Die Datenschutz-Grundverordnung als demokratisches Level Playing Field?

Stefan Brink, Kira Vogt

Entwicklung des Datenschutzrechts in Europa

Das Sammeln ist ein Urbedürfnis der Menschen. Ebenso ist es ein Urbedürfnis, einmal gesammelte Dinge auch behalten zu wollen, wenn sie nicht getauscht oder verkauft werden. Zu erkennen, dass etwas nicht mehr gebraucht wird und sich davon zu trennen, fällt dagegen schwer. Daher verwundert es nicht, dass auch bei personenbezogenen Daten bislang häufig eine „Hamster-Mentalität" anzutreffen war - und es bis heute ist. Getreu dem Motto „Das könnte noch einmal nützlich werden, behalten wir mal vorsorglich die Daten." legten Einzelpersonen, aber auch Unternehmen und Staaten, eine regelrechte Datensammelwut an den Tag – was sich bitter rächte. Denn vom ungesteuerten Datensammeln bis zur Zweckentfremdung von Daten, die ja ohnehin schon mal da sind, ist es nur ein sehr kurzer Schritt. Der Blick auf dunkle Seiten von Europas Vergangenheit zeigt, wie leicht es ist, Daten für missbräuchliche Zwecke zu verwenden, wenn es keine Gesetze gibt, die dies verhindern. In den Niederlanden war etwa es zu Beginn des letzten Jahrhunderts üblich, ein Register aller Einwohner*innen zu erstellen, in dem unter anderem auch die Religionszugehörigkeit verzeichnet wurde. Als die Nationalsozialisten im zweiten Weltkrieg die Macht übernahmen, fiel es ihnen daher noch leichter als anderswo, Menschen jüdischen Glaubens zu identifizieren, in Konzentrationslager zu stecken und zu ermorden.[1] Vor der Wiederholung der Geschichte bewahrt uns – hoffentlich – auch das Menschenrecht Datenschutz.

Für die Einordnung der EU-Datenschutz-Grundverordnung als demokratisches Level playing field bedarf es zunächst der Betrachtung des Datenschutzes als Menschenrecht. Menschenrechte und Demokratie sind, jedenfalls in der europäischen Geschichte und Rechtstradition untrennbar miteinander verbunden. Nach dem Zweiten Weltkrieg war es zunächst

1 S. *Ehmann*, ZD 2021, 509, Fn. 31 m. w. N.

der Europarat, der in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) das Recht jeder Person auf Achtung des Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz statuierte. Vor der Einführung unionsrechtlicher Datenschutzbestimmungen war es ebenfalls der Europarat, der Anfang der 1980er Jahre mit der Konvention 108 das erste internationale, rechtliche bindende Übereinkommen im Bereich des Datenschutzes erzielte.[2] Daher ist es nicht verwunderlich, dass die ersten europäischen Urteile zum Datenschutz ebenfalls aus Straßburg stammen. Schon 1987 stellte der Europäische Gerichtshof für Menschenrechte fest, dass die Speicherung von Informationen über das Privatleben einer Person durch eine öffentliche Behörde einen Eingriff in das Recht aus Artikel 8 darstellt.[3] Dies gelte, wie er im Jahr 2000 klarstellte, unabhängig davon, ob die gespeicherten Daten später verwendet werden oder nicht.[4]

Während der EGMR den Schutz von Informationen in das Recht auf Privatleben hineinlas und dies bis heute tut, stellte das Bundesverfassungsgericht bereits 1983 neben das Allgemeine Persönlichkeitsrecht, das selbst keine einfachgesetzliche Ausprägung erfahren hatte, ein aus der Allgemeinen Handlungsfreiheit nach Artikel 2 Abs. 1 in Verbindung mit dem Recht auf Menschenwürde aus Artikel 1 Abs. 1 GG abgeleitetes „Recht auf informationelle Selbstbestimmung". Unter den Bedingungen der modernen Datenverarbeitung, so das Bundesverfassungsgericht im *Volkszählungsurteil*, wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten auf verfassungsgesetzlicher Ebene geleistet. Das Grundrecht gewährleiste insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[5]

In der Europäischen Union wurde neben dem Recht auf Privatleben in Artikel 7 der Charta der Grundrechte der Europäischen Union (GRCh) ganz ausdrücklich auch ein Recht auf Datenschutz aufgenommen. Gemäß Artikel 8 GRCh hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Dass der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein Grundrecht ist, betont auch Erwägungsgrund 1 der EU-Datenschutz-Grundverordnung (EU) 2016/679 (DS-GVO), seit dem 25. Mai 2018 geltende Nachfolgerin der Richtli-

2 Übereinkommen Nr. 108 des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981.
3 EGMR, *Leander gegen Schweden*, Urteil vom 26. März 1987, Az. 9248/81 Rn. 48.
4 EGMR, *Amann gegen Schweiz*, Urteil vom 16. Februar 2000 (Große Kammer), Az. 27798/95, Rn. 69.
5 BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83, Rn. 147.

nie 95/46/EG. Dabei verfolgt die DS-GVO umfassend das Ziel der Wahrung von Demokratie und Rechtsstaatlichkeit in einer freiheitlichen Informationsgesellschaft.[6] Gemäß Erwägungsgrund 2 der DS-GVO sollten die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Die Datenschutz-Grundverordnung soll so zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen. Damit schafft die DS-GVO das Fundament für einen viel umfangreicheren digitalen Grundrechtsschutz in Europa, bei dem der Datenschutz mit weiteren Rechtsgebieten verzahnt werden muss.[7] Schon in Artikel 1 Abs. 1 der DS-GVO wird dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten der freie Verkehr solcher Daten an die Seite gestellt. Auch Erwägungsgrund 4 Satz 2 betont, dass das Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht ist; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.

Betroffenenrechte

Der demokratische Ansatz der DS-GVO zeigt sich zuerst in der Ausgestaltung der Betroffenenrechte. Im Vergleich zur Vorgängerin, der Datenschutzrichtlinie, setzt die DS-GVO hier auf noch größere Partizipation der Betroffenen. Die Verfügungsgewalt über die eigenen Daten soll so weit wie möglich bei der betroffenen Person liegen bzw. dieser so schnell wie möglich wieder zurückgegeben werden.

Bester Beleg dafür ist Artikel 15 DS-GVO: Dieser normiert nicht nur, wie der Titel suggeriert, ein Recht auf Auskunft über die verarbeiteten Daten, sondern auch ein Recht auf Kopie. Gemäß Artikel 15 Abs. 1 DS-GVO können betroffene Personen zunächst eine Bestätigung des Verantwortlichen anfordern, ob dieser sie betreffende personenbezogene Daten verar-

6 *Weichert*, vorgänge Nr. 231/232, 147, 152.
7 *Weichert*, vorgänge Nr. 231/232, 147, 156.

beitet. Ist dies der Fall, haben sie ein Recht auf Auskunft über diese Daten und auf weitere Informationen wie die Zwecke, zu denen die Daten verarbeitet werden, und die Empfänger, gegenüber denen die Daten offengelegt worden sind oder zukünftig offengelegt werden. Während die Informationspflichten nach Artikel 13 und 14 DS-GVO Verantwortliche verpflichten, gewisse (abstrakte) Angaben im Zeitpunkt der Datenerhebung zur Verfügung zu stellen, erhalten Betroffene mit Artikel 15 DS-GVO die Möglichkeit, den Weg ihrer personenbezogenen Daten möglichst konkret nachzuvollziehen. Artikel 15 Abs. 3 DS-GVO gewährt zudem ein Recht auf Kopie der verarbeiteten Daten, die häufig auch in elektronischer Form, zum Beispiel zum (geschützten) Download, bereitgestellt werden kann. Mit diesem Anspruch haben Betroffene also das Recht, ihre Daten im Kontext der Verarbeitung zu sehen. Artikel 15 DS-GVO gibt Betroffenen damit den Schlüssel zur Schatztruhe der weiteren Betroffenenrechte in die Hand. Wenngleich alle Betroffenenrechte auch unabhängig voneinander geltend gemacht werden können und Betroffene nicht mit dem Auskunftsrecht starten müssen, ist dies in der Regel der sinnvollste Ausgangspunkt. Mithilfe des Auskunfts- und Kopierechts erhalten Betroffene den notwendigen Überblick zur besseren Einschätzung, ob ihre personenbezogenen Daten richtig sowie zweck- und rechtmäßig verarbeitet werden und ob eine Geltendmachung weiterer Betroffenenrechte sinnvoll erscheint.

Der oben angesprochene Aspekt der informationellen Selbstbestimmung spiegelt sich auch im Recht auf Löschung und Vergessenwerden des Artikels 17 DS-GVO wider. Wo das digital abrufbare Bild einer Person zum Teil wichtiger wird als das reale und wo dieses Bild nicht allein und im Laufe der Zeit sogar immer weniger von der betroffenen Person selbst bestimmt wird, soll Betroffenen damit das Bestimmungsrecht so weit wie möglich zurückgegeben werden.[8] In der Informationstechnologie herrschte lange die Auffassung vor, ein bestmöglicher Schutz vor Angriffen könne nur erreicht werden, wenn Daten weitestmöglich vor Zugriffen und Zerstörung geschützt würden. Dies führte dazu, dass etliche IT-Systeme gar nicht darauf ausgelegt waren, einzelne Datenfelder, aber auch ganze Datengruppen eines bestimmten Alters wieder zu löschen. Erst neuerdings setzt sich die Erkenntnis durch, dass Daten dann am besten vor Angriffen geschützt sind, wenn sie nicht mehr vorhanden sind. Bei Verzahnung der Grundsätze der Zweckbindung, Datenminimierung und Speicherbegrenzung (Artikel 5 Abs. 1 lit. b, c und d DS-GVO) ergibt sich genau dieses

8 S. BeckOK Datenschutzrecht, Wolff/Brink-*Worms*, 37. Edition vom 01.08.2021, Art. 17 Rn. 2.

Bild: Personenbezogene Daten dürfen nur, soweit für festgelegte Zwecke erforderlich, verarbeitet werden und grundsätzlich auch nur für diese Zeit in einer Form gespeichert werden, welche die Identifizierbarkeit der Betroffenen ermöglicht. Das Recht auf Löschung ergänzt diese Prinzipien, indem Betroffene die Löschung zusätzlich aktiv einfordern können. Erwägungsgrund 65 berücksichtigt dabei die hohe Schutzbedürftigkeit von Kindern und betont in Satz 3 das Recht auf Löschung insbesondere in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten – insbesondere die im Internet gespeicherten – später löschen möchte. Daher sollten Betroffene nach Satz 4 das Recht auch noch ausüben können, wenn sie keine Kinder mehr sind.

Neben dieser Rücksichtnahme auf besonders vulnerable Personen einerseits erkennt die DS-GVO andererseits auch, dass das Individuum nicht in jedem Fall im Vordergrund stehen sollte. Für den Erhalt einer Demokratie ist es unerlässlich, relevantes Wissen für die nachkommenden Generationen zu bewahren. Daher enthält die DS-GVO an mehreren Stellen Ausnahmen für (ausschließlich) im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke. Das Prinzip der Speicherbegrenzung nach Artikel 5 Abs. 1 lit. e DS-GVO gestattet für diese Fälle ein längeres Vorhalten personenbezogener Daten, sodass gemäß Artikel 17 Abs. 3 lit. d DS-GVO von der unverzüglichen Löschpflicht abgewichen werden. Selbstverständlich unterliegt die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person, wie Artikel 89 DS-GVO klarstellt. Eine solche Weiterverarbeitung personenbezogener Daten erfolgt nach Erwägungsgrund 156 Satz 3 erst dann, wenn der Verantwortliche geprüft hat, ob es möglich ist, diese Zwecke durch die Verarbeitung von personenbezogenen Daten, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, zu erfüllen, sofern geeignete Garantien bestehen. Als Öffnungsklausel gestattet Artikel 89 DS-GVO den Mitgliedstaaten die genauere Ausgestaltung. Von der Möglichkeit, die Betroffenenrechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung und Widerspruch zu beschränken, hat der deutsche Gesetzgeber für Forschungs- oder Statistikzwecke in § 27 Abs. 2 Bundesdatenschutzgesetz (BDSG) Gebrauch gemacht, jedoch nur unter der Bedingung, dass diese Rechte voraussichtlich die Verwirklichung Zwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Zweckerfüllung notwendig ist. Eine

entsprechende Regelung für die Beschränkung der Rechte auf Einschränkung der Verarbeitung und Widerspruch im Falle im öffentlichen Interesse liegender Archivzwecke findet sich in § 28 Abs. 4 BDSG. Die datenschutzrechtlichen Normen schaffen so eine Balance zwischen Individualrechtsschutz und dem Schutz von Kollektivgütern.

Artikel 20 DSGVO normiert darüber hinaus das Recht auf Datenübertragbarkeit. Danach hat die betroffene Person das Recht, sie betreffende personenbezogene Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format (zurück) zu erhalten, um diese Daten einem anderen Verantwortlichen ohne Behinderung durch den ersten Verantwortlichen zu übermitteln. Allerdings gilt dies nur bei automatisierten Verarbeitungen, deren Rechtsgrundlage eine Einwilligung oder ein Vertrag bildet. Wie Erwägungsgrund 68 erläutert, sollen Betroffene bei Verarbeitungen mit automatischen Mitteln so eine bessere Kontrolle über ihre Daten erhalten.

Absatz 2 sieht noch eine weitere Erleichterung vor. Danach kann die betroffene Person erwirken, dass die personenbezogenen Daten direkt von einem an den anderen Verantwortlichen übermittelt werden. Die großzügige Einschränkung „soweit dies technisch machbar ist", trägt jedoch leider dazu bei, dass Datenübertragbarkeit in der Praxis noch nicht weit verbreitet ist – schließlich sollen Verantwortliche nach Erwägungsgrund 68 Satz 2 lediglich dazu „aufgefordert werden", interoperable Formate zur Ermöglichung der Datenübertragbarkeit zu entwickeln. Hier wäre es hilfreich, schon die Hersteller in die Pflicht zu nehmen, um schnellere Fortschritte bei der Datenübertragbarkeit zu erreichen.

Durch dergestalt differenzierte und effektive Datenschutzrechte lässt die DS-GVO das angestrebte demokratische level playing field entstehen.

Verantwortlicher

Ein demokratisches level playing field setzt aber nicht nur differenzierte Betroffenenrechte voraus. Es kann nur effektiv werden, wenn es auf der Gegenseite auch die Verantwortlichen für die Datenverarbeitung in die Pflicht nimmt.

Genau das tut die DS-GVO in überzeugender Weise: Nach Artikel 5 Abs. 2 der EU-Datenschutz-Grundverordnung unterliegen verantwortliche Stellen, die personenbezogene Daten verarbeiten, einer Rechenschaftspflicht. Das bedeutet, dass sie jederzeit nachweisen können müssen, die Verordnung einzuhalten. Verantwortliche müssen sich also rechtfertigen können: Sie dürfen die Daten nur verarbeiten, wenn sie dafür eine Rechts-

grundlage haben (Grundsatz der Rechtmäßigkeit). Außerdem dürfen sie personenbezogene Daten grundsätzlich nur für den vorgesehenen Zweck verwenden (Grundsatz der Zweckbindung). Nach Artikel 4 Nr. 7 DS-GVO ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Begriff des Verantwortlichen ist dabei weit zu verstehen – auch dieses Verständnis ist wesentliche Grundlage für die Effektivität des Schutzes der Betroffenen. Laut Europäischem Gerichtshof ist zum Beispiel auch ein Petitionsausschuss insoweit als Verantwortlicher im Sinne der DS-GVO einzustufen, als er allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet.[9] Ein Betroffener hatte eine Petition beim Petitionsausschuss des Hessischen Landtags eingereicht und anschließend ein Auskunftsersuchen nach Artikel 15 DSGVO gestellt. Der Landtagspräsident lehnte den Auskunftsantrag mit der Begründung ab, dass das Petitionsverfahren eine parlamentarische Aufgabe sei und das betreffende Parlament nicht in den Anwendungsbereich der Verordnung 2016/679 falle.[10] Dabei ließ der EuGH offen, ob der Petitionsausschuss als „Behörde" oder „andere Stelle" im Sinne der Definition des Begriffs „Verantwortlicher" in Artikel 4 Nr. 7 DS-GVO anzusehen ist[11] – der Rechenschaftspflicht über die Einhaltung des Datenschutzes unterliegt der Petitionsausschuss in jedem Fall.

Grundsätzlich zielt die DS-GVO auf eine Gleichbehandlung aller verantwortlichen Stellen ab. Nur zum Teil sieht sie Erleichterungen für bestimmte Verantwortliche wie kleinere Unternehmen vor. Diese wirken sich in der Praxis jedoch nur zum kleinen Teil wirklich erleichternd aus. Nach Artikel 30 Abs. 5 DSGVO müssen die Verzeichnisse der Verarbeitungstätigkeiten nicht von Unternehmen oder Einrichtungen geführt werden, die weniger als 250 Personen beschäftigen – es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Abs. 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10. Vor allem die Rückausnahme der „nicht nur gelegentlich[en]" Verarbeitung

9 EuGH, Urteil vom 9. Juli 2020, Rs. C-272/19, Rn. 74.
10 EuGH, Urteil vom 9. Juli 2020, Rs. C-272/19, Rn. 19.
11 S. EuGH, Urteil vom 9. Juli 2020, Rs. C-272/19, Rn. 65, 73.

führt dazu, dass kleinere Unternehmen einen dem der großen nicht unähnlichen Aufwand betreiben müssen.

Ein demokratisches level playing field wird so geschaffen – ob dies immer auf verhältnismäßige Weise gelingt, sei dahingestellt.

Fehlende Herstellerhaftung

Um ein echtes „level playing field" darstellen zu können, fehlt es der Datenschutz-Grundverordnung derzeit daher noch an einer entscheidenden Voraussetzung: der Haftung nicht nur für die personenbezogene Daten verarbeitenden Verantwortlichen und Auftragsverarbeitern, sondern auch für diejenigen, die Datenverarbeitungsprogramme herstellen. Die in der DS-GVO aufgestellten Grundsätze *Data protection by design and default* sind derzeit nur dann ausreichend erfüllbar, wenn Unternehmen zum Beispiel bei der Erstellung eines Online-Formulars selbst entscheiden können, welche personenbezogenen Daten sie wirklich benötigen und eben auch nur diese abfragen bzw. abfragen lassen – oder jedenfalls eine Differenzierung zwischen Pflicht- und freiwilligen Datenfeldern nutzen. Möchte das verantwortliche Unternehmen dagegen Daten mithilfe eines altbekannten Programms oder auch einer neuen App erfassen, sind seine Möglichkeiten der Implementierung dieser Grundsätze wesentlich begrenzter. In Deutschland wird zwar zum Teil eine datenschutzrechtliche Herstellerbindung über den Umweg der deliktischen Produzentenhaftung § 823 Abs. 1 BGB erwogen: Wenngleich danach keine unmittelbare Pflicht bestehe, ein Produkt bereits in der Planungsphase datenschutzkonform auszugestalten, ließe sich eine den Grenzen der Zumutbarkeit unterliegende Herstellerpflicht begründen, nur solche Produkte in den Verkehr zu bringen, die datenschutzkonform nutzbar sind.[12] Solange aber nicht die DS-GVO den Datenschutz-Aufsichtsbehörden die Möglichkeit gibt, mithilfe (der Androhung) abschreckender Bußgelder und anderer Maßnahmen Herstellende in die Pflicht zu nehmen, wird sich dies weiterhin negativ auf die Schlagkraft des Datenschutzes auswirken.

12 *Specht-Riemenschneider*, MMR 2020, 73, 77.

Modell DS-GVO

In nicht wenigen Ländern dieser Erde ist das zu Beginn erwähnte umfassende Datensammeln bis heute anzutreffen – allen voran in China mit seinem Sozialkreditsystem. Dort führt unerwünschtes bis straffälliges Verhalten zu Punktabzug, während erwünschtes Verhalten den Punktestand erhöht. Dazu werden jedwede Daten verwendet, auf welche die Regierung durch Videoüberwachung mit Gesichtserkennung oder Analyse von Internetnutzungsverhalten dank Übermittlung der Daten durch chinesische Internetriesen zugreifen kann.[13]

Der Blick über die Grenzen Europas hinaus zeigt aber auch, dass demokratische Ansätze nicht nur datenschutzrechtlichen Parlamentsgesetzen inhärent sein können. So findet der California Consumer Privacy Act (CCPA) seinen Ursprung sogar in einer basisdemokratischen Volksabstimmung.[14]

Die Vorteile einer Stärkung des Datenschutzes haben auch andere Länder erkannt. Darauf reagiert auch die DS-GVO, indem sie vergleichbares Datenschutzniveau weltweit anerkennt. Nach Angemessenheitsbeschlüssen für Argentinien, Japan, Kanada und weitere Staaten[15] hat die EU-Kommission im Sommer 2021 das Verfahren zur Annahme des Angemessenheitsbeschlusses für die Republik Korea eingeleitet.[16] Mit den Angemessenheitsbeschlüssen soll nach Artikel 45 der DS-GVO in den jeweiligen Staaten ein mit dem der EU vergleichbares Schutzniveau für personenbezogene Daten aus der Europäischen Union bescheinigt werden. Die endgültige Überprüfung solcher Beschlüsse obliegt dem Europäischen Gerichtshof. Mit den Urteilen gegen das Safe-Harbor-Abkommen[17] und das EU/US-Privacy-Shield[18] hat dieser bereits zwei Angemessenheits-beschlüsse für die USA gekippt. Dennoch stellen Angemessenheitsbeschlüsse aus Sicht der Datenexporteure und -importeure die einfachste Möglichkeit der Datenübermittlung dar. In derartigen Fällen dürfen personenbezogene Da-

13 *Wagner*, ZD 2020, 140, 141.
14 *Botta*, DSRITB 2019, 657, 660.
15 Die Liste der Drittländer mit Angemessenheitsbeschlüssen veröffentlicht die EU-Kommission unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de.
16 S. Pressemitteilung der Europäischen Kommission vom 16. Juni 2021, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/ip_21_2964.
17 EuGH, Urteil vom 6. Oktober 2015, Rs. C-362/14 (*Schrems I*).
18 EuGH, Urteil vom 16. Juli 2020, Rs. C-311/18 (*Schrems II*).

ten nämlich, wie Erwägungsgrund 103 Satz 2 erläutert, ohne weitere Genehmigung aus Europa an dieses Land übermittelt werden.

Nicht zuletzt aufgrund des Erlasses neuer Datenschutzgesetze, die zu großen Teilen als Abbild der DS-GVO modelliert sind, sowie der Einrichtung neuer Datenschutz-Aufsichtsbehörden zählen dadurch immer mehr Staaten zu den sogenannten „sicheren Drittländern" – und erweitern das menschenrechtliche level playing field.

Fazit

Die DS-GVO erschafft ein demokratisches level playing field, indem sie alle betroffenen Bürgerinnen und Bürger mit differenzierten Rechten hinsichtlich ihrer personenbezogenen Daten ausstattet, gleichzeitig die Verantwortlichen (mit Ausnahme der Hersteller) effektiv in die Pflicht nimmt und ihre Wirkung auch im außereuropäischen Bereich entfaltet. Auch wenn die DS-GVO dabei durchaus als Modell dienen kann, wird sie in den kommenden Jahren der Weiterentwicklung bedürfen, um mit dem digitalen Fortschritt mithalten zu können.