] Das Gleiche gilt, falls der Arbeitgeber Fehleingaben oder Fehlbedienungen nachvollziehen und dadurch künftig vermeiden können will.[1591] 1422

Beide Zwecke rechtfertigen es grundsätzlich, personenbezogene Daten hierfür zu erheben. Teilweise kann sich dies bis zu einer rechtlichen Pflicht verdichten. Systeme, die es den Beschäftigten erlauben, auf personenbezogene Daten anderer oder auf sensible Unternehmensdaten zuzugreifen, müssen zum Schutz dieser Daten nämlich entsprechend abgesichert sein. Dies erfordert bereits aus Gründen der Datensicherheit, die Zugriffsberechtigung der Beschäftigten zu überprüfen und ihre Eingaben und Zugriffe individuell zuordenbar zu protokollieren.[1592] 1423

Das Anlegen von Mitarbeiterprofilen – und sei es nur die abstrakte Möglichkeit hierzu – kann hingegen mit keinem dieser Zwecke begründet werden. Entsprechend dürften die Daten nicht so gespeichert werden, dass sie im Hinblick auf den betroffenen Beschäftigten miteinander verknüpft werden können. 1424

Die Datenverarbeitung kann weiter dazu genutzt werden, einen etwaigen Schulungsbedarf bei den einzelnen Mitarbeitern zu erkennen.[1593] Eine er- 1425

1590 *Wächter* 2014, Rn. 221.
1591 LAG Köln v. 29.9.2014 – 2 Sa 181/14, NZA-RR 2015, S. 128, 130.
1592 *Martini*, in: Paal/Pauly 2018, Art. 32 DS-GVO, Rn. 37.
1593 BAG v. 14.11.2006 – 1 ABR 4/06, E 120, S. 146, Rn. 39 f. (=NZA 2007, S. 399); BAG v. 17.11.2016 – 2 AZR 730/15, NZA 2017, S. 394, Rn. 34 f.

höhte Risikostufe kann hier u.a. dadurch vermieden werden, dass Leistungs- und Verhaltenskontrollen und insbesondere über die Teilnahme an der Schulung hinausgehende arbeitsrechtliche Maßnahmen ausgeschlossen werden. Gerade Kollektivvereinbarungen eignen sich für derartige die Zweckbindung sichernde Regelungen. Darüber hinaus werden aber auch technische und organisatorische Maßnahmen erforderlich sein. In der Rechtsprechung hat z.B. ein System Anerkennung gefunden, bei dem die Daten zunächst nur (extern) pseudonymisiert erhoben wurden und die Auflösung des Pseudonyms unter dem Vorbehalt der Zustimmung des Betriebsrats stand.[1594]

3.6.2.3.3.2.2 Darstellung kontextbezogener Informationen

1426 Die meisten Assistenzsysteme, auf die in dieser Arbeit verwiesen wird (siehe 1.3.2, S. 71) zeichnen sich jedoch dadurch aus, dass sie den Beschäftigten kontextbezogen Informationen darstellen oder Handlungsanweisungen zu ihrer Arbeit geben. Eine solche Funktionalität ist nicht weniger legitim als die Dokumentation oder die Ermittlung des Schulungsbedarfs. Da sie sich aber in der Regel auch mit einer sehr eingeschränkten Datenverarbeitung realisieren lassen dürfte, kann sie nach dem Erforderlichkeitsprinzip auch nur geringe Eingriffe in das Recht der Beschäftigten auf Schutz ihrer personenbezogenen Daten rechtfertigen.

1427 Dies lässt sich an einem fiktiven Beispiel erläutern: Ein Assistenzsystem, dass einem Monteur die passende Anleitung für eine Reparatur anzeigt oder die jeweils relevanten Maschinenteile in seinem Blickfeld hervorhebt, benötigt hierfür nicht zwingend personenbezogene Daten. Soweit es z.B. nur darum geht, die Berechtigung des Bedieners zu prüfen, kann es u.U. mit anonymen Daten betrieben werden (siehe 3.4.2.2.7.2.2, S. 462). Soll das System auf die Präferenzen des Mitarbeiters hin personalisierbar sein, wäre allenfalls eine pseudonyme Datenverarbeitung denkbar. Eine längerfristige Datenspeicherung wird, wenn überhaupt, nur dezentral erforderlich sein.

1428 Dieses System könnte nun dahingehend erweitert werden, dass es Wartungsaufträge nicht nur an den nächstbefindlichen freien Mitarbeiter verteilt, sondern z.B. nicht eilige Aufträge jenen Arbeitern zuweist, die diesbezüglich noch Übungsbedarf haben. Die hierfür benötigten Daten müssen –

1594 BAG v. 17.11.2016 – 2 AZR 730/15, NZA 2017, S. 394, Rn. 35.

ggf. pseudonym – längerfristig vorgehalten werden. Der dauerhaft gespeicherte Datensatz könnte aber auf Fähigkeitsprofile beschränkt werden. Die Angaben darüber, wer wann welchen Auftrag wie schnell und wie zuverlässig erfüllt hat, müssten dann nur zur Auswertung zwischengespeichert werden. Gespeichert würde nur eine Note.[1595] Die gesteigerten Transparenzanforderungen aus dem Bereich der Kontrollmaßnahmen finden hier mangels möglicher arbeitsrechtlicher Konsequenzen keine Anwendung.

3.6.2.4 Übermittlung von Daten in Wertschöpfungsnetzwerken

Die Vernetzung von Assistenz- und vor allem Produktionssystemen ist nicht auf den innerbetrieblichen Einsatz beschränkt. Diese Systeme können unternehmensweit und ggf. auch unternehmensübergreifend in Wertschöpfungsnetzwerken miteinander kommunizieren (siehe 1.2.2, S. 63). Bei diesem Austausch geht es in erster Linie um Maschinendaten, die zur Abstimmung von Produktion und Logistik benötigt werden. 1429

Der Begriff des Wertschöpfungsnetzwerks bezeichnet keine bestimmte, in ihrem Inhalt feststehende Art der Zusammenarbeit. Er ist darum ebenso entwicklungsoffen wie der Begriff der Industrie 4.0 selbst. Im Grunde wird damit nur ausgedrückt, dass die beteiligten Unternehmen sehr eng miteinander zusammenarbeiten und Informationen nach einem gemeinsamen technischen Standard automatisiert miteinander austauschen – und dies stets sofort und u.U. mit sehr kleinen Informationspaketen. Beispielgebend für die Gestaltung eines Wertschöpfungsnetzwerks soll hier diejenige des „Industrial Data Space“[1596] herausgegriffen werden. 1430

3.6.2.4.1 Gemeinsame Verantwortlichkeit

Wenn Beschäftigte mit in Wertschöpfungsnetzwerke eingebundene Systemen interagieren, ist es aber nicht unwahrscheinlich, dass zumindest Daten ohne gezielten Personenbezug (siehe 3.3.4.3.2, S. 340) verarbeitet werden. Die enge Zusammenarbeit, wie sie in Wertschöpfungsnetzwerken üb- 1431

1595 Zum Scoring im Arbeitsverhältnis *Wächter* 2017, S. 227 f.

1596 *Fraunhofer* 2016. Die Initiative wurde später in „International Data Space“ umbenannt, *IDS* 2018. Da das dieser Betrachtung zugrundeliegende Whitepaper (*Fraunhofer* 2016) aber noch die alte Bezeichnung enthält, soll diese auch hier verwendet werden.

lich sein wird, wirft die Frage auf, ob die beteiligten Unternehmen dadurch zu gemeinsamen Verantwortlichen nach Art. 26 DS-GVO werden und welche Konsequenzen dies für die Datenverarbeitung und die Gestaltung der Systeme hätte.

3.6.2.4.1.1 Voraussetzungen der gemeinsamen Verantwortlichkeit

1432 Die Voraussetzungen der gemeinsamen Verantwortlichkeit sind denkbar abstrakt geregelt. Als gemeinsame Verantwortliche gelten gemäß Art. 4 Nr. 7 und 26 Abs. 1 S. 1 DS-GVO diejenigen, die das gemeinsam tun, was die Verantwortlichkeit im Sinne der Datenschutz-Grundverordnung ausmacht, nämlich die Festlegung von Zielen und Mitteln der Datenverarbeitung.

1433 Diese Voraussetzungen sind – ebenso wie bei der Bestimmung einer einzelnen Verantwortlichkeit – im Sinne eines wirksamen und umfassenden Schutzes der betroffenen Person weit auszulegen.[1597] Die Zusammenarbeit der gemeinsamen Verantwortlichen muss darum nicht auf Augenhöhe stattfinden und darf auch sehr arbeitsteilige Züge annehmen. So ist es für eine gemeinsame Verantwortlichkeit unschädlich, wenn nicht alle Beteiligten Zugriff auf die verarbeiteten Daten haben.[1598]

1434 Welches Maß an Beteiligung aber umgekehrt notwendig ist, steht bisher noch nicht fest. Der Europäische Gerichtshof hat sich in einer Reihe sehr stark einzelbezogener Urteile zur gemeinsamen Verantwortlichkeit im Sinne der Datenschutzrichtlinie geäußert. Daran lassen sich angesichts des unveränderten Wortlauts der Voraussetzungen[1599] wesentliche Hinweise für die Rechtslagenach der Datenschutz-Grundverordnung erkennen.

3.6.2.4.1.1.1 Die Entscheidung des EuGH zu Facebook

1435 Die wohl relevanteste Konstellation betraf die Verantwortlichkeit bei der Zusammenarbeit mit Facebook, der erste Fall einen Betreiber einer Face-

1597 EuGH, ECLI:EU:C:2018:388, Rn. 28 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*; kritisch zur damit einhergehenden Entfernung vom Wortlaut *Schulz,* ZD 2018, S. 363, 364.

1598 EuGH, ECLI:EU:C:2018:388, Rn. 38 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*.

1599 So auch BeckOK DSR/*Spoerr*, Art. 26 DS-GVO, Rn. 15.

book-Fanpage,[1600] der zweite Fall einen Website-Betreiber, der einen Like-Button auf seiner Seite eingebunden hatte.[1601] Beide Male bejahte der Gerichtshof eine gemeinsame Verantwortlichkeit mit Facebook.

Dazu war zunächst der Zweck der Datenverarbeitung zu ermitteln. Er besteht beim Betrieb einer Fanpage nicht allein in der (technischen) Realisierung der Fanpage, sondern auch in Werbung. Das betrifft zum einen die Werbung, welche die Plattform im Umfeld der Fanpage oder anderer Seiten anzeigt. Zum anderen dient die Fanpage ihrem Betreiber aber auch dazu, sich dort der Öffentlichkeit zu präsentieren und „in den Medien- und Meinungsmarkt einzubringen."[1602] Dabei wird er von Facebook mit anonymisierten statistischen Auswertungen zu den Besuchern seiner Fanpage unterstützt. 1436

Der Zweck eines sog. Social-Plugins wie dem Like-Button besteht darin, die Sichtbarkeit des eigenen Web-Angebots auf dem sozialen Netzwerk zu erhöhen.[1603] Die Schaltfläche wird auf jeder Webseite angezeigt und der Besucher der Webseite kann durch einen Klick darauf seinem bei dem sozialen Netzwerk registrierten Umfeld kundtun, dass ihm diese Webseite gefalle. 1437

In beiden Fällen verläuft die Verarbeitung der Daten recht ähnlich, nämlich immer dann, wenn der Browser des Nutzers Web-Elemente vom Server des Betreibers des sozialen Netzwerks lädt. Bei der Fanpage ist dies weniger überraschend, schließlich wird auch die Fanpage selbst von den Servern von Facebook geladen.[1604] Aber auch die Schaltfläche des Like-Buttons wird in die aufnehmende Seite nur eingebunden. Wenn der Browser des Nutzers die Webseite aufruft, geschieht dies stückweise. Zunächst liest das Programm den „Bausatz" der Webseite aus, und fügt die einzelnen Elemente sodann entsprechend zusammen. Zu diesen Elementen gehören in 1438

1600 EuGH, ECLI:EU:C:2018:388, Rn. 39 f. – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*.

1601 EuGH, ECLI:EU:C:2019:629, Rn. 64 ff. – *Fashion ID*.

1602 EuGH, ECLI:EU:C:2018:388, Rn. 15 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*.

1603 EuGH, ECLI:EU:C:2019:629, Rn. 80 – *Fashion ID*.

1604 In der technischen Realisierung ergeben sich noch Unterschiede. So wird der eigentliche Seiteninhalt oft über ein sog. Content Delivery Network (CDN) geladen. Das Tracking findet hingegen auf den Servern von Facebook statt (siehe *ULD* 2011, S. 3 f.). Für die Frage der gemeinsamen Verantwortlichkeit mit Facebook ist allein letzteres relevant. Der CDN-Betreiber ist hier nur Auftragsverarbeiter von Facebook (siehe *ULD* 2011, S. 15 f.) und steht in keiner Verbindung zu dem Fanpage- oder Website-Betreiber.

der Regel auch solche auf anderen Servern als denen des Website-Betreibers. Im Fall des Like-Buttons sind dies die Server von Facebook.[1605]

1439 Für die Mittel der Verarbeitung stellt der Europäische Gerichtshof auf verschiedene Methoden ab, die aber tatsächlich in einem engen Zusammenhang zueinanderstehen. Im Fall der Like-Buttons genügt dem Gerichtshof bereits, dass – gewissermaßen erst auf die Initiative des die Schaltfläche einbindenden Website-Betreibers hin – die IP-Adresse[1606] des Besuchers an Facebook übermittelt wird.[1607]

1440 Bei den Fanpages verhält es sich etwas komplizierter, da hier jedem, der die Fanpage aufruft, klar sein muss, dass bereits technisch bedingt Daten wie die IP-Adresse an Facebook übermittelt werden. Der Gerichtshof stellt hier auf den Einsatz von Cookies ab, die beim Besuch der Fanpage auf dem Gerät der Nutzer gespeichert werden. Diese Cookies enthalten einen eindeutigen Benutzercode, der mit den Anmeldedaten registrierter Facebook-Nutzer verknüpft werden kann. Dieser Benutzercode wird beim Aufruf der Fanpage erhoben und verarbeitet.[1608] Dadurch kann Facebook auch bei wechselnden IP-Adressen erkennen, wer die Fanpage besucht und daraus die angebotenen Statistiken erstellen. Tatsächlich werden diese Tracking-Cookies auch beim Aufruf eines Social-Plugins wie dem Like-Button gesetzt, sodass Facebook den Benutzer auf allen entsprechend präparierten Webseiten wiedererkennen und so sein Verhalten im Web nachverfolgen kann.[1609] Die Erkenntnisse hieraus dürften ebenfalls in die Erstellung der Fanpage-Statistiken und die Vermittlung von Werbeanzeigen einfließen.

1441 Der Europäische Gerichtshof stellt für die Mitwirkung an der Festlegung von Zweck und Mittel der Datenverarbeitung auf verschiedene Aspekte ab. Beim Like-Button begnügt er sich mit der Feststellung, dass die Datenerhebung und -übermittlung ohne die Mitwirkung des die Schaltfläche einbindenden Website-Betreibers schlicht nicht möglich gewesen wäre,[1610]

1605 EuGH, ECLI:EU:C:2019:629, Rn. 26 – *Fashion ID*; Grundlegend *ULD* 2011, S. 3 f.
1606 EuGH, ECLI:EU:C:2019:629, Rn. 26 – *Fashion ID*.
1607 EuGH, ECLI:EU:C:2019:629, Rn. 75 – *Fashion ID*.
1608 EuGH, ECLI:EU:C:2018:388, Rn. 15 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*.
1609 Zur genauen technischen Analyse der Datenverarbeitung *ULD* 2011.
1610 EuGH, ECLI:EU:C:2019:629, Rn. 75 ff. – *Fashion ID*.

dies zumal die Datenverarbeitung unabhängig davon erfolgt, ob der Besucher der Webseite bei Facebook registriert ist.[1611]

Die Argumentation zu den Fanpages ist wiederum etwas komplexer. Ihnen liegt die Annahme zugrunde, dass eine Plattform wie Facebook nicht ihrer selbst wegen besucht wird, sondern wegen des von Dritten dort dargebotenen Inhalts. Wer eine Fanpage auf Facebook betreibe, gebe Facebook also die Möglichkeit, Daten über die Besucher der Fanpage zu verarbeiten und für sein System der Werbung zu verwenden. Allein der Umstand, dass man Nutzer auf die Plattform lockt, reicht dem Gericht jedoch nicht aus – sonst würde schließlich jeder Nutzer von Facebook zu einem gemeinsamen Verantwortlichen.[1612] 1442

Entscheidend für die gemeinsame Verantwortlichkeit ist folglich nicht, dass Facebook die Daten für (eigene) Werbung verwendet. Diesbezüglich legt Facebook selbst Zweck und Mittel fest. Für das Gericht ist vielmehr maßgeblich, dass und wie die Daten dazu verwendet werden, die statistischen Auswertungen zu erstellen, mit deren Hilfe der Fanpage-Betreiber für sich selbst Werbung machen kann. Dies ist – gleichwohl es das Gericht nicht in dieser Deutlichkeit sagt – der Zweck, den Plattformbetreiber und Fanpage-Betreiber gemeinsam festlegen. Der Beitrag des Fanpage-Betreibers bei der Festlegung der Mittel besteht darin, die Kriterien festzulegen, nach denen die Statistiken erstellt werden und Kategorien von Personen zu bezeichnen, deren Daten dabei berücksichtigt werden sollen.[1613] Es sind diese Vorgaben für die Datenverarbeitung, die ausreichen. An der eigentlichen Datenverarbeitung muss der Fanpage-Betreiber – ebenso wenig wie derjenige, der ein Social-Plugin einbindet[1614] – nicht beteiligt sein.[1615] 1443

1611 EuGH, ECLI:EU:C:2019:629, Rn. 83 – *Fashion ID*.
1612 EuGH, ECLI:EU:C:2018:388, Rn. 35 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*.
1613 EuGH, ECLI:EU:C:2018:388, Rn. 36 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*.
1614 EuGH, ECLI:EU:C:2019:629, Rn. 82 – *Fashion ID*.
1615 EuGH, ECLI:EU:C:2018:388, Rn. 38 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*.

3.6.2.4.1.1.2 Die Entscheidung des EuGH zur Verkündigungstätigkeit der Zeugen Jehovas

1444 In der zweiten Entscheidung des Europäischen Gerichtshofs ging es um die Datenverarbeitung im Rahmen der Verkündigungstätigkeit der Mitglieder der Gemeinschaft der Zeugen Jehovas.[1616] Die Mitglieder fertigten bei ihren Hausbesuchen Notizen über Namen, Adresse, religiöse Überzeugung und Familienverhältnisse der Besuchten an. Die Mitglieder taten dies zwar selbständig und ohne, dass es von ihnen verlangt wurde. Die Gemeinschaft erfuhr auch nichts vom Inhalt dieser Notizen. Sie hatte aber Anleitungen herausgegeben, wie solche Notizen zu fertigen waren. Außerdem koordinierte sie die Verkündungstätigkeit der einzelnen Mitglieder.

1445 Das Gericht sah die einzelnen Mitglieder und die Gemeinschaft der Zeugen Jehovas als gemeinsame Verantwortliche an.[1617] Dabei legte es nicht dar, welche Beteiligung der Gemeinschaft der Festlegung des Zwecks und welche der Festlegung des Mittels zuzuordnen sind. Für ersteres scheint aber maßgeblich zu sein, dass die Verkündung die wesentliche Betätigungsform der Gemeinschaft und ihrer Mitglieder ist. Sie ist gewissermaßen bereits der Zweck der Gemeinschaft selbst. Für zweiteres, die Festlegung des Mittels, bleiben damit die übrigen im Urteil angeführten Gründe. Danach war es entscheidend, dass die Gemeinschaft die Verkündungstätigkeit koordinierte, und ihr die hierzu durchgeführte Datenverarbeitung durch die Mitglieder bekannt war. Daraus lasse sich schließen, dass die Gemeinschaft ihre Mitglieder zur Verarbeitung personenbezogener Daten ermuntere.

3.6.2.4.1.1.3 Folgen für die Voraussetzungen der gemeinsamen Verantwortlichkeit

1446 Aus diesen Urteilen lassen sich unterschiedlich strenge Anforderungen für die jeweilige Festlegung entnehmen. Der Zweck ist schnell und leicht gemeinsam gesetzt. Hier genügt schon ein teilweise gleichlaufendes Interesse der Beteiligten.[1618] So geht es Facebook mit dem Betrieb der Fanpage gewissermaßen nur als Zwischenziel darum, dass der Fanpage-Betreiber möglichst gut für sich Werbung machen kann. Das eigentliche Ziel des Platt-

1616 EuGH, ECLI:EU:C:2018:551 – *Jehovan todistajat*.
1617 EuGH, ECLI:EU:C:2018:551, S. 73 – *Jehovan todistajat*.
1618 So wohl auch BeckOK DSR/*Spoerr*, Art. 26 DS-GVO, Rn. 16.

formbetreibers ist es, für Fanpage-Betreiber und letztlich auch für Nutzer attraktiv zu sein und so selbst besser Werbung vermitteln zu können. Der Fanpage-Betreiber wiederum und ebenso derjenige, der Social-Plugins in seiner Website einbindet[1619] nimmt dieses Eigeninteresse von Facebook in Kauf, wenn ihm dies hilft, der auf der Fanpage beworbene Tätigkeit erfolgreicher nachzugehen.

Ein solcher teilweiser Gleichlauf von Interessen wohnt jeder Zusammenarbeit inne und ist nicht zuletzt die Grundlage vieler Datenübermittlungen. Abgesehen vom schlichten Verkauf der Daten oder einer Übermittlungspflicht, bei welcher der übermittelnde Teil bezogen auf die Daten tatsächlich nur ein Fremdinteresse fördert, geht es bei der Übermittlung nämlich oft darum, dass der empfangende Teil die Daten für etwas verwendet, was wiederum für den übermittelnde Teil von Interesse ist. Die Aufteilung der Datenverarbeitung in einzelne Schritte ist damit kein exklusives Merkmal der gemeinsamen Verantwortlichkeit.[1620] 1447

So handelt ein Reisebüro, dass personenbezogene Daten über die Reservierungswünsche seiner Pauschalreisekunden an eine Fluggesellschaft weiterleitet zu dem Zweck, dass diese Reservierungen vorgenommen werden. Die Fluggesellschaft verarbeitet die Daten ebenfalls zu diesem Zweck. Dass sich die übergeordneten Zwecke – Erfüllung des Reise- bzw. des Beförderungsvertrags – unterscheiden, spielt für diesen punktuellen Gleichlauf keine Rolle. An dieser Gemeinsamkeit des Zwecks ändert sich schließlich auch nichts, wenn das Reisebüro und die Fluggesellschaft zur besseren Steuerung des gesamten Prozesses eine gemeinsame EDV-Plattform betreiben.[1621] Jeder handelt weiterhin zu punktuell übereinstimmenden, im Grunde aber verschiedenen Zwecken. 1448

Die gemeinsame Zwecksetzung darf nicht vernachlässigt werden, sie ist aber nur eine Art Mindestvoraussetzung.[1622] Das Hauptaugenmerk muss in der Festlegung der Mittel liegen. Der Europäische Gerichtshof hatte hier Fälle vorliegen, in denen ein Beteiligter im Grunde überhaupt keine Datenverarbeitung durchführte. Dies sind Konstellationen, die üblicherweise dadurch bewältigt werden, dass der tatsächlich handelnde Beteiligte ent- 1449

1619 EuGH, ECLI:EU:C:2019:629, Rn. 80 – *Fashion ID*.
1620 *Kremer,* CR 2019, S. 225, 228.
1621 Zu beiden Beispielen *Art. 29-Grp.,* WP 169, S. 24.
1622 A.A. *Art. 29-Grp.,* WP 169, S. 23, die ausreichen lassen, wenn Zweck oder Mittel zusammen festgelegt werden. Wie der eindeutige Wortlaut („und"), der sich auch bereits in der Datenschutzrichtlinie findet, überspielt werden soll, wird indessen nicht klar.

weder in die Organisation des Verantwortlichen eingegliedert wird (so die „Vertriebsmitarbeiter" der Gemeinschaft der Zeugen Jehovas) oder eine Auftragsdatenverarbeitung durchgeführt wird. So hatte die Aufsichtsbehörde im Fanpage-Fall im nationalen Revisionsverfahren auch vorgetragen, dass der Fanpage-Betreiber mit Facebook einen ungeeigneten, weil Datenschutzrecht missachtenden Anbieter „mit der Erstellung, Bereithaltung und Wartung eines Internetauftritts" beauftragt habe.[1623] Auch die zweite Vorlagefrage des Bundesverwaltungsgerichts stellte auf das Verhältnis der gemeinsamen Verantwortlichkeit zur Auftragsdatenverarbeitung ab.[1624]

1450 Die gemeinsame Verantwortlichkeit scheint in diesem Kontext vor allem ein Instrument zu sein, mit dem die Umgehung der Auftragsdatenverarbeitung verhindert und so Schlupflöcher im Konzept der Verantwortlichkeit geschlossen werden sollen.[1625] Es ist notwendig, weil der „Auftraggeber" – also der Betreiber der Fanpage, der einbindenden Website oder die Religionsgemeinschaft – ohne den „Auftragnehmer" nie in Kontakt mit den Daten käme. Folglich könnte man eine Zusammenarbeit der beiden Beteiligten nicht dadurch unterbinden, dass man die Übermittlung der personenbezogenen Daten verbietet. Dieser Weg kann z.B. bei einer Auftragsdatenverarbeitung beschritten werden, die infolge des fehlenden Weisungsrechts des Auftraggebers nach Art. 28 Abs. 3 S. 2 lit. a DS-GVO unzulässig ist.[1626] Dies war in den vom Europäischen Gerichtshof entschiedenen Fällen jedoch nicht möglich, weil der „Auftraggeber" zu keinem Zeitpunkt Handlungen ausführte, die man für sich betrachtet als Datenverarbeitung nach Art. 4 Nr. 2 DS-GVO qualifizieren konnte.

3.6.2.4.1.1.4 Abgrenzung der gemeinsamen Verantwortlichkeit zur Übermittlung

1451 Besonders in Abgrenzung zu jenen Konstellationen, in denen eine Übermittlung zwischen selbständigen Verantwortlichen zulässig wäre, dürfen

---

1623 EuGH, ECLI:EU:C:2018:388, Rn. 22 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*.

1624 EuGH, ECLI:EU:C:2018:388, Rn. 24 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*.

1625 So allgemein ohne Bezug zur Umgehung der Auftragsdatenverarbeitung *Art. 29-Grp.*, WP 169, S. 27.

1626 Zur Privilegierungswirkung der Auftragsdatenverarbeitung auf die Übermittlung BeckOK DSR/*Spoerr*, Art. 28 DS-GVO, Rn. 31.

an die gemeinsame Verantwortlichkeit keine allzu niedrigen Anforderungen gestellt werden. Da sich hinsichtlich der gemeinsamen Zweckfestsetzung kaum Unterschiede zwischen den beiden Konstellationen ergeben, sind bei der gemeinsamen Verantwortlichkeit umso höhere Anforderungen an die Festlegung der Mittel zu stellen. Es genügt demnach nicht, wenn sich die Beteiligten darauf einigen, welche Daten auf welchem Weg übermittelt werden. Der Beitrag des übermittelnden Teils muss sich vielmehr auch auf die spätere Verarbeitung beziehen.

Zwar ist es das Wesen der gemeinsamen Verantwortlichkeit, dass der andere Beteiligte (hier der Empfänger) die Verarbeitung aus – wenn auch abgestimmtem – Eigeninteresse und vor allem im Gegensatz zu einem Auftragsdatenverarbeiter weisungsfrei vornimmt.[1627] Der nicht unmittelbar an der Datenverarbeitung beteiligte (hier der Übermittler) muss aber gewisse Vorgaben zur Art und Weise der Datenverarbeitung gemacht haben, die der andere tatsächlich[1628] berücksichtigt.[1629] Die im Rahmen der gemeinsamen Verantwortlichkeit erfolgende Zurechnung der Datenverarbeitung zu dem nicht unmittelbar beteiligten Verantwortlichen (dazu näher sogleich unter 3.6.2.4.1.2.1, S. 552), ist nur gerechtfertigt, wenn sie nicht nur ihrem Zweck nach, sondern auch in ihrer konkreten Gestalt von den wenigstens stillschweigend[1630] erklärten Vorstellungen dieses Beteiligten mitbestimmt ist.[1631] 1452

3.6.2.4.1.2 Rechtsfolgen der gemeinsamen Verarbeitung

Gemäß Art. 26 Abs. 1 S. 2 und Abs. 2 DS-GVO müssen die gemeinsamen Verantwortlichen ihre Aufgabenverteilung – insbesondere im Hinblick auf die Informationspflichten – klären, dokumentieren und die Dokumentation der betroffenen Person zur Verfügung stellen. Der Verantwortliche kann gemäß § 26 Abs. 3 DS-GVO seine Betroffenenrechte bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen. 1453

1627 Zu dieser Abgrenzung auch *Martini*, in: Paal/Pauly 2018, Art. 26 DS-GVO, Rn. 3.
1628 So auch *Martini*, in: Paal/Pauly 2018, Art. 26 DS-GVO, Rn. 19 f.
1629 So wohl auch *Marosi/Matthé*, ZD 2018, S. 361, 362.
1630 EuGH, ECLI:EU:C:2019:629, Rn. 80 – *Fashion ID*.
1631 *Kartheuser/Nabulsi*, MMR 2018, S. 717, 720; *Schreiber*, ZD 2019, S. 55 f.; BeckOK DSR/*Spoerr*, Art. 26 DS-GVO, Rn. 13f.

1454 Darüber hinaus enthält nur Art. 82 Abs. 4 DS-GVO noch eine Regelung zum Handeln mehrerer Verantwortlicher. Verursacht eine Datenverarbeitung, an der mehrere Verantwortliche beteiligt sind, einen Schaden, so haftet gemäß Art. 82 Abs. 4 DS-GVO jeder Verantwortliche, der seine Nichtverantwortlichkeit für den schadensverursachenden Umstand nicht nach Art. 82 Abs. 3 DS-GVO nachweisen kann, für den gesamten Schaden. Obwohl hier nicht direkt auf die gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 S. 1 DS-GVO abgestellt wird, ist davon auszugehen, dass diese Fälle zumindest auch von Art. 82 Abs. 4 DS-GVO abgedeckt werden.

3.6.2.4.1.2.1 Der Grad der gemeinsamen Verantwortlichkeit

1455 Zu weitergehenden Rechtsfolgen der gemeinsamen Verantwortlichkeit äußert sich die Datenschutz-Grundverordnung nicht. Unklar ist insbesondere, was dem nur mittelbar beteiligten Verantwortlichen zugerechnet werden kann. Der Europäische Gerichtshof hat in den von ihm entschiedenen Fällen betont, dass es durchaus verschiedene Grade der Verantwortlichkeit geben kann,[1632] und diesbezüglich auf die verschiedenen Verarbeitungsvorgänge abgestellt. Die gemeinsame Verantwortlichkeit führe nicht dazu, dass einem Beteiligten alle vor- oder nachgelagerten Vorgänge in der Verarbeitungskette zugerechnet würden, sondern nur jene, für die er als Verantwortlicher anzusehen sei.[1633]

1456 Es genügt folglich nicht jeder irgendwie geartete Zusammenhang zwischen der Datenverarbeitung und der Zusammenarbeit der Beteiligten. Die gemeinsame Verantwortung bezieht sich immer nur auf diejenige Verarbeitung, zu der ein relevanter Beitrag geleistet wird. Die *Art. 29-Gruppe*[1634] nennt hierfür das Beispiel einer einheitlichen Plattform, über die mehrere Behörden mit dem Bürger kommunizieren. Die Plattform übernehme lediglich die Datenerhebung und -übermittlung; die Speicherung und weitere Verarbeitung der Daten fänden bei den Behörden statt. In diesem Fall müssten die Beteiligten lediglich gewährleisten, dass die über die Plattform abgewickelte Übermittlung der Daten sicher sei. Von einer Ver-

1632 EuGH, ECLI:EU:C:2018:388, Rn. 43 – *ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein*; EuGH, ECLI:EU:C:2018:551, Rn. 66 – *Jehovan todistajat.* So auch schon zuvor *Art. 29-Grp.*, WP 169, S. 23.

1633 EuGH, ECLI:EU:C:2019:629, Rn. 74 – *Fashion ID*.

1634 *Art. 29-Grp.*, WP 169, S. 26.

antwortlichkeit für die daran anschließende dezentrale Datenverarbeitung ist hingegen keine Rede.

Gewendet auf den Fanpage-Fall muss sich der Betreiber nicht sämtliche (rechtswidrige) Datenverarbeitung des Plattformbetreibers im Zusammenhang mit den Besuchen der Fanpage zurechnen lassen. Welche Daten Facebook über den beim Besuch der Seite gesetzten Cookie noch erhebt, spielt für den Fanpage-Betreiber keine Rolle. Auch welche Daten bei dem Seitenaufruf selbst erhoben werden, ist zweitrangig. Entscheidend sind nur jene Daten, zu deren Verarbeitung der Fanpage-Betreiber mit der Parametrierung der Statistik einen relevanten Beitrag geleistet hat. Im Fall der von dem Website-Betreiber initiierten Datenverarbeitung durch das Social-Plugin ist dieser nur für die Erhebung und Übermittlung gemeinsam verantwortlich, nicht aber für die anschließenden Verarbeitungsvorgänge beim Betreiber des sozialen Netzwerks.[1635] Für die Gemeinschaft der Zeugen Jehovas gilt nach diesem Maßstab, dass sie sich nicht sämtliche Notizen ihrer Mitglieder zurechnen lassen muss, sondern nur solche, die in Übereinstimmung mit ihrer Anleitung erstellt wurden. 1457

3.6.2.4.1.2.2 Die Folgen für Betroffenenrechte und die Rechtmäßigkeit der Verarbeitung

Bezieht man die Zurechnung lediglich auf jene Verarbeitung, zu der ein relevanter Beitrag geleistet wurde, hat dies auch Folgen für die Regelung zur Ausübung der Betroffenenrechte in Art. 26 Abs. 3 DS-GVO. Der nicht selbst verarbeitende gemeinsame Verantwortliche ist nicht etwa nur der Empfangsbote des anderen gemeinsamen Verantwortlichen, sondern gesamtschuldnerischer Verpflichteter dieser Betroffenenrechte.[1636] 1458

Die gemeinsame Datenverarbeitung – und nur diese – wird den Beteiligten zugerechnet. Insofern ergibt sich ein gewisser Gleichlauf mit der Auftragsdatenverarbeitung[1637]. Dies geht in beide Richtungen: Zum einen kann jeder gemeinsame Verantwortliche für alles in Verantwortung und Haftung 1459

1635 EuGH, ECLI:EU:C:2019:629, Rn. 74 – *Fashion ID*.

1636 *Martini*, in: Paal/Pauly 2018, Art. 26 DS-GVO, Rn. 36; *Petri*, in: Simitis et al. 2019, Art. 26 DS-GVO, Rn. 29.

1637 Zur Zurechnung der Datenverarbeitung im Rahmen der Auftragsdatenverarbeitung *Martini*, Art. 28 DS-GVO, Rn. 2; *Petri*, in: Simitis et al. 2019, Art. 28 DS-GVO, Rn. 29 ff.; *Thomale*, in: Auernhammer 2020, Art. 28 DS-GVO, Rn. 6 ff., jeweils m.w.N.; a.A. z.B. *Roßnagel/Kroschwald*, ZD 2014, S. 495, 497.

genommen werden, für das er einen relevanten Beitrag geleistet hat. Was dies ist, muss sich aus der Dokumentation nach Art. 26 Abs. 1 S. 2, Abs. 2 S. 1 DS-GVO ergeben. Zum anderen besteht wie im Falle der Auftragsdatenverarbeitung zwischen den gemeinsamen Verantwortlichen im Rahmen dieser Verantwortlichkeit ein Verarbeitungsprivileg.[1638]

3.6.2.4.1.2.3 Wirkweise der Privilegierung

1460 Wie dieses Verarbeitungsprivileg genau wirkt, ist bisher kaum diskutiert worden. Die Autoren, die es ansprechen, beziehen sich für die Privilegierung bewusst auf die Auftragsdatenverarbeitung[1639] oder grenzen sich gerade von der dortigen Privilegierung ab.[1640] Darum muss zunächst die Wirkweise des Verarbeitungsprivilegs bei der Auftragsdatenverarbeitung näher beleuchtet werden.

1461 Die gängige Diskussion,[1641] orientiert sich stark an der alten Rechtslage nach § 11 BDSG 2003 und fragt danach, ob der Auftragsdatenverarbeiter im Verhältnis zum Verantwortlichen ein Dritter sei. Wäre dies nämlich der Fall, stellte die Weitergabe der Daten untereinander eine Übermittlung dar, für die es zusätzlich zu den Anforderungen an die interne Verarbeitung der Daten eines eigenständigen Erlaubnistatbestands bedürfe. Nach § 3 Abs. 8 S. 3 BDSG 2003 war der Auftragsdatenverarbeiter aber kein Dritter, die Weitergabe keine Übermittlung nach § 3 Abs. 4 S. 2 Nr. 3 BDSG 2003 und folglich der internen Verarbeitung gleichgestellt.

1638 *Kremer,* CR 2019, S. 225, 231; *Martini,* in: Paal/Pauly 2018, Art. 26 DS-GVO, Rn. 3a; *Piltz,* in: Gola 2018, Art. 24 DS-GVO, Rn. 8.

1639 Für einen Gleichlauf zur Auftragsdatenverarbeitung *Kremer,* CR 2019, S. 225, 231; *Martini,* in: Paal/Pauly 2018, Art. 26 DS-GVO, Rn. 3a.

1640 Gegen einen Erlaubnistatbestand und mit dem Hinweis, dass sich der mit der gemeinsamen Verantwortlichkeit verbundene Anstieg der Komplexität sogar risikoerhöhend auswirken könnte *Thomale,* in: Auernhammer 2020, Art. 28 DS-GVO, Rn. 6. In der sechsten Auflage hatte sich *Thomale* zwar auch gegen einen Erlaubnistatbestand aber zumindest für eine Erleichterung ausgesprochen *Thomale,* in: Auernhammer 2018, Art. 26 DS-GVO, Rn. 5.

1641 Gegen die Einordnung als Dritter und ebenso gegen das Erfordernis einer gesonderten Rechtsgrundlage *Martini*, Art. 28 DS-GVO, Rn. 10; *Petri,* in: Simitis et al. 2019, Art. 28 DS-GVO, Rn. 29 ff.; *Thomale,* in: Auernhammer 2020, Art. 28 DS-GVO, Rn. 6 ff., jeweils m.w.N.; a.A. z.B. *Roßnagel/Kroschwald,* ZD 2014, S. 495, 497.

Die Grundannahme dieser Diskussion ist falsch oder zumindest ungenau formuliert. Die Einordnung des Auftragsdatenverarbeiters – bzw. des gemeinsamen Verantwortlichen – als Dritten und die Frage, ob es für die Weitergabe der Daten einer zusätzlichen Erlaubnisgrundlage bedarf, ist unabhängig voneinander zu beantworten. Zumindest die Erlaubnistatbestände für die Datenverarbeitung durch Private unterschieden und unterscheiden nicht zwischen der internen und der externen Datenverarbeitung. So wurden z.B. in § 28 Abs. 1 S. 1 und Abs. 2 BDSG 2003 das „Erheben, Speichern, Verändern oder Übermitteln" bzw. die „Übermittlung oder Nutzung" in einer Reihe und ohne eine Differenzierung hinsichtlich der Rechtsfolgen genannt. In Art. 6 Abs. 1 UAbs. 1 lit. b und f DS-GVO ist gleich nur von Verarbeitung die Rede, zumal in der Begriffsdefinition von Verarbeitung in Art. 4 Nr. 2 DS-GVO auch nicht zwischen den einzelnen Arten der Verarbeitung differenziert wird. 1462

Es gab und gibt darum keinen Grundsatz, demzufolge ein Erlaubnistatbestand immer nur bis zur (Unternehmens-)Grenze des Verantwortlichen reicht und es für jede Überschreitung dieser Grenze eines weiteren Erlaubnistatbestands bedarf. Vielmehr muss zwischen Erlaubnistatbestand und Verarbeitungsgrundlage unterschieden werden. Jede Verarbeitungshandlung muss einen Erlaubnistatbestand nach Art. 6 Abs. 1 UAbs. 1 DS-GVO erfüllen. Dieser Erlaubnistatbestand benennt eine Verarbeitungsgrundlage. Im Fall des Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO ist diese Grundlage der durchzuführende Vertrag, in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO ist es das berechtigte Interesse. Es muss also für jeden Verarbeitungsschritt einzeln geprüft werden, ob er zur Erfüllung des Vertrags bzw. zur Wahrung des berechtigten Interesses erforderlich ist. 1463

Es gibt keinen Automatismus, dergestalt, dass eine Datenerhebung, die einen Erlaubnistatbestand erfüllt, eine interne Weiterverarbeitung nach sich zieht, die ebenfalls diesen Anforderungen genügt. Der Erlaubnistatbestand ist für jede Verarbeitungshandlung stets erneut zu prüfen. Es ist nur so, dass die Verarbeitungsgrundlage oft beides abdeckt – den Erlaubnistatbestand der Erhebung und denjenigen der anschließenden Verarbeitung. Ist die Erhebung für die Zweckerreichung erforderlich, liegt es nahe, dass dies auch für einen weiteren Verarbeitungsschritt gilt. Welcher dies ist, richtet sich nach dem Erforderlichkeitsprinzip. 1464

Ist der Zweck wie im Fall des Reiseveranstalters, der Reservierungsdaten an den Fluganbieter übermittelt, von vornherein auf die Einschaltung Dritter angelegt, muss die Erforderlichkeit der Übermittlung nicht weiter erörtert werden. Die Übermittlung an diesen Dritten ist hier das einzige geeignete Mittel zur Vertragserfüllung. 1465

1466 Könnte der nächste Verarbeitungsschritt aber auch intern vorgenommen werden, stellt sich die Frage, ob diese interne Verarbeitung ein milderes, gleich wirksames Mittel im Vergleich zur Übermittlung an einen Dritten darstellt. Dies wird man normalerweise bejahen müssen, weil die interne Datenverarbeitung weniger in die Grundrechte der betroffenen Person eingreift als die Übermittlung zu einem Dritten, den der Verantwortliche nicht kontrolliert und mit dem die betroffene Person auch keine rechtlich relevante Beziehung eingegangen ist. Die interne Datenverarbeitung ist also zumindest ein milderes Mittel. Ist es auch im Wesentlichen zur Zweckerreichung gleich geeignet, geht die interne der externen Datenverarbeitung vor.

1467 Die Auftragsdatenverarbeitung – und auch die gemeinsame Verantwortlichkeit – setzen bei der Beurteilung des milderen Mittels an. Durch die Weisungsgebundenheit des Auftragsdatenverarbeiters nach Art. 28 Abs. 3 S. 2 lit. a DS-GVO bzw. die Vereinbarung mit dem anderen gemeinsamen Verantwortlichen nach Art. 26 Abs. 1 S. 2 DS-GVO besteht nämlich keine Vermutung mehr, dass die externe Datenverarbeitung mit einem tieferen Eingriff in die Grundrechte der betroffenen Person verbunden ist. Die interne Datenverarbeitung ist damit kein milderes Mittel mehr und folglich im Rahmen der Erforderlichkeitsprüfung auch nicht mehr der externen Verarbeitung vorzuziehen. Der Verantwortliche kann sich zwischen den beiden gleich milden Mitteln entscheiden.

1468 Die Einordnung des Datenempfängers als Dritten spielt für die Verarbeitungsprivilegierung im engeren Sinne, also mit Blick auf die Zulässigkeit, keine Rolle. Folglich kann die Privilegierung sowohl in der Auftragsdatenverarbeitung als auch der gemeinsamen Verantwortlichkeit gleich wirken.

3.6.2.4.1.3 Gemeinsame Verantwortlichkeit in Wertschöpfungsnetzwerken

1469 In einem Wertschöpfungsnetzwerk arbeiten Unternehmen sehr eng und auf einer automatisierten Basis miteinander zusammen. Ob daraus aber eine gemeinsame Verantwortlichkeit im Hinblick auf die ggf. auch ausgetauschten personenbezogenen Beschäftigtendaten folgt, ist zweifelhaft.

3.6.2.4.1.3.1 Die Funktionen und Rollen im Industrial Data Space

Der Industrial Data Space, der hier als Beispiel für ein Wertschöpfungsnetzwerk herangezogen werden soll, versteht sich in erster Linie als Referenzarchitekturmodell u.a. für den Austausch von Daten und die Kontrolle der Nutzung dieser Daten. Dafür werden verschiedene Rollen definiert.[1642] Diese sind u.a. 1470

- Der Datengeber: Er registriert seine Datenquellen und gibt an, welche Daten abgerufen und unter welchen Bedingungen sie genutzt werden können.
- Der Datennutzer: Er ruf die Daten ab, die über das Referenzmodell schematisiert worden sind und überführt sie in sein Zielmodell.
- Der Datenbroker: Er ermöglicht, überwacht und protokolliert den Datenaustausch. Dazu betreibt er einen Verzeichnisdienst und stellt Datengeber und Datennutzer Funktionen bereit, mit denen diese Vereinbarungen über die Datennutzung treffen können.
- Die Zertifizierungsstelle: Sie stellt sicher, dass die Software die definierten Anforderungen erfüllt und die Normen und Standards eingehalten werden.

Entsprechend dieser Rollenbeschreibung steht der automatisierte, standardisierte und sichere Datenaustausch beim Industrial Data Space im Vordergrund. Die am Netzwerk angeschlossenen Unternehmen teilen sich keine gemeinsame Datenhaltung. Die Plattform fungiert vielmehr nur als Mittler zwischen den einzelnen auf diese Weise föderierten Datenbanken.[1643] 1471

Darüber hinaus enthält die Sicherheitsarchitektur einen Nutzungskontrolle genannten Teil.[1644] So können dem Datennutzer etwa Mindeststandards in Bezug auf die Sicherheit und Datenverarbeitung[1645] vorgegeben oder Nutzungsbeschränkungen im Hinblick auf die Nutzungsdauer oder die Weitergabe der Daten auferlegt werden. Die Datengeber können aber auch nur bestimmte Abfragen zulassen oder nur Informationen auf einem be- 1472

1642 *Fraunhofer* 2016, S. 16 f.
1643 *Fraunhofer* 2016, S. 5.
1644 *Fraunhofer* 2016, S. 24.
1645 Worauf sich die Mindeststandards der Datenverarbeitung beziehen, wird in dem Konzept des Industrial Data Space nicht näher erläutert. Da das Wertschöpfungsnetzwerk aber vor allem Maschinendaten im Blick hat, ist nicht davon auszugehen, dass es sich hier um detaillierte datenschutzrechtliche Vorgaben handelt.

stimmten Aggregationslevel freigeben. Roh- und nicht benötigte Daten können so unzugänglich bleiben.

1473 Als ein Anwendungsbeispiel im Industrial Data Space wird u.a. die kooperative Bewirtschaftung von Produktionsanlagen genannt.[1646] Eine zustandsbasierte Wartung (siehe 1.1.2.2.2, S. 56) scheitere oft an der mangelnden Verfügbarkeit und Standardisierung der Daten, teils aber auch aus unternehmenspolitischen Gründen. Über den Industrial Data Space könnten Daten sicher mit Wartungsdienstleistern und Kunden ausgetauscht werden.

3.6.2.4.1.3.2 Die Struktur der Plattform als gemeinsam festgelegtes Mittel

1474 Wie das Beispiel des Industrial Data Space zeigt, geht es bei Wertschöpfungsnetzwerken oft vordergründig um den Datenaustausch. Die Datengeber können zwar definieren, welche Daten unter welchen Bedingungen übermittelt werden. Das ist aber das Wesen jeder Übermittlung und definiert nur das Ausgangsmaterial der Datenverarbeitung seitens des Empfängers. Wie der Datennutzer aber damit verfährt, nachdem er die Daten in sein Zielmodell überführt hat, wird durch die Struktur der Plattform nur in Ansätzen vorgegeben. Er muss gewisse Mindeststandards in Bezug auf die Sicherheit und Datenverarbeitung erfüllen. Grundsätzlich ist er aber frei, mit den Daten nach Belieben zu verfahren.

1475 Als maßgeblicher Beitrag für eine gemeinsame Verantwortlichkeit kommt zunächst die – tatsächlich wirkende – Nutzungskontrolle in Betracht. Sie ist der Plattform aber nicht immanent, sondern muss erst vom Datengeber entsprechend eingestellt werden. Und auch wenn er dies tut, ist fraglich, ob die einstellbaren Parameter zu einer gemeinsamen Verantwortlichkeit führen. Sie betreffen nämlich in weiten Teilen den Datenabruf von der Plattform; nur die Nutzungsdauer und die Weitergabe der Daten scheinen sich auf die Datenverarbeitung beim Datengeber zu beziehen. Und selbst diese Parameter geben nur einen sehr groben Rahmen vor, innerhalb dessen der Datennutzer alle relevanten Entscheidungen letztlich allein trifft. Inhaltliche Anforderungen, wie die Daten aufzubereiten sind, werden nicht gemacht.

1646 *Fraunhofer* 2016, S. 29.

3.6.2.4.1.3.3 Über die Plattform geschlossene Vereinbarungen

Als einziges Instrument, über das sich eine gemeinsame Verantwortlichkeit konstruieren lässt, bleiben darum die Vereinbarungen zwischen Datengeber und Datennutzer. Im Konzept des Industrial Data Space stellt der Databroker die hierfür notwendigen Funktionen bereit. Voraussetzung für eine gemeinsame Verantwortlichkeit ist aber, dass der Datengeber hierdurch erheblich mehr Einfluss auf die Verarbeitung seitens des Datennutzers nehmen kann als über die Definierung der Rahmenbedingungen. Ob eine gemeinsame Verantwortlichkeit entsteht, bestimmt sich dann nach der konkreten Vereinbarung. Dabei ist zwischen zwei Arten von Vereinbarungen zu unterscheiden: solche, die die Funktion des jeweiligen datengetriebenen Dienstes betreffen und solche, die auf den Schutz der ausgetauschten Daten abzielen. 1476

Bei der ersten Art von Vereinbarungen handelt es sich im Grunde um ähnliche Verarbeitungsbeiträge, wie sie den vom Europäischen Gerichtshof entschiedenen Fällen zugrunde lagen. Dass sie grundsätzlich eine gemeinsame Verantwortlichkeit begründen können, steht außer Frage. Bei Wertschöpfungsnetzwerken dürfte dies aber nur selten der Fall sein. Die Funktionalität der hierüber mit Daten „angetriebenen" Dienste ist nämlich nicht auf personenbezogene Daten gerichtet. Es ist darum eher unwahrscheinlich, dass auch die Verarbeitung personenbezogener Daten derart maßgeblich von funktionalen Anforderungen beeinflusst wird, dass man diese Vorgaben als relevanten Beitrag im Sinne der Festlegung eines gemeinsamen Mittels nach Art. 26 Abs. 1 S. 1 DS-GVO qualifizieren müsste. 1477

Die zweite Art von Verarbeitungen, solche zum Schutz der Daten, ist bisher nicht angesprochen worden. Sie kann sich in Wertschöpfungsnetzwerken sowohl auf den Schutz von Betriebs- und Geschäftsgeheimnissen als auch auf den Schutz von personenbezogenen Daten beziehen. Da auch sie die Art und Weise der Datenverarbeitung beeinflussen, können sie grundsätzlich als gemeinsame Festlegung der Mittel gewertet werden. Diese Art von Vereinbarungen haben das alleinige Ziel, die mit der Wirkung der Auftragsdatenverarbeitung vergleichbare Privilegierungswirkung (siehe 3.6.2.4.1.2.3, S. 554) der gemeinsamen Vereinbarung zu erzeugen. 1478

Für die Berücksichtigung reiner Schutzvereinbarungen spricht nicht zuletzt die Rolle, welche die gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 S. 1 DS-GVO im Gefüge der Datenschutz-Grundverordnung einnimmt. Sie kommt nämlich oft dann zum Tragen, wenn der Weg der Auftragsdatenverarbeitung nach Art. 28 DS-GVO in Ermangelung eines Weisungsverhältnisses nicht beschritten werden kann. Die gemeinsame Ver- 1479

antwortlichkeit ist aber nicht als bloßer Sanktionsmechanismus ausgestaltet, der „Auftraggebern" eine Datenverarbeitung zurechnet, die sie gar nicht oder jedenfalls nicht in der konkreten Art und Weise an einen „Auftragnehmer" hätten auslagern dürfen. Dies zeigen die Rechtsfolgen in Art. 26 Abs. 1 S. 2 und Abs. 2 DS-GVO. Die dort geforderten Vereinbarungen und deren Dokumentation ergeben nur Sinn, wenn eine gemeinsame Datenverarbeitung auch zulässig ausgestaltet werden kann.

3.6.2.4.2 Erlaubnistatbestand

1480 Unabhängig von der Einstufung als gemeinsame Verantwortliche benötigen die Verantwortlichen für die Datenübermittlung auf der einen und die Datenerhebung auf der anderen Seite einen Erlaubnistatbestand.

1481 Die Zulässigkeit der Datenverarbeitung in Wertschöpfungsnetzwerken und insbesondere die Übermittlung an andere Unternehmen kann nicht ohne Weiteres auf die Durchführung des Beschäftigungsverhältnisses gestützt werden. Der Datenaustausch wirkt sich über die Veränderung von Produktions- und Logistikabläufen zwar auf die Arbeit der Beschäftigten aus. Da die Daten aber in erster Linie zur Produktionssteuerung ausgetauscht werden und nicht speziell dazu, den Beschäftigten Weisungen zu erteilen oder arbeitsrechtliche Maßnahme zu ergreifen, ist diese Wirkung allenfalls mittelbarer Natur (siehe 3.6.1.3.1, S. 512). Sie dient darum weder der Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO noch ist sie dafür erforderlich.

1482 Die Übermittlung personenbezogener Daten in Wertschöpfungsnetzwerken kann darum nur nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zulässig sein.[1647] Danach braucht es zunächst ein legitimes, d.h. von der Rechtsordnung anerkanntes Interesse (siehe 3.6.1.3.2, S. 513). Die Übermittlung von Daten zur Abstimmung von Produktion und Logistik stellt ein solches berechtigtes Interesse im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO dar. Die am Wertschöpfungsnetzwerk beteiligten Unternehmen können sich diesbezüglich auf ihre unternehmerische Freiheit nach Art. 16 GRC berufen.

1647 *Wedde,* in: Däubler et al. 2020, § 26 BDSG, Rn. 189.

3.6.2.4.3 Die Erforderlichkeit i.e.S.

Beim Austausch von Daten in Wertschöpfungsnetzwerken wird es selten auf den Personenbezug der Daten ankommen. Die funktionalen Anforderungen werden regelmäßig auch erfüllt, wenn lediglich anonymisierte oder extern pseudonymisierte Daten übersendet würden.[1648] Eine Verarbeitung personenbezogener Daten im Sinne von Art. 4 Nr. 1 DS-GVO wird in den meisten Fällen darum nicht erforderlich und folglich auch nicht zulässig sein. 1483

Die Hürden für den Arbeitgeber sind dennoch vergleichsweise niedrig. Da der Personenbezug übermittelter Daten nämlich aus der Sicht des Empfängers bestimmt wird, kommt es darauf an, ob das empfangende Unternehmen das verwendete Pseudonym auflösen kann. Selbständigen Unternehmen, bei denen insbesondere das eine Unternehmen nicht das andere beherrscht, fehlen in der Regel die rechtlichen Mittel, sich die fehlenden Merkmale nach Art. 4 Nr. 1 DS-GVO vom anderen zu verschaffen. Für eine sog. externe Pseudonymisierung, die nicht unter die Verordnung fällt (siehe 3.3.4.5.2, S. 343) genügt es schon, die Daten einem nur intern verwendeten Pseudonym zuzuordnen, wenn die Zuordnungsregel entsprechend gegen äußeren Zugriff abgesichert wird. 1484

An dieser Trennung der Verantwortlichen ändert sich auch durch eine Vereinbarung zur gemeinsamen Verantwortlichkeit nach Art. 26 Abs. 1 S. 2 DS-GVO nichts grundlegend. Zwar kann die Übermittlung der identifizierenden Merkmale hier vereinbart werden. Dies ist jedoch weder eine zwingende Voraussetzung noch eine zwingende Folge der gemeinsamen Verarbeitung. 1485

Kann beim Datenaustausch nicht auf anonymisierte oder pseudonymisierte Daten zurückgegriffen werden, muss der Erforderlichkeitsprüfung mehr Aufmerksamkeit geschenkt werden. Wie bei der Verarbeitung zur Erfüllung eines Vertrags stellt sich hier die Frage, wie deren Zweck genau lautet. Ähnlich der Situation bei Assistenzsystemen muss man hier von den funktionalen Anforderungen ausgehen, die ein Produktionssystem zu erfüllen hat (siehe 3.6.1.2.1.4, S. 501). Der Wille des Arbeitgebers allein, im Produktionsverbund agieren zu können, genügt dafür noch nicht. Es muss vielmehr klarwerden, welcher Arbeitsschritt im Verbund auszuführen ist. Dabei muss sich die Erforderlichkeit auch speziell auf die personenbezogene Übermittlung beziehen. Gerade der Umstand, aufgrund dessen nicht 1486

1648 *Wedde,* in: Däubler et al. 2020, § 26 BDSG, Rn. 188 f.

auf anonymisierte oder pseudonymisierte Daten zurückgegriffen werden kann, bedarf einer eingehenden Erörterung. Die Frage, ob der bezweckte Arbeitsschritt nicht ebenso gut intern durchgeführt werden könnte, dürfte angesichts der stark arbeitsteilig organisierten Industrie[1649] hingegen zumeist nur theoretischer Natur sein.

3.6.2.4.4 Interessenabwägung

1487 Nicht jedes grundrechtlich geschützte Interesse ist aus sich heraus so überzeugend, dass es mit hinreichender Wahrscheinlichkeit die hierfür erforderliche Datenverarbeitung rechtfertigen kann. Das genaue Ergebnis hängt von einer Interessenabwägung im Einzelfall ab. Für diese Abwägung ist das Interesse zunächst zu gewichten. Sodann ist es den grundrechtlich oder grundfreiheitlich geschützten Interessen der betroffenen Person gegenüberzustellen.

3.6.2.4.4.1 Gewichtung des Interesses

1488 Ebenso wie die Abwägung selbst, kann die Gewichtung des Interesses nicht schematisch, sondern muss stets bezogen auf den Einzelfall erfolgen. Es besteht aber eine gewisse Vermutung für das Gewicht eines Interesses, wenn es in den Erwägungsgründen ausdrücklich anerkannt wird. Neben den in ErwG 47 S. 2 angesprochenen Beziehungen zwischen Arbeitgeber und Beschäftigten kommt speziell für den Datenaustausch in Wertschöpfungsnetzwerken ein Vergleich mit dem konzernweiten Datenaustausch für interne Verwaltungszwecke nach ErwG 48 S. 1 in Betracht.

1489 Wertschöpfungsnetzwerke unterscheiden sich zwar in wesentlichen Punkten von Unternehmensgruppen, sodass aus ErwG 48 keine direkten Schlüsse gezogen werden können.[1650] So steht hinter der ausdrücklichen Erwähnung dieser Form der Zusammenarbeit, dass hier die Tätigkeit einzelner Beschäftigter oder die Vorgesetztenstrukturen über mehrere Unternehmen verteilt sein können.[1651] Davon kann in Produktionsverbünden keine Rede sein. Die Gründe, ein einheitliches Unternehmen in eine Unternehmensgruppe zu zerlegen, sind aber nicht a priori anerkennenswerter als jene,

1649 *Stockburger/Hengstenberg,* Spiegel Online, 19.8.2016.
1650 *Seifert* 2018, S. 182.
1651 *Schneider et al.,* in: Forgó et al. 2019, Teil VI Kapitel 1, Rn. 9.

die Produktion nicht vollständig selbst, sondern unter maßgeblicher Hinzuziehung von Zulieferern zu organisieren. Die enge wirtschaftliche Zusammenarbeit von Unternehmen wird darum allgemein als berechtigtes Interesse anzuerkennen sein, dass prinzipiell die Übermittlung von Beschäftigtendaten rechtfertigen kann.

3.6.2.4.4.2 Kriterien für die Abwägung

Die Unterscheidung zwischen Kontrolle und Einsichtnahme kann im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO nicht angewendet werden, weil dieser Erlaubnistatbestand nur zum Tragen kommt, wenn eine Maßnahme gerade keiner der beiden Zweckkategorien zugerechnet werden kann. Bei der Interessenabwägung ist aber zu beachten, dass es sich zumeist um Daten ohne gezielten Personenbezug handelt, deren Verarbeitung typischerweise nur mit einem geringen Eingriff in die Rechte des betroffenen Beschäftigten verbunden ist. Es dürfte kaum möglich sein, sich anhand dieser Daten ein einigermaßen umfassendes Bild über die Arbeit oder die Persönlichkeit des betroffenen Beschäftigten zu machen. 1490

Der Schwerpunkt der Zulässigkeitsprüfung liegt darum nicht bei der Aussagekraft der einzelnen Daten. In den wenigen Fällen, in denen der Personenbezug der Daten nicht effektiv ausgeschlossen werden kann, dürfte dieser Prüfungspunkt keine besonderen Probleme bereiten. Die Interessenabwägung entfaltet ihre Wirkung dafür bei den Besonderheiten der Übermittlung und der daran anschließenden Datenverarbeitung. 1491

3.6.2.4.4.2.1 Besondere Anforderungen an die Beteiligten

Die Grundsätze des Datenschutzrechts nach Art. 5 DS-GVO einzuhalten bedeutet nicht nur, dass der Umfang der Daten und die Anzahl der Empfänger auf ein notwendiges Minimum zu begrenzen sind. Die Daten dürfen darüber hinaus auch nur gebunden an den Übermittlungszweck[1652] und so lange und so intensiv wie nötig verarbeitet werden. Die Einhaltung dieser Anforderung ist gemäß Art. 25 Abs. 1 DS-GVO technisch und organisatorisch abzusichern. 1492

1652 *Hofmann/Hornung* 2018, S. 243; *Roßnagel, et al.* 2006, S. 115; *Wedde*, in: Däubler et al. 2020, § 26 BDSG, Rn. 189.

1493 Die Verantwortung hierfür trifft die übermittelnde und die empfangende Stelle grundsätzlich jeweils unabhängig voneinander für ihre Seite des Datenaustauschs. Eine gemeinsame Verantwortlichkeit des übermittelnden Arbeitgebers nach Art. 26 Abs. 1 S. 1 DS-GVO ist keine zwingende Folge der Beteiligung an einem Wertschöpfungsnetzwerk. Die Zuverlässigkeit des Empfängers ist allerdings im Rahmen der Interessenabwägung für die Übermittlung zu berücksichtigen und wirkt sich damit indirekt trotzdem auf den Übermittler aus.

1494 Die Einhaltung dieser Anforderungen wird die beteiligten Unternehmen gerade bei dem besonders umfangreichen automatischen Datenaustausch in Wertschöpfungsnetzwerken vor erhebliche Herausforderungen stellen. Das Mindeste ist es, die Berechtigung jedes potenziellen Empfängers für jede Datenkategorie einzeln im Vorhinein festzulegen. Die Funktionen, die eine Plattform wie der Industrial Data Space dem Datengeber bieten soll (siehe 3.6.2.4.1.3.1, S. 557), sind darum nicht nur im wohlverstandenen Eigeninteresse des Unternehmens zu nutzen. Es ist hierzu auch datenschutzrechtlich verpflichtet, wenn es über das Wertschöpfungsnetzwerk personenbezogene Daten austauschen will. Ein nach dem Prinzip der vollständigen Transparenz aufgebautes Netzwerk,[1653] bei dem jeder Beteiligte auf alle – ggf. auch personenbezogenen – Informationen zugreifen kann, ist folglich nicht nur unter dem Gesichtspunkt des Schutzes von Unternehmensgeheimnissen problematisch,[1654] sondern unterliegt auch datenschutzrechtlichen Beschränkungen.[1655]

1495 Sobald sich die Zusammenarbeit, der in über ein Wertschöpfungsnetzwerk zusammengeschlossenen Unternehmen aber verstetigt, ist davon auszugehen, dass über einen längeren Zeitraum eine Vielzahl von Daten ausgetauscht werden. Damit steigen die Kombinationsmöglichkeiten, die sich dem Datenempfänger bieten und mit ihr die Aussagekraft der Daten. Darauf muss mit einem entsprechenden Schutzkonzept reagiert werden, dass die Verarbeitung der Daten auch beim Empfänger z.B. wirksam an den mithilfe der Plattform verfolgten Zweck bindet.

1653 *New,* HBR 2010, S. 76–83.
1654 *Hofmann,* JurPC Web-Dok. 158/2015, Rn. 18 ff.
1655 *Hofmann/Hornung* 2018, S. 243.

3.6.2.4.4.2.2 Mögliche Umsetzung in Wertschöpfungsnetzwerken

Für die intensive Zusammenarbeit weniger Unternehmen bietet sich klassisch das Instrument der Auftragsdatenverarbeitung nach Art. 28 DS-GVO an. Die notwendige Zuverlässigkeit des Auftragsdatenverarbeiters kann hier gemäß Art. 28 Abs. 5 DS-GVO durch die Einhaltung von branchenweiten Verhaltensregeln nach Art. 40 DS-GVO oder eines genehmigten Zertifizierungsverfahrens nach Art. 42 DS-GVO nachgewiesen werden. 1496

Die Auftragsdatenverarbeitung ist aber so konzipiert, dass der Auftragnehmer nur im Interesse und auf Weisung des Verantwortlichen verarbeitet. Hat er an den Daten ein eigenes Interesse, verarbeitet er sie also gewissermaßen auf eigene Rechnung, scheidet eine Auftragsdatenverarbeitung aus.[1656] Das wird bei Wertschöpfungsnetzwerken, bei denen es darum geht, die jeweils eigene Produktion und Logistik untereinander abzustimmen, aber regelmäßig der Fall sein.[1657] Darüber hinaus würden sich Kontrollpflichten in einem solchen Netzwerk nicht durchsetzen lassen.[1658] 1497

Für Wertschöpfungsnetzwerke bietet sich zumindest bei sehr intensiver Zusammenarbeit das Konzept der gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO als Ersatz zur Auftragsdatenverarbeitung an. So kann auch in nicht-hierarchischen Strukturen die notwendige Zuverlässigkeit der Partner gewährleistet werden. Der Umstand allein, dass die spezifischen Anforderungen an eine Auftragsdatenverarbeitung hier nicht erfüllt werden können, ist unschädlich. Gerade die Kontrollpflichten für die Auftragsdatenverarbeitung sind auf einen umfangreichen Austausch u.U. auch sensibler personenbezogener Daten ausgelegt, wie dies etwa bei Lohn- und Gehaltsabrechnungen über externe Dienstleister der Fall wäre. Der Datenaustausch in Wertschöpfungsnetzwerken wird kaum je ein vergleichbares Gefahrenpotenzial entwickeln, das solch weitreichende Instrumente erforderlich machte. Entsprechend könnte auch der weniger wirksame Ansatz der gemeinsamen Verantwortlichkeit genügen. 1498

Für die konkrete Ausgestaltung der gemeinsamen Verantwortlichkeit können Anleihen am System der Auftragsdatenverarbeitung genommen werden. So werden die Beteiligten in großen und u.U. flexibel ausgestalteten Wertschöpfungsnetzwerken oft nicht in der Lage sein, sämtliche potenziel- 1499

1656 *Petri,* in: Simitis et al. 2019, Art. 28 DS-GVO, Rn. 3; BeckOK DSR/*Schild*, Art. 4 DS-GVO, Rn. 98.
1657 *Hornung/Hofmann* 2018, S. 46.
1658 *Plattform Industrie 4.0* 2016, S. 14.

le Partner eingehend zu prüfen. Wie bei der Auftragsdatenverarbeitung nach Art. 28 Abs. 5 DS-GVO könnten auch hier Zertifizierungen oder branchenweite Verhaltensregeln eine praktikable Lösung erleichtern.[1659]

1500 Eine zentrale Aufgabe wird dabei Plattformbetreibern zukommen. Sie können zum einen die technische Infrastruktur stellen, um das Wertschöpfungsnetzwerk zu realisieren, zum anderen aber auch die Zertifizierung vornehmen oder Verhaltensregeln vorgeben.[1660] Hierzu passt, dass auch im Industrial Data Space eine Zertifizierungsinstanz[1661] vorgesehen ist. Dies wäre eine Möglichkeit, die Interessenabwägung für den Arbeitgeber positiv zu gestalten.

3.6.2.5 Automatische Entscheidung

1501 Produktions- und Assistenzsysteme, die den Beschäftigten Anweisungen erteilen, eine bestimmte Tätigkeit zu verrichten, sei es ein einzelner Handgriff und oder eine komplexe Wartungsaufgabe, können dies prinzipiell auch vollautomatisch tun. In diesen Fällen stellt die Verordnung neben den bereits diskutierten allgemeinen Vorgaben für die Zulässigkeit der Datenverarbeitung in Art. 22 DS-GVO zusätzliche Anforderungen[1662] auf, die sich spezifisch darauf beziehen, dass die Entscheidung automatisiert getroffen wurde.

3.6.2.5.1 Anwendungsbereich der Norm

1502 Nach Art. 22 DS-GVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

1659 *Hofmann* 2017, S. 180 ff.
1660 *Hornung/Hofmann* 2018, S. 49. Zu dem Potenzial von Plattformen in der Industrie 4.0 allgemein *Spindler* 2018, S. 152 ff.
1661 *Fraunhofer* 2016, S. 17.
1662 BeckOK DSR/*Lewinski*, Art. 22 DS-GVO, Rn. 3 f.

3.6.2.5.1.1 Entscheidung

Die Entscheidung muss gegenüber der betroffenen Person eine rechtliche Wirkung[1663] entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen. Zumindest ersteres kann bei Weisungen des Arbeitgebers unschwer bejaht werden. Sie konkretisieren die Leistungspflicht des Arbeitnehmers und legen ihm so die Rechtspflicht auf, der betreffenden Weisung zu folgen, also etwa eine bestimmte Arbeit zu erledigen oder Aufgaben in einer bestimmten Reihenfolge zu erfüllen. Auch die Tatsache, dass der Arbeitnehmer womöglich ein Interesse an einer (rechtmäßigen) Weisung des Arbeitgebers hat, ändert daran nichts.[1664] Etwas anderes gälte nur, wenn die Anweisung des Systems nicht als Weisung im Rechtssinne gestaltet wäre, sondern lediglich als Empfehlung.[1665] Das mag im Hinblick auf die spezifischen Fähigkeiten des Menschen sinnvoll sein (siehe 1.2.3.1, S. 64), ist aber eine Ausgestaltungsentscheidung des Arbeitgebers. 1503

3.6.2.5.1.2 Gegenstand und Grad der Automatisierung

Gemäß Art. 22 Abs. 1 DS-GVO kommt die Norm zur Anwendung, wenn eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung im Raum steht. Ein Vergleich mit der Überschrift zeigt, dass sich die Automatisierung nicht allein auf die Datenverarbeitung bezieht, sondern auch auf die Entscheidung selbst. Auch die Entscheidungsfindung muss demnach automatisiert ablaufen. Es genügt also nicht, dass die Ent- 1504

1663 A.A. *Schulz,* in: Gola 2018, Art. 22 DS-GVO, Rn. 22, demzufolge die rechtliche Wirkung selbst auch beeinträchtigend sein muss.

1664 A.A. *Bomhard* 2019, S. 60, der darauf abstellt, dass der Arbeitnehmer ohne eine Weisung des Arbeitgebers nicht arbeiten könne und seinen Anspruch auf Arbeitsentgelt verliere. Diese Annahme ist falsch, der Arbeitgeber geriete in diesem Fall in Annahmeverzug nach § 293 BGB; der Arbeitnehmer behielte gemäß § 615 Abs. 1 S. 1 BGB seinen Anspruch auf Arbeitsentgelt (dazu nur ErfK/*Preis*, § 615 BGB, Rn. 75). Der Arbeitnehmer muss die geschuldete Leistung also gemäß §§ 294 f. BGB nur in jenem Rahmen anbieten, dem auch das Weisungsrecht unterliegt (siehe 2.4.2, S. 190), ErfK/*Preis*, § 615 BGB, Rn. 16 ff. Daran ändert auch die Einordnung der Arbeitsleistung als absolute Fixschuld nichts, BAG v. 23.9.2015 – 5 AZR 146/14, E 152, S. 327, 25 f. (=NZA 2016, S. 293); ErfK/*Preis*, § 615 BGB, Rn. 7. Unklar zum Anwendung auf Weisungen *Brecht et al.*, PinG 2018, S. 10, 13.

1665 *Däubler* 2018, § 10 Rn. 12.

scheidung in irgendeiner Weise auf automatisierten Verfahren beruht, sie muss auch automatisiert getroffen werden.[1666]

1505 Die Norm erhält durch diese Einschränkung einen vergleichsweise kleinen Anwendungsbereich. Jede relevante menschliche Beteiligung an der Entscheidungsfindung, die sich nicht in symbolischen Gesten erschöpft, führt dazu, dass die Entscheidung nicht ausschließlich, sondern eben nur teilweise auf einer automatisierten Entscheidung beruht. Was als relevant zu betrachten ist, bestimmt sich am Schutzgedanken der Norm. Die Aussage, der Mensch solle nicht der Entscheidung einer Maschine unterworfen werden, nicht zu deren Objekt werden,[1667] ist für sich genommen aber nicht hilfreich, solange man die spezifischen Risiken automatisierter Entscheidungen nicht kennt, die den europäischen Verordnungsgeber zu dieser Entscheidung motiviert haben.

1506 Die risikobasierten Erwägungen für Art. 22 DS-GVO lassen sich der Verordnung nur indirekt entnehmen. Die Schutzmaßnahmen nach ErwG 71 S. 6 lassen die Befürchtung erkennen, automatisierte Entscheidungen könnten häufiger sachlich unrichtig[1668] sein oder auf verpönten Kriterien wie Ethnie, Weltanschauung usw. beruhen. Und selbst wenn dies nicht der Fall wäre, wenn die Entscheidung von einem Menschen also genauso getroffen worden wäre, ist jedenfalls die Intransparenz automatisierter Entscheidungen problematisch (siehe 2.4.7.3.1.2, S. 213).[1669] Wenn die betroffene Person die Gründe für die Entscheidung nicht einsehen kann, hinterlässt das den bösen Schein einer falschen oder diskriminierenden Entscheidung, der selbst schon zu vermeiden ist.

1507 Von einem relevanten menschlichen Beitrag kann man nur sprechen, wenn die genannten Risiken durch ihn wirksam beseitigt würden. Der Mensch muss folglich über die notwendige Sach- und Fachkunde verfügen, um die automatisierte Entscheidung auf Richtigkeit und Rechtmäßigkeit zu überprüfen. Das muss er wenigstens in der Form einer Plausibili-

---

1666 *Helfrich,* in: Sydow 2018, Art. 22 DS-GVO, Rn. 42; BeckOK DSR/*Lewinski*, Art. 22 DS-GVO, Rn. 22 f.; *Martini,* in: Paal/Pauly 2018, Art. 22 DS-GVO, Rn. 15a; *Scholz,* in: Simitis et al. 2019, Art. 22 DS-GVO, Rn. 25 f.; *Schulz,* in: Gola 2018, Art. 22 DS-GVO, Rn. 14.

1667 BeckOK DSR/*Lewinski*, Art. 22 DS-GVO, Rn. 2.; ähnlich *Martini,* in: Paal/Pauly 2018, Art. 22 DS-GVO, Rn. 8.

1668 *Weichert,* in: Däubler et al. 2020, Art. 22 DS-GVO, Rn. 21.

1669 Zum Transparenzproblem *Weichert,* in: Däubler et al. 2020, Art. 22 DS-GVO, Rn. 16 f.

tätskontrolle tun.[1670] Damit wird die Fehleranfälligkeit kompensiert. Um der Transparenz Genüge zu tun, muss der Mensch mindestens über die wesentlichen Entscheidungsgründe im Bilde sein, sodass er die Entscheidung ggf. gegenüber der betroffenen Person rechtfertigen könnte. Diesbezüglich geht es aber nur um eine Parallelwertung, wie sie ein Mensch anstellen würde. Eine genaue Kenntnis des Algorithmus wird man nicht verlangen können.

Damit dem automatisierten Vorgang schließlich der Charakter der Entscheidung genommen wird, muss der Mensch seinerseits über einen Entscheidungsspielraum verfügen, welcher die Entscheidung zu seiner eigenen werden lässt.[1671] Das muss nicht heißen, dass der Mensch Einfluss auf den Inhalt der Entscheidung nehmen können muss, dergestalt, dass er den Vorschlag des Systems durch eine eigene Entscheidung ersetzen kann. Es genügt bereits, wenn er den Entscheidungsvorschlag bestätigen oder ablehnen kann.[1672] Die Vorarbeit des Computers mag den Menschen träge machen und in der trügerischen Sicherheit wiegen, einen objektiven und richtigen Vorschlag unterbreitet zu bekommen.[1673] Dies ist besonders problematisch, wenn Algorithmen als etwas gänzlich Neutrales mystifiziert werden.[1674] Der Wortlaut der Norm spricht aber eine klare Sprache. Die Entscheidung muss ausschließlich und nicht nur wesentlich auf der automatisierten Verarbeitung beruhen. 1508

3.6.2.5.1.3 Qualität der Datenverarbeitung

Die Vorgängernorm zu Art. 22 DS-GVO, Art. 15 DSRL enthielt in Absatz 1 noch die Einschränkung, dass die Datenverarbeitung „zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise 1509

1670 Zu Kompetenz und Kontrolldichte BeckOK DSR/*Lewinski*, Art. 22 DS-GVO, Rn. 23 f.; a.A. *Wolber,* CR 2003, S. 623, 625, die keine auf die Entscheidung bezogenen Kenntnisse verlangt.

1671 BeckOK DSR/*Lewinski*, Art. 22 DS-GVO, Rn. 25; *Martini,* in: Paal/Pauly 2018, Art. 22 DS-GVO, Rn. 18 f.; *Weichert,* in: Däubler et al. 2020, Art. 22 DS-GVO, Rn. 25.

1672 *Martini,* in: Paal/Pauly 2018, Art. 22 DS-GVO, Rn. 20; a.A. *Bretthauer* 2017, S. 170 f.

1673 In diese Richtung auch *Mantz/Spittka,* in: Sassenberg/Faber 2019, § 6, Rn. 31, die die Norm aus diesem Grund rechtspolitisch für beobachtungsbedürftig halten.

1674 Siehe zum sog. Search Engine Bias *Hartl* 2017, S. 52 ff.

ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens." Diese Einschränkung ist nun beinahe wortgleich und um weitere Beispiele für Aspekte der Persönlichkeit ergänzt in ErwG 71 S. 1 und 2 enthalten. Dabei werden die Arbeitsleistung und der Aufenthaltsort ausdrücklich erwähnt.

3.6.2.5.1.3.1 Ausnahmen für einfache Entscheidungen

1510 Diese Einschränkung ist in Art. 22 DS-GVO hineinzulesen.[1675] Nicht jedes personenbezogene Datum lässt Rückschlüsse auf die in ErwG 71 S. 1 und 2 erwähnten persönlichen Aspekte zu. Insbesondere die Verarbeitung identifizierender Merkmale wie des Fingerabdrucks[1676] oder einer eindeutigen Kennung weist keine der genannten spezifischen Risiken automatisierter Entscheidungen auf. Systeme, die anhand dieser eingeschränkten Parameter etwa die Zugangsberechtigung eines Beschäftigten prüfen und eine entsprechende Entscheidung folgen lassen, unterziehen die betroffene Person keiner Bewertung ihrer persönlichen Aspekte, die aufgrund ihrer Komplexität in gesteigerten Maße unrichtig oder diskriminierend sein könnte.[1677]

1511 Dies hat zur Folge, dass nicht sämtliche Assistenzsysteme, die personenbezogene Daten zu automatisierten Entscheidungen heranziehen, unter Art. 22 DS-GVO fallen. Wird z.B. nur ermittelt, ob der Arbeitsschritt richtig durchgeführt wurde, um ad-hoc bestätigende oder korrigierende Anweisungen zu geben, geht damit keine Bewertung persönlicher Merkmale einher. Systeme, welche die Hände von Kommissionierern oder Monteuren filmen und überprüfen, ob der Artikel richtig einsortiert bzw. das Bauteil korrekt angebracht wurde, treffen dadurch nicht zwingend automatisierte Entscheidungen nach Art. 22 DS-GVO. Gleiches gilt, soweit lediglich die Eintragungen über die zeitliche Verfügbarkeit in einem „Schicht-Doodle" (siehe 2.4.7.1.2, S. 207) ausgewertet werden.

1675 *Schulz*, in: Gola 2018, Art. 22 DS-GVO, Rn. 20; *Weichert*, in: Däubler et al. 2020, Art. 22 DS-GVO, Rn. 15.

1676 BeckOK DSR/*Lewinski*, Art. 22 DS-GVO, Rn. 10; noch zur im Wesentlichen inhaltsgleichen Regelung in Art. 15 DSRL und § 6a BDSG *Hornung* 2005, S. 282 f.

1677 *Weichert*, in: Däubler et al. 2020, Art. 22 DS-GVO, Rn. 17.

3.6.2.5.1.3.2 Umgang mit Fähigkeitsprofilen

Bei Assistenzsystemen, die auf Fähigkeitsprofile zurückgreifen, um Aufgaben oder Schichten passgenau einzelnen Mitarbeitern zuweisen zu können, ist dagegen zu differenzieren. Ein System, das diese Profile eigenständig auswertet, und selbst entscheidet, ob der jeweilige Mitarbeiter für die Arbeit geeignet ist, wird von Art. 22 DS-GVO erfasst. Die Unterscheidung zwischen Einsichtnahme und Kontrolle spielt hier keine Rolle. Maßgeblich ist nur, dass die Entscheidung automatisiert aufgrund der Bewertung von persönlichen Aspekten erfolgt, nicht welchen Inhalts sie ist. 1512

Etwas anderes gilt aber, wenn die Qualifikation der Mitarbeiter bereits ohne Weiteres aus dem Profil ersichtlich wird, also lediglich ausgelesen und nicht automatisiert ermittelt wird. Ist bspw. in einem „Schicht-Doodle" (siehe 2.4.7.1.2, S. 207) hinterlegt, dass in der fraglichen Zeit Schweißarbeiten zu verrichten sind, kommen nur diejenigen Mitarbeiter in Betracht, die hierfür die notwendige Fachkunde besitzen. Sie wird im Fähigkeitsprofil schlicht vermerkt sein, ebenso wie in einer Kartei vermerkt ist, zu welchen Bereichen der Beschäftigte Zugang hat. Hier werden keine Aspekte der Person bewertet; Art. 22 Abs. 1 DS-GVO wäre nicht einschlägig. 1513

Die Regelung in Art. 22 DS-GVO betrifft schließlich nur die Verwendung der Daten zur Entscheidungsfindung, nicht aber das Erheben und Verknüpfen der Daten zu Profilen.[1678] Würden also Daten aus einem ersten Assistenzsystem, das selbst nicht unter Art. 22 DS-GVO fällt, zweckändernd dazu verwendet, Fähigkeitsprofile für ein zweites Assistenzsystem aufzubauen, änderte dies im Hinblick auf Art. 22 DS-GVO nichts an der Beurteilung der beiden Systeme. Die Weiterverwendung der Daten könnte zwar mit dem Erhebungszweck unvereinbar und die Profilbildung darum unzulässig sein. Abgesehen davon, dass dies bei einer Begrenzung der Zwecke auf die Einsichtnahme nicht sonderlich wahrscheinlich wäre, würde das erste System aber weiterhin nicht in den Anwendungsbereich von Art. 22 Abs. 1 DS-GVO fallen. 1514

3.6.2.5.2 Ausnahmsweise Gestattung

Das Verbot der automatisierten Entscheidung wirkt nicht absolut, sondern enthält in Art. 22 Abs. 2 DS-GVO verschiedene Gestattungstatbestände. 1515

1678 BeckOK DSR/*Lewinski*, Art. 22 DS-GVO, Rn. 3.

Für den Beschäftigungskontext ist hier Art. 22 Abs. 1 lit. a DS-GVO relevant, der die Entscheidung vom Verbot in Absatz 1 freistellt, wenn sie u.a. für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Die übrigen Gestattungstatbestände spielen im Beschäftigungsverhältnis hingegen keine Rolle.

3.6.2.5.2.1 Für die Vertragserfüllung erforderlich

1516 Die Erforderlichkeit einer automatisierten Entscheidung für die Vertragserfüllung ist im Grundsatz genauso wie die Erforderlichkeit der Datenverarbeitung zu beurteilen.[1679] Das gilt insbesondere für den Maßstab der Erforderlichkeit, der auch im Rahmen des Art. 22 DS-GVO nicht bedeutet, dass die Automatisierung der Entscheidung schlechthin unverzichtbar sein muss (siehe 3.4.1.4.7, S. 403). Diese Aussage wäre nur dann richtig, wenn man erstens auf den – nach dem jeweiligen mitgliedstaatlichen Vertragsrecht zu ermittelnden[1680] – konkreten Vertragszweck abstellt[1681] und zweitens bei der Entscheidung über die Erforderlichkeit die Kosten einer menschlichen Entscheidung nicht völlig außer Acht lässt.

1517 Der Vertragszweck muss vom Arbeitgeber zunächst durch sein Weisungsrecht konkretisiert werden. Dies geschieht, indem er die Funktionen festlegt, über die das Produktions- oder Assistenzsystem verfügen soll, wobei ihm ein gewisser Entscheidungsspielraum zusteht (siehe 3.6.1.2.1.6, S. 505).

1518 Dieses Vorgehen ist dann problematisch, wenn die unternehmerische Entscheidung für eine bestimmte Funktion weite Teile der Erforderlichkeitsprüfung vorwegnimmt. Dies wäre etwa bei der Personalisierung eines Systems der Fall (siehe 3.6.1.2.1.4.2, S. 502). Eine solche Zweckkonkretisierung unterliegt nur einer eingeschränkten Willkür- und Plausibilitätskontrolle, was sich letztlich auf den Kontrollumfang der Erforderlichkeitsprüfung auswirkt. Insbesondere die Frage, ob Daten überhaupt mit dieser Zielrichtung verarbeitet werden sollen, wird so einer eingehenden Prüfung entzogen. Der Effekt dieser Entscheidung wird aber dadurch begrenzt, dass die konkrete Umsetzung dieser Entscheidung einer umfangrei-

---

1679 So auch *Buchner,* in: Kühling/Buchner 2018, Art. 22 DS-GVO, Rn. 30; *Scholz,* in: Simitis et al. 2019, Art. 22 DS-GVO, Rn. 41 ff.

1680 So auch *Martini,* in: Paal/Pauly 2018, Art. 22 DS-GVO, Rn. 31.

1681 *Martini,* in: Paal/Pauly 2018, Art. 22 DS-GVO, Rn. 31; *Scholz,* in: Simitis et al. 2019, Art. 22 DS-GVO, Rn. 42.

chen Kontrolle nach dem Erforderlichkeitsprinzip unterliegt, was insbesondere den Umfang der Datenverarbeitung, die Intensität, die Speicherdauer und die Zweckbindung betrifft (siehe 3.6.1.2.2, S. 506). Zumindest innerhalb von Vertragsverhältnissen kommt hinzu, dass entsprechend der gegenseitigen Rücksichtnahmepflichten eine abschließende Interessenabwägung vorzunehmen ist (siehe 3.4.1.3.4.2.1, S. 381).

Die Interessenabwägung ist umso wichtiger, je weniger die Entscheidung des Arbeitgebers einer differenzierten Umsetzung bedarf, je weniger sie also anhand des Erforderlichkeitsprinzips ausgestaltet und abgemildert werden kann. Die Entscheidung, ein System automatisiert Weisungen erteilen zu lassen, würde nämlich gleichsam bedeuten, dass diese automatisierten Entscheidungen nach Art. 22 Abs. 2 lit. a DS-GVO erforderlich wären. Angesichts dieses Effektes der Zwecksetzung, muss diese Entscheidung des Arbeitgebers in der Interessenabwägung besonders kritisch betrachtet werden. 1519

Es stellt sich ganz allgemein die Frage, welche Vorteile das vollautomatisierte Erteilen von Weisungen im Beschäftigungsverhältnis haben soll. Dabei geht es weniger um die Art der Entscheidungsfindung, deren Effizienz durchaus auf der Hand liegen kann. Die Erforderlichkeitsprüfung erstreckt sich auch auf die Frage, ob das Ergebnis dieses automatisierten Prozesses als bindende Weisung oder nur als Vorschlag formuliert wird. Der Vorteil einer Weisung wird nämlich dadurch zunichtegemacht, dass der Arbeitgeber dem Beschäftigten in diesem Fall gemäß Art. 22 Abs. 3 Var. 3 DS-GVO ein „Anfechtungsrecht" einräumen muss. 1520

Dieses Anfechtungsrecht nach Art. 22 Abs. 3 DS-GVO ist nicht im Sinne einer Anfechtung nach §§ 119 ff. BGB zu verstehen, sondern verleiht der betroffenen Person – hier dem Arbeitnehmer – einen Anspruch auf Überprüfung der Entscheidung.[1682] Da die betroffene Person nach Art. 22 Abs. 3 Var. 1 DS-GVO auch das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen hat, muss diese Überprüfung durch einen Menschen erfolgen, der eigene Plausibilitäts- und Richtigkeitserwägungen anstellt.[1683] Im Rahmen dieses Prozesses ist der betroffenen Person gemäß Art. 22 Abs. 1 Var. 2 DS-GVO dann auch die Möglichkeit zu geben, den eigenen Standpunkt darzulegen. 1521

1682 *Kühling, et al.* 2016, S. 65; BeckOK DSR/*Lewinski*, Art. 22 DS-GVO, Rn. 50; zur Umsetzung als „Remonstrationsknopf" *Bomhard* 2019, S. 18.

1683 BeckOK DSR/*Lewinski*, Art. 22 DS-GVO, Rn. 48; *Martini,* in: Paal/Pauly 2018, Art. 22 DS-GVO, Rn. 39c; *Scholz,* in: Simitis et al. 2019, Art. 22 DS-GVO, Rn. 59.

1522 Eine automatisiert getroffene Entscheidung wäre also ohnehin nicht letztverbindlicher Natur. Hinzu kommt, dass ein so gestaltetes System das spezifische Potenzial des Menschen in der Industrie 4.0 als im eigentlichen Sinne intelligentes Element (siehe 1.2.3.1, S. 64) nicht ansatzweise ausschöpfen würde.

1523 Schließlich müssen bei der Zwecksetzung auch gewisse Richtungsentscheidungen des Gesetzgebers berücksichtigt werden. Der Schutz der Persönlichkeit der Arbeitnehmer im Sinne einer guten Arbeit ist zwar nur sehr zurückhaltend im einfachen Recht verankert (siehe 2.3.6.2, S. 178). Das automatisierte Erteilen von Weisungen stellt für den Beschäftigten aber eine unter Persönlichkeitsaspekten betrachtet sehr beeinträchtigende Arbeitsgestaltung dar. Der betroffene Arbeitnehmer wird gerade bei einem kleinteiligen Kontrollansatz nahezu vollständig seiner Handlungsautonomie beraubt. Wenn die Vorteile dann derart zweifelhaft erscheinen, ist es auch nach den Maßstäben einer Plausibilitätskontrolle nicht gerechtfertigt, Weisungen automatisiert zu erteilen.

1524 Ein Arbeitgeber wird sich darum in aller Regel nicht auf den Gestattungstatbestand in Art. 22 Abs. 2 lit. a DS-GVO berufen können. Er muss sich folglich in den Bereichen, in denen er persönliche Aspekte der Beschäftigten für automatisierte Anweisungen durch das System nutzen will, auf im Rechtssinne bloße Hinweise und Empfehlungen beschränken.[1684]

3.6.2.5.2.2 Die übrigen Gestattungstatbestände

1525 Die beiden anderen Tatbestände sind für den Beschäftigungskontext nicht relevant. Von der Öffnungsklausel in Art. 22 Abs. 2 lit. b DS-GVO hat der deutsche Gesetzgeber im Beschäftigungskontext keinen Gebrauch gemacht. Die einzige direkt darauf beruhende Regelung in § 37 BDSG 2018 betrifft lediglich das Versicherungswesen. Hieran können auch Kollektivvereinbarungen nichts ändern. Dies zeigt ein Vergleich mit den Öffnungsklauseln in Art. 9 Abs. 2 lit. b und Art. 88 Abs. 1 DS-GVO. Während Kollektivvereinbarungen dort eigens genannt sind, werden sie in Art. 22 Abs. 2 lit. b DS-GVO nicht erwähnt. Für automatisierte Entscheidungen können die Tarif- oder Betriebsparteien darum keine Ausnahmen vom Verbot in Art. 22 Abs. 1 DS-GVO vereinbaren.

1684 *Däubler* 2018, § 10 Rn. 12; *Neighbour,* in: Sassenberg/Faber 2019, § 8, Rn. 70.

Automatisierte Entscheidungen mit der Einwilligung des betroffenen Beschäftigten nach Art. 22 Abs. 2 lit. c DS-GVO zu gestatten, ist dagegen auch im Beschäftigungsverhältnis grundsätzlich möglich. Allerdings muss auch diese Einwilligung freiwillig sein. Damit bestehen hier dieselben Vorbehalte, wie sie auch in Bezug auf die übrige Datenverarbeitung bestehen (siehe 3.6.1.5, S. 523). Diese Lösung ist darum wohl nicht praktikabel. 1526

3.7 Fazit zum Beschäftigtendatenschutz

Hinter der datenschutzrechtlichen Betrachtung steht die Frage, wie die Arbeitsbedingungen in der Industrie 4.0 trotz der technologischen Umwälzungen so gestaltet werden können, dass das Persönlichkeitsrecht der Beschäftigten dennoch gewahrt bleibt und – daran anschließend – inwiefern sich hieraus Beschränkungen für die technische Umsetzung ergeben. 1527

3.7.1 Primärrechtliche Vorgaben und Anwendbarkeit

Die einschlägigen Vorschriften im einfachen Datenschutzrecht sind – besonders, wenn sie die materielle Zulässigkeit der Verarbeitung betreffen – in hohem Maße ausfüllungsbedürftig und teilweise sogar generalklauselartig gefasst. Den Grundrechten der beteiligten Personen kommt hier darum eine besondere Bedeutung zu. 1528

Aufgrund der europarechtlichen Determinierung des Datenschutzrechts kommen vornehmlich europäische Grundrechte zum Tragen. Dies ergibt sich aus dem Anwendungsvorrang der EU-grundrechtskonform auszulegenden Datenschutz-Grundverordnung vor den Grundrechten des Grundgesetzes. Hieran ändert auch die Öffnungsklausel im Bereich des Beschäftigtendatenschutzes nach Art. 88 DS-GVO nichts. Europäische Grundrechte behalten hier grundsätzlich insofern ihre Geltung, als es um die Einhaltung der Grenzen der Öffnungsklausel sowie der in der Öffnungsklausel selbst aufgestellten Anforderungen geht. 1529

Darüber hinaus muss die Öffnungsklausel in Art. 88 DS-GVO – die eine Kann-Vorschrift darstellt – auch von den Mitgliedstaaten genutzt werden, um den Anwendungsvorrang des Unionsrechts zu verdrängen. Das hat der deutsche Gesetzgeber im Hinblick auf die Regelung in Art. 26 Abs. 1 S. 1 BDSG 2018, in der lediglich die Anforderungen des Erlaubnistatbestandes in Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO paraphrasiert werden, jedoch nicht getan. Die deutsche Generalklausel ist darum nur in Randbereichen (§ 26 1530

Abs. 7 BDSG 2018) anwendbar. Die Grundrechte des Grundgesetzes kommen folglich nur zum Tragen, soweit sich die Datenverarbeitung auf andere Erlaubnistatbestände in § 26 BDSG 2018 stützt, etwa auf Kollektivvereinbarungen. In dem großen Bereich der Datenverarbeitung zur Erfüllung eines Vertrags kommt dagegen Art. 6 Abs. 1 UAbs. 1 S. 1 BDSG 2018 und mit ihm die EU-Grundrechte zur Anwendung.

1531 Dies gilt jedoch nur für die spezifischen Regelungen des Datenschutzes. Das Datenschutzrecht regelt eine unüberschaubare Vielzahl an Lebensbereichen mit äußerst unterschiedlichen Interessenlagen. Dies kann nur gelingen, weil es mit dem Erforderlichkeitsprinzip an den Wertungen desjenigen Rechtsgebiets anknüpft, die es vorfindet. Die Zwecksetzung als Anknüpfungspunkt ist maßgeblich durch das jeweilige Fachrecht – in diesem Fall durch das Arbeitsrecht – geprägt. Da das Arbeitsrecht weiterhin größtenteils im Kompetenzbereich der Mitgliedstaaten liegt, kommen hier Grundrechte des Grundgesetzes zur Anwendung. Dies gilt insbesondere für das den Verarbeitungszweck konkretisierende Weisungsrecht des Arbeitgebers.

1532 Der Anwendungsbereich des einfachen und noch viel mehr des grundrechtlichen Datenschutzrechts ist äußerst weitgehend und erfasst im Kontext der automatisierten Datenverarbeitung sämtliche Informationen, die einem einzelnen Beschäftigten zugeordnet werden können. Für die Zuordenbarkeit kommt es maßgeblich auf die Wahrscheinlichkeit an, mit der sie vorgenommen wird. Es zählen darum weder entfernte, nur theoretisch bestehende Verbindungen noch rechtlich unzulässige Zuordnungsmöglichkeiten. Für Produktions- und Assistenzsysteme hat dies drei wesentliche Konsequenzen:

- Daten, die ungezielt verarbeitet wurden, etwa, weil Daten über den Beschäftigten versehentlich miterfasst wurden, unterfallen nicht dem Anwendungsbereich des Datenschutzrechts. Es ist so unwahrscheinlich, dass diese Daten als Informationsquelle für den Arbeitgeber dienen werden, dass die Grundrechte der Beschäftigten nicht gefährdet sind.
- Der Personenbezug von Daten kann bereits durch eine hinreichend technisch abgesicherte externe Pseudonymisierung aufgehoben werden, wenn ausgeschlossen ist, dass eine der beiden Parteien einen Anspruch auf Übermittlung der jeweils fehlenden Merkmale hat. Das ist bei einem vertraglichen Verbot, das Pseudonym mitzuteilen, anzunehmen.
- Kamerabasierte Systeme, welche die Beschäftigten zwar filmen, die aber die Bilder nicht nach personenbeziehbaren Merkmalen auswerten, über keine Schnittstellen nach außen verfügen und die Bilder auch so-

fort wieder löschen, unterfallen nicht dem Datenschutzrecht. Bei entsprechender technischer Absicherung wird auch hier die Schwelle zum Grundrechtseingriff nicht erreicht.

Der weite Anwendungsbereich hat zur Folge, dass die wesentlichen datenschutzrechtlichen Fragen weit überwiegend in der Interessenabwägung zu klären sind. Hier besteht auf europäischer Ebene gerade bei der Abwägung mit den Wirtschaftsgrundrechten des Arbeitgebers noch keine ausdifferenzierte Rechtsprechung. Keine der beiden grundrechtlich geschützten Seiten ist per se höher zu gewichten. Die Erschließung neuer wirtschaftlicher Potenziale kann durchaus ein Mehr an Datenverarbeitung rechtfertigen. In dieser Allgemeinheit gilt dies jedoch nur, wenn keine eingriffsvertiefenden Umstände hinzukommen. Dies wäre aber z.B. der Fall, wenn die Datenverarbeitung ein besonders umfassendes Bild des Verhaltens des Beschäftigten liefert, wenn sie nicht hinreichend transparent erfolgt oder, wenn sie in letzter Konsequenz die wirtschaftliche Lebensgrundlage des Beschäftigten gefährdet. Gerade letzteres ist angesichts des enormen Beobachtungsdrucks nur gerechtfertigt, wenn der Beschäftigte hierzu einen Anlass geliefert hat. 1533

3.7.2 Konkretisierung datenschutzrechtlicher Anforderungen

Die Datenschutz-Grundverordnung enthält zwar für begleitende Fragen wie die Transparenz der Datenverarbeitung ausdifferenzierte Regelungen, die Kernfrage der Zulässigkeit der Datenverarbeitung richtet sich aber nach wenigen in Art. 5 und 6 DS-GVO geregelten Grundsätzen. Das Hauptinstrument hierfür ist die Erforderlichkeitsprüfung, die auch im Rahmen des Beschäftigungsverhältnisses aus dem bekannten Dreischritt aus Geeignetheit, Erforderlichkeit und Angemessenheit der Datenverarbeitung besteht. Fraglich ist aber, wie in diesem Aufbau die Besonderheiten des Arbeitsrechts berücksichtigt werden können. 1534

Das Arbeitsverhältnis zeichnet sich dadurch aus, dass der Arbeitgeber kraft seines Weisungsrechts nicht nur einen tatsächlichen, sondern auch einen rechtlich fundierten Entscheidungsspielraum hat, wie er den Arbeitnehmer einsetzt. Aus dem Recht – und teilweise auch der Pflicht – die Leistungspflicht des Arbeitnehmers zu konkretisieren, erwächst ein gewisser Entscheidungsspielraum, wie datenschutzfreundlich Arbeitsprozesse gestaltet werden. Die dogmatische Einordnung dieses Spielraums folgt nicht unmittelbar aus den Regelungen der Datenschutz-Grundverordnung. Die Schranken für die Zwecksetzung und die Erforderlichkeitsprüfung verhal- 1535

ten sich zueinander wie kommunizierende Röhren; was das Ergebnis der Prüfung betrifft sind die Ansätze nicht selten austauschbar. Für eine stärkere Betonung der Grenzen der Zwecksetzung spricht aber, dass auf diese Weise das Prinzip der Zweckbindung und die dort vorzunehmende Vereinbarkeitsprüfung gestärkt werden kann. Dies ist umso wichtiger, als die Einordnung eines Zwecks zu den Kategorien Einsichtnahme oder Kontrolle nicht selten über die Zulässigkeit einer Datenverarbeitung entscheidet.

1536 Der Entscheidungsspielraum des Arbeitgebers äußert sich darin, dass er die funktionalen Anforderungen an das Produktions- und Assistenzsystem festlegen kann. Diese Anforderungen sind auch dann zu akzeptieren, wenn sie mittelbar auf die Verarbeitung personenbezogener Daten hinauslaufen. Die Funktionalität ist an dieser Stelle nur abstrakt festzulegen. Die konkrete Umsetzung der aus der geforderten Funktionalität erwachsenden Anforderungen, insbesondere die genaue technische und organisatorische Gestaltung des Systems, unterliegen dagegen einer strengen Erforderlichkeitsprüfung, innerhalb derer kein Raum für Entscheidungsspielräume des Arbeitgebers ist.

1537 Eine Kontrolle der Zwecksetzung selbst ist dem aktuellen Datenschutzrecht fremd. Insbesondere das – ohnehin rechtsfolgenlose – Prinzip der Datensparsamkeit nach § 3a S. 1 BDSG 2003 wurde nicht in die Datenschutz-Grundverordnung übernommen. Die Kontrollinstrumente müssen hier vor allem dem Arbeitsrecht entnommen werden. Was dem Weisungsrecht des Arbeitgebers Grenzen setzt, beschränkt zugleich auch seine datenschutzrechtliche Zwecksetzungsbefugnis. Hierzu zählen grundsätzlich auch die Prinzipien der menschengerechten Gestaltung. Da diese Prinzipien aber selbst nur wenig abwägungsfest ausgestaltet sind, kann dadurch keine wirksame Kontrolle etabliert werden. Der zentrale Prüfungspunkt bleibt darum die abschließende Interessenabwägung im Rahmen der Angemessenheit, in der sämtliche Aspekte – auch die der menschengerechten Gestaltung – einzufließen haben.

1538 Bei der Abwägung ist auch der technische Datenschutz zu beachten. Der Verantwortliche hat die Einhaltung der Vorgaben der Datenschutz-Grundverordnung durch technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik sicherzustellen. Abstriche können hier nur bei einem – durch die Verarbeitung personenbezogener Daten stets induzierten – einfachen Risiko gemacht werden. Wenn die Kosten einer Schutzmaßnahme nach dem Stand der Technik den Nutzen eines Systems in Frage stellen würden, darf der Arbeitgeber hier auch günstigere und weniger wirksame Maßnahmen nach den allgemeinen Regeln der Technik einsetzen. Bei einem hohen Risiko können allerdings keine Abweichun-

gen geduldet werden. Der Verantwortliche muss hier den Stand der Technik einhalten oder von der problematischen Datenverarbeitung Abstand nehmen.

Neben dem Erlaubnistatbestand zur Vertragserfüllung stehen den Beteiligten mit der Kollektivvereinbarung, der Einwilligung und der Generalklausel für berechtigte Interessen noch weitere Instrumente zur Verfügung, über die eine Datenverarbeitung gerechtfertigt werden kann. Hierdurch kann aber nicht wesentlich von den skizzierten Grundsätzen abgewichen werden. In Kollektivvereinbarungen können größtenteils nur konkretisierende Regelungen getroffen werden. Die Einwilligung kann nur wirksam eingeholt werden, wenn die Benutzung des Systems für den Beschäftigten optional erfolgt, und die Generalklausel wird vom Erlaubnistatbestand zur Vertragserfüllung verdrängt, soweit ein unmittelbarer Zusammenhang mit dem Beschäftigungsverhältnis besteht. Für die Anforderungen an die Zulässigkeit der Datenverarbeitung haben sie darum nur eingeschränkte Bedeutung. 1539

3.7.3 Die Zulässigkeit der Datenverarbeitung in typischen Situationen

Da die Zulässigkeit der Datenverarbeitung nicht selten von einer abschließenden Interessenabwägung abhängt, können belastbare Aussagen letztlich nur zu bestimmten typisierten Szenarien getroffen werden. 1540

Dem vorgelagert lassen sich aber einige übergreifende Kriterien formulieren. So hat der Zweck entscheidenden Einfluss auf die Zulässigkeit der Datenverarbeitung. An Kontrollmaßnahmen, die auf arbeitsrechtliche Konsequenzen für den Einzelnen hinauslaufen können, sind besonders strenge Anforderungen zu stellen. Die Einsichtnahme in Daten zur Organisation der betrieblichen Abläufe ist in vielen Fällen dagegen weit weniger problematisch. Die Datenverarbeitung hat darüber hinaus stets transparent zu erfolgen, was grundsätzlich aber auch durch generalisierende Informationen an die Beschäftigten erreicht werden kann. Verdeckte Maßnahmen sind nur als letztes Mittel bei einem konkreten Verdacht einer Verfehlung gerechtfertigt. Schließlich muss jede Datenverarbeitung sowohl im übertragenen als auch im wörtlichen Sinne kontrollfreie Räume zulassen. Sie darf weder örtlich noch funktional als lückenlose Totalüberwachung ausgestaltet sein, da andernfalls ein nicht zu rechtfertigender Überwachungsdruck entstünde. 1541

Eine besonders einschneidende typische Situation stellt die Videoüberwachung dar. Zu Kontrollzwecken ist sie nur ausnahmsweise bei einem kon- 1542

kreten Verdacht einer Verfehlung des Beschäftigten zulässig. Dies betrifft aber im Grunde keine Spezifika der Industrie 4.0. Als Maßnahmen zur Einsichtnahme ist die Verarbeitung personenbezogener Videodaten in der Regel nicht erforderlich; jedenfalls eine längerfristige personenbezogene Speicherung der Aufnahmen wäre unverhältnismäßig.

1543 Standortdaten rangieren in ihrer Sensibilität unterhalb der Videodaten. Für Kontrollzwecke bedarf es aber auch hier eines konkreten Verdachts einer Verfehlung. Eine Datenverarbeitung zur Einsichtnahme lässt sich dagegen bereits mit betrieblichen Bedürfnissen rechtfertigen. Die Erforderlichkeitsprüfung wird hier aber in der Regel ergeben, dass eine nur anlassbezogen durchgeführte Ortung ausreicht. Nur in Ausnahmefällen, etwa wenn es für die Sicherheit der Beschäftigten oder hoher Vermögenswerte erforderlich ist, kann auch eine permanente Ortung zulässig sein.

1544 Der weiteste Spielraum eröffnet sich dem Arbeitgeber bei der Verarbeitung von Betriebsdaten. Sie ist zu Kontrollzwecken nicht zwingend davon abhängig zu machen, dass ein konkreter Verdacht einer Pflichtverletzung gegen den Beschäftigten besteht. Neben stichprobenartigen Kontrollen etwa des Ordnungsverhaltens darf auch das Leistungsverhalten anlassbezogen kontrolliert werden. Damit hierdurch kein übermäßiger Überwachungsdruck entsteht, müssen die Voraussetzungen für eine solche Kontrolle aber transparent niedergelegt sein. Für Maßnahmen zur Einsichtnahme kommt es schließlich maßgeblich auf die Erforderlichkeitsprüfung i.e.S. an, in deren Rahmen auch zumutbare technische und organisatorische Maßnahmen zu berücksichtigen sind. Ist die Datenverarbeitung erforderlich, wird sie in der Regel auch angemessen sein.

1545 Eine Besonderheit stellt die Übermittlung von Daten in Wertschöpfungsnetzwerken dar. Die Datenverarbeitung lässt sich nicht auf die Vertragserfüllung stützen und kann folglich nur mit der Generalklausel der Verarbeitung zur Wahrung berechtigter Interessen gerechtfertigt werden. Entsprechend strenger sind die Anforderungen an die Zulässigkeit zu handhaben. Eine personenbezogene Übermittlung ist hier nur in Ausnahmefällen zulässig, und dies auch nur, wenn die Zweckbindung der Daten auch beim Empfänger sichergestellt ist. In der Regel dürfte es aber zur Zweckerreichung genügen, pseudonymisierte Daten zu übermitteln.

1546 Eine Sonderrolle nehmen weiterhin die automatisierten Entscheidungen ein. Die Datenschutz-Grundverordnung regelt hier nicht den ganzen Verarbeitungsprozess, sondern nur die eigentliche Verwendung der Daten. Für Entscheidungen, die ohne relevantes menschliches Eingreifen und auf der Basis einer automatisierten Bewertung persönlicher Aspekte des Be-

schäftigten getroffen werden, folgen daraus empfindliche Einschränkungen. Angesichts des nicht unerheblichen Risikos und vor allem der Unvereinbarkeit mit den Prinzipien der menschengerechten Gestaltung der Arbeit sind solche automatisierten Entscheidungen unzulässig.