provet

Projektgruppe verfassungsverträgliche Technikgestaltung

Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht

---

Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V. (vzbv)

Verantwortlicher:

Univ.-Prof. Dr. jur. Alexander Roßnagel

Durchführende:

Univ.-Prof. Dr. jur. Alexander Roßnagel

Dr. jur. Christian Geminn

Kassel, den 26. November 2019

Kurzdarstellung

Die Datenschutz-Grundverordnung hat die Stellung von Verbrauchern bei der Verarbeitung personenbezogener Daten an vielen Stellen verbessert. Hier sind unter anderem das Aufenthaltsprinzip, das Recht auf Datenübertragung, die Verpflichtung zum Datenschutz durch Systemgestaltung, das Beschwerderecht und die Sanktionierung von Verstößen zu nennen.

Dennoch bleibt sie hinter ihren Möglichkeiten zurück. Einerseits hat die Grundverordnung eine erhebliche Rechtsunsicherheit geschaffen, die sich zumeist zuungunsten der Verbraucher auswirkt. Diese Unsicherheit resultiert überwiegend daraus, dass die Grundverordnung zu abstrakt bleibt und klarstellende Präzisierungen unterlässt – sowohl was ihr Verständnis als auch was ihre praktische Umsetzung betrifft. Dies verleitet Anbieter dazu, die vorhandenen Auslegungsspielräume zu Ungunsten von Verbrauchern zu nutzen. Andererseits konnten sich bestimmte verbraucherfreundliche Regelungen bei der Entstehung der Grundverordnung schlicht nicht durchsetzen. Dies betrifft etwa das Scoring. Beides behindert die Innovationen, die die Datenschutz-Grundverordnung 2018 in die europäische Datenschutzpraxis einführen wollte. Sie können ihre verbraucherschützenden Potentiale nicht entfalten.

Dieses Gutachten zeigt, dass Probleme auf zwei Ebenen bestehen. Zunächst sind Probleme zu nennen, die auf Mängeln im Normtext beruhen. Hier schlägt das Gutachten 28 Formulierungen vor, um den Text der Datenschutz-Grundverordnung aus Verbrauchersicht zu verbessern. Darüber hinaus bestehen aber auch konzeptionelle Probleme, die nicht mit kleineren Eingriffen in den Normtext beseitigt werden können. Auch hierzu formuliert das Gutachten Lösungsansätze, deren Umsetzung weiter in die Zukunft gerichtet ist.

Die Evaluation der Datenschutz-Grundverordnung, die für das Jahr 2020 vorgesehen ist, bietet die ideale Gelegenheit, den Unionsgesetzgeber auf die genannten Defizite hinzuweisen, und Vorschläge vorzustellen, die Verordnung konstruktiv weiterzuentwickeln. Ziel muss es dabei sein, das Machtgefälle zwischen Anbietern und Verbrauchern zu reduzieren. Dies wird erreicht, indem in der Grundverordnung angelegte Innovationen besser zur Geltung gebracht werden.

Der Erfolg der verbraucherfreundlichen Innovationen der Datenschutz-Grundverordnung darf nicht allein von der Auslegung des geltenden Normtextes aus dem Jahr 2016 abhängen. Es sind vielmehr Präzisierungen vorzunehmen, die grundrechtsfreundlichere Regelungen direkt im Wortlaut der jeweiligen Normen verankern und Rechte der Verbraucher und Pflichten der Verantwortlichen eindeutiger fassen. Bereits kleine Veränderungen des Textes können die notwendige Präzisierung erreichen oder zumindest die Bestimmtheit der Regelung deutlich steigern und eine erheblich die Verbraucher stärkende Wirkung entfalten. Dort, wo dies nicht der Fall ist, müssen anstelle des Unionsgesetzgebers, die Gesetzgeber der Mitgliedstaaten, der Europäische Datenschutzausschuss und die nationalen Datenschutzaufsichtsbehörden tätig werden Gesetze oder Leitlinien erlassen. Auch hierzu bietet das Gutachten Anregungen.

Konkret schlägt das Gutachten die folgenden Überarbeitungen der Datenschutz-Grundverordnung vor, wobei die Reihung der Vorschläge keine Priorisierung bestimmter Vorschläge indiziert:

Ausübung persönlicher oder familiärer Tätigkeiten:

- Rücknahme der vollständigen Ausnahme von invasiver Datenverarbeitung aus dem Anwendungsbereich der Datenschutz-Grundverordnung in Art. 2 Abs. 2 lit. c DSGVO; stattdessen risikoadäquate Differenzierung auch bei persönlichen und familiären Tätigkeiten; vollständige Ausnahme aus dem Anwendungsbereich nur bei geringen Risiken; bei erhöhten Risiken teilweise Anwendung ausgewählter Regelungen der Datenschutz-Grundverordnung.

Aufenthaltsprinzip:

- Ausweitung des räumlichen Anwendungsbereichs der Datenschutz-Grundverordnung auf jede Form der Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Europäischen Union aufhalten.

Grundsätze der Datenverarbeitung:

- Anpassung der deutschen Sprachfassung der Datenschutz-Grundverordnung: Ersetzung des Begriffspaars „Treu und Glauben“ in Art. 5 Abs. 1 lit. a DSGVO durch den Begriff „Fairness“.
- Ergänzung der Datenschutz-Grundverordnung um ein Gebot der Datenvermeidung in Art. 5 Abs. 1 lit. c DSGVO.
- Modernisierung und risikoadäquate Weiterentwicklung der Grundsätze der Datenverarbeitung.

Verhältnis zwischen Einwilligung und anderen Erlaubnistatbeständen:

- Klarstellung in Art. 6 Abs. 1 UAbs. 1 DSGVO, dass ein Verantwortlicher sich neben einer Einwilligung nicht zusätzlich auf einen anderen gesetzlichen Erlaubnistatbestand berufen kann.

Profiling:

- Eigenständiger Erlaubnistatbestand für Profiling, das im Grundsatz unzulässig und nur in definierten Ausnahmefällen möglich sein soll.

Verarbeitung der Daten von Kindern:

- Berücksichtigung der besonderen Schutzinteressen bei der Prüfung der Vereinbarkeit eines neuen Verarbeitungszwecks mit dem bisherigen Verarbeitungszweck, wenn die Daten eines Kindes für einen anderen Zweck verwendet werden sollen.
- Übernahme von Erwägungsgrund 38 Satz 2 DSGVO in den Normtext, die Daten von Kindern nicht für Werbezwecke und Profiling zu verwenden.
- Ausschluss der Einwilligung eines Kindes in die Verarbeitung besonderer Kategorien von personenbezogenen Daten nach Art. 9 Abs. 2 lit. a DSGVO.

- Besondere Berücksichtigung der Tatsache, dass personenbezogene Daten im Kindesalter erhoben worden sind, beim Recht auf Widerspruch.
- Ausnahme der Einwilligung eines Kindes in die Verarbeitung personenbezogener Daten zur automatisierten Entscheidung.
- Aufnahme einer Verpflichtung zu besonderer Berücksichtigung der Grundrechte und Interessen von Kindern bei der Risikoanalyse und bei der Festlegung von Schutzmaßnahmen in der Datenschutz-Folgenabschätzung.

Bestimmung des Vertragszwecks:

- Präzisierung des Erlaubnistatbestandes von Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO: objektive (funktionale) Bestimmung der zur Erfüllung eines Vertrages notwendigen Verarbeitung personenbezogener Daten unabhängig von der Vertragsformulierung.

Informationspräsentation:

- Ergänzung der Datenschutz-Grundverordnung um bereichs-/technologiespezifische Regelungen zur Informationspräsentation im Kontext spezieller Anwendungsbereiche und Technologien.
- Situations-, interessen- und entscheidungsgerechte Informationspräsentation
- Beschränkung der Informationen auf die tatsächlichen Umstände der jeweils anstehenden Verarbeitung.

Informationspflichten des Verantwortlichen:

- Ergänzung einer Grundregel zur Auflösung des Konflikts zwischen Informationsanspruch und Geheimnisschutz: Bereitstellung eines möglichst hohen Maßes an Information unter gleichzeitiger Wahrung von Geschäftsgeheimnissen und geistigem Eigentum; Verpflichtung zu einem Maximum an Information.
- Klarstellung, dass die Information über die Tragweite auch die rechtlichen und tatsächlichen Auswirkungen auf die betroffene Person umfasst.
- Klarstellung, dass Information über die „involvierte Logik“ auch die Kriterien für die Entscheidung und ihre Gewichtung umfassen müssen.
- Klarstellung, dass eine Arbeitsteilung im Kontext automatisierter Entscheidungen im Einzelfall nicht zu einem Unterbleiben oder einer Verkürzung der Information führen darf; Informationspflicht bei arbeitsteiligen automatisierten Entscheidungsverfahren jedes Kooperationspartners über seinen Anteil am Verfahren samt den Schnittstellen zu allen anderen Anteilen.
- Ergänzung um eine Informationspflicht bei jedem Profiling, auch wenn dieses nicht unmittelbar mit einer automatisierten Entscheidung verbunden ist, sondern für andere Bewertungszwecke verwendet wird.

Das Auskunftsrecht der betroffenen Person:

- Verpflichtung des Verantwortlichen zur Protokollierung aller Empfänger personenbezogener Daten; Pflicht zur Bekanntgabe des Protokolls gegenüber der betroffenen Person.
- Verpflichtung des Verantwortlichen zu einer gesonderten Information für jedes Profiling, dessen Umfang, Inhalt, Zielsetzung und Verwendungszweck.
- Präzisierung des Rechts auf Kopie; Ergänzung einer Pflicht zur Mitteilung aller verarbeiteten Daten, wenn keine Kopie zur Verfügung gestellt werden kann.

Das Recht auf Datenübertragung:

- Ersetzung des Titels der Vorschrift, der nicht nur eine Möglichkeit, sondern die Handlung, die der Verbraucher fordern kann und zu der der Verantwortliche verpflichtet ist: Recht auf Datenübertragung.
- Ausweitung des Rechts auf Datenübertragung auf die von der betroffenen Person verursachten Daten.
- Festlegung der Übertragung der Daten in einem interoperablen Format und in deutscher (oder der jeweiligen Landessprache des Mitgliedstaates) oder englischer Sprache.

Automatisierte Entscheidungen im Einzelfall:

- Streichung der Einschränkung „ausschließlich".
- Ergänzung um ein Verbot, automatisiert vorbereiteten Entscheidungen ausgeliefert zu sein, die der menschliche Entscheider im Regelfall unbesehen übernimmt, ohne dass die betroffene Person eine Möglichkeit hat, vor der Entscheidung ihren Standpunkt vorzutragen.
- Streichung der Einschränkung, dass die Entscheidung der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie „in ähnlicher Weise erheblich" beeinträchtigt; benachteiligende Beeinträchtigung soll ausreichen.
- Streichung von Art. 22 Abs. 2 lit. a DSGVO. Die Einwilligung der betroffenen Person nach Art. 22 Abs. 2 lit. c DSGVO genügt.
- Aufnahme von qualitativen Anforderungen an eine auf einer automatisierten Verarbeitung beruhende Entscheidung gemäß Erwägungsgrund 71 DSGVO und dem Vorbild von § 31 BDSG.
- Ergänzung von Art. 22 Abs. 3 DSGVO um die Wendung „und die Erläuterung der Entscheidungsgründe".

Datenschutz durch Systemgestaltung:

- Aufnahme einer Verpflichtung zu besonderem Schutz der Grundrechte und Interessen von Kindern.

- Technologie- oder bereichsspezifische Konkretisierung der Verpflichtung zur Systemgestaltung durch den Europäischen Datenschutzausschuss.
- Ausweitung der Verpflichtung auf die Hersteller von datenverarbeitenden Systemen.

Datenschutz durch Voreinstellungen:

- Beschränkung des Zwecks auf die Funktionalität des jeweiligen Dienstes.
- Ergänzung um das Prinzip der Datenvermeidung.
- Aufnahme einer Verpflichtung zu besonderem Schutz der Grundrechte und Interessen von Kindern

Zu den Sanktionen:

- Präzisierung der Bußgeldtatbestände durch eine Leitlinie des Ausschusses nach Art. 70 Abs. 1 Satz 2 lit. k DSGVO; Präzisierung durch unverbindliche Bußgeldkataloge der mitgliedstaatlichen Aufsichtsbehörden.
- Verpflichtung der Aufsichtsbehörden zur Veröffentlichung einer jährlichen Statistik zu ihrer Bußgeldpraxis.

Das Datenschutzrecht regelt eine Rechtmaterie, die stark durch immer wieder neue Geschäftsmodelle und den dynamischen Fortschritt der Informationstechnik herausgefordert wird. Die Datenschutz-Grundverordnung kann deshalb nicht der Endpunkt der Diskussion um die konzeptionelle Ausformung des Datenschutzrechts sein. Vielmehr zeichnen sich bereits jetzt Entwicklungen ab, die das aktuelle Datenschutzrecht schlicht überfordern. Dies liegt zum einen daran, dass die Datenschutz-Grundverordnung die zentralen Konzepte des Datenschutzrechts, die in den 1970er Jahren entwickelt worden sind, im Wesentlichen übernommen hat. Zum anderen ist es darauf zurückzuführen, dass der Unionsgesetzgeber es abgelehnt hat, risikospezifische Grundregeln zu erlassen, die den größten Gefährdungen der Grundrechte durch moderne Informationstechnikanwendungen gerecht werden. Das Gutachten bietet zu diesen Grundfragen des Datenschutzrechts Denkanstöße und skizziert Lösungsansätze, die bezogen auf die Risiken dieser Herausforderungen Benachteiligungen von Verbrauchern verhindern sollen.

Executive Summary

The GDPR has improved the standing of consumers regarding the processing of personal data in many places. Examples are the residence principle, the right to data portability, data protection by design, the right to lodge a complaint and the sanctioning of violations.

Yet, it does not realise its full potential. On the one hand, the GDPR has created significant legal uncertainty, which often affects consumers adversely. This uncertainty results mostly from the fact that the GDPR remains abstract and omits clarifying specifications – both concerning its understanding and its practical implementation. This entices providers to use the existing room for manoeuvre to the disadvantage of consumers. On the other hand, certain consumer-friendly provisions simply were unsuccessful during the creation of the GDPR. This concerns for instance scoring. Both hinder the innovations that the GDPR aimed to introduce 2018 into the European data protection practice. They are unable to unfold their potentials when it comes to protecting consumers.

This report shows that issues exist on two levels. First, there are issues that result from deficits in the text of the regulation. Here, the report suggests 28 alterations of the text in order to improve it – from the point of view of consumers. Beyond that, there are conceptional issues that cannot be resolved with smaller alterations of the text of the norm. The report formulates approaches to these issues whose implementation is directed more towards the future.

The evaluation of the GDPR that is scheduled for the year 2020 presents the ideal opportunity to point out these issues to union lawmakers and to present proposals that constructively evolve the GDPR. The goal must be to reduce the power gradient between providers and consumers. This goal is achieved by better bringing to bear the innovations that are laid out already in the GDPR.

The success of the consumer-friendly innovations of the GDPR must not solely depend on the interpretation of the applicable text from 2016. Instead there need to be specifications that anchor provisions that are more friendly to fundamental right and that frame the rights of consumers and the obligations of controllers more clearly directly in text of the relevant articles of the GDPR. Even small changes of the text can achieve the necessary specifications or at least significantly increase the clarity of existing provisions and strengthen the position of consumers. Where this is not the case, instead of the union lawmakers, the lawmakers of the member states, the European Data Protection Board and the national data protection authorities need to enact laws or guidelines. The report contains proposals regarding this as well.

In particular, the report proposes the following revisions of the GDPR:

Processing in the course of a purely personal or household activity:

- Retraction of the complete exemption of invasive data processing from the material scope of the GDPR in Art. 2(2)(c); instead risk-adequate differentiation also in the context of personal or household activity; complete exemption from the material scope only for low-risk processing; for heightened risks application of select provisions of the GDPR.

Residence principle:

- Expansion of the territorial scope of the GDPR to include every type of processing of personal data of data subjects that reside in the European Union.

Principles relating to processing of personal data:

- Adjustment of the German language version of the GDPR: Replacing the term "Treu und Glauben" in Art. 5(1)(a) with "Fairness".
- Amendment of the GDPR with an obligation to data avoidance in Art. 5(1)(c).
- Modernising and risk-adequate evolution of the principles.

Relations between consent and other grounds for lawful processing:

- Clarification in Art. 6(1)(1) GDPR that a controller in addition to consent cannot rely on another ground for lawful processing.

Profiling:

- Separate provisions on lawfulness regarding profiling, which shall be unlawful by default and only possible in pre-defined exceptions.

Processing of data of children:

- Consideration of the special protection that children merit when assessing the compatibility of a new purpose with the initial purpose, if the data of a child are to be used for another purpose.
- Transfer of recital 38(2) GDPR to the articles, prohibiting the use of personal data of children for the purposes of marketing or profiling.
- Exclusion of the consent of a child from the processing of special categories of personal data according to Art. 9(2)(a) GDPR.
- Special consideration of the fact that personal data has been obtained during childhood in the right to object.
- Exclusion of the consent of a child to the processing of personal data for automated individual decision-making.
- Incorporation of an obligation to special consideration of the fundamental rights and interests of children in the context of risk analysis and when determining measures for protection during a data protection impact assessment.

Determining the purpose of a contract:

- Specification of Art. 6(1)(1)(b) GDPR: objective (functional) specification of the processing of personal data that is necessary to fulfil a contract independently from the phrasing of the contract.

Presenting information:

- Addition of sector specific or technology specific provisions regarding the presentation of information in the context of specific fields of processing and technologies.
- Presentation of information that is adequate to the situation, the interests and the decisions involved.
- Limitation of information to the actual circumstances of the respective processing that is about to occur.

Information to be provided by the controller:

- Addition of a basic rule to resolve the conflict between the right to access and the protection of trade secrets: provision of the highest amount of information possible while protecting trade secrets and intellectual property; obligation to provide a maximum of information.
- Clarification that information on the "logic involved" entails the criteria for the decision and their balancing.
- Clarification that a division of labour or cooperation in the context of automated individual decision-making must not lead to an omission or limitation of information to be provided to the data subject; obligation to inform about divided / cooperative automated decision processes that has to be met by every cooperating partner concerning his or her contribution to the process including the interfaces to all other contributions.
- Addition of an obligation to provide information for every profiling, even if it is not directly linked to an automated individual decision but is instead used for other assessment purposes.

Right of access by the data subject:

- Obligation of the controller to log all recipients of personal data; obligation to present the log to the data subject.
- Obligation of the controller to separately inform the data subject of any profiling, its extent, contents, goals and purposes.
- Specification of the right to be provided with a copy; addition of an obligation to communicate all processed data wherever no copy can be provided.

Right to data portability:

- Rephrasing the title of the norm in a way that not only presents a possibility, but the action that the consumer may demand and that the controller is obligated to perform: "Recht auf Datenübertragung" / "right to data transfer".
- Expansion of the right to data transfer to the data caused by the data subject.
- Stipulation of the transfer of data in an interoperable format and in German (or the respective language of the member state) or in English.

Automated individual decision-making:

- Deletion of the limitation “solely”.
- Addition of a prohibition to be subjected to automatically prepared decisions that the human decider adopts without review and without giving the data subject the opportunity to present his or her point of view prior to the decision.
- Deletion of the limitation that the decision must produce legal effects concerning the data subject or “similarly significantly affects him or her”; a detrimental effect shall be sufficient.
- Deletion of Art. 22(2)(a) GDPR. The consent of the data subject according to Art. 22(2)(c) shall be sufficient.
- Addition of qualitative requirements for a decision that is based on an automatically prepared decision in the image of § 31 of the German Federal Data Protection Act.
- Amendment of Art. 22(3) GDPR with the phrase “to clarification of the reasons for the decision”.

Data protection by design:

- Addition of an obligation to award special protection to the fundamental rights and interests of children.
- Technologically specific or sector-specific specification of the obligation of data protection by design by the Board.
- Expansion of the obligation to producers/manufacturers of systems that process personal data.

Data protection by default:

- Limitation of the purpose to the functionality of the respective service.
- Amendment of the principle of data avoidance.
- Addition of an obligation to award special protection to the fundamental rights and interests of children.

Regarding administrative fines:

- Specification of the provisions on administrative fines through guidelines issued by the Board in accordance with Art. 70(1)(2)(k) GDPR; specification through non-binding catalogues on fines by the data protection authorities of the member states.
- Obligation of the data protection authorities to publish an annual statistic on the issuing of fines.

Data protection law governs a field of law that is challenged constantly and profoundly by emerging business models and the dynamic evolution of information technology. Therefore,

the GDPR cannot be the final act in the discussion on the structural foundation and implementation of data protection law. Rather, developments are on the horizon that simply overstrain the current data protection law. The reason for this is on the one hand that the GDPR in essence maintains the fundamental concepts of data protection law that were developed in the 1970s. On the other hand, it results from the refusal of the union lawmakers to enact technologically specific basic rules that do justice to the biggest threats to fundamental rights caused by modern information technology. The report offers food for thought regarding these fundamental questions and outlines approaches that prevent disadvantages for consumers in the context of the risks that emerge from these challenges.

Inhaltsverzeichnis

1. Einführung

Am 24. Mai 2016 trat nach mehr als vierjähriger Verhandlung die 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 (Datenschutz-Grundverordnung – DSGVO)[1] in Kraft. Nach Ablauf einer zweijährigen Übergangsfrist ist sie seit dem 25. Mai 2018 in allen EU-Mitgliedsstaaten unmittelbar anwendbar. Seitdem wird die Datenschutz-Grundverordnung in der Praxis der Datenverarbeitung personenbezogener Daten angewendet.

Nach Art. 97 DSGVO soll bereits zwei Jahre später eine erste Evaluation dieses Normenwerks vorliegen. Bis zum 25. Mai 2020 soll die Europäische Kommission einen Bericht über die Bewertung und Überprüfung der Datenschutz-Grundverordnung veröffentlichen. Danach sollen Evaluationen alle vier Jahre erfolgen. Für die Evaluation sind „die Standpunkte und Feststellungen des Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen" zu berücksichtigen. Soweit erforderlich, soll die Kommission Änderungen der Datenschutz-Grundverordnung vorschlagen. Sie berücksichtigt dabei insbesondere die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft.

Der Verbraucherzentrale Bundesverband (vzbv) will sich im Prozess der Evaluation der Datenschutz-Grundverordnung aus Sicht der Verbraucher[2] positionieren. Der Verbraucherzentrale Bundesverband hat die Autoren um ein Rechtsgutachten zur Evaluation der Datenschutz-Grundverordnung gebeten, das ihm als Basis der Positionierung in der Debatte um die Evaluation der Datenschutz-Grundverordnung, aber auch der künftigen Fortentwicklung des Datenschutzes als argumentative Grundlage dienen kann.

1.1 Status quo des europäischen Datenschutzrechts

Die Datenschutz-Grundverordnung gilt seit dem 25. Mai 2018 mit all ihren Regelungen in allen Mitgliedstaaten unmittelbar und ist Teil ihrer Rechtsordnung. Sie bestimmt vorrangig das Datenschutzrecht in der Union und im Europäischen Wirtschaftsraum. Sie genießt gegenüber allen Regelungen der Mitgliedstaaten Anwendungsvorrang. Kommt die Anwendung mitgliedstaatlicher Regelungen und der Datenschutz-Grundverordnung zu unterschiedlichen Ergebnissen, ist die Datenschutz-Grundverordnung anzuwenden. Dies gilt allerdings nur dem Grundsatz nach. Denn die Datenschutz-Grundverordnung enthält 70 Öffnungsklauseln. Durch diese überlässt sie in vielen Bereichen und Aspekten die Regelungskompetenz den Mitgliedstaaten. Für das europäische Datenschutzrecht besteht somit eine Ko-Regulierung durch Union und Mitgliedstaaten.

Die Datenschutz-Grundverordnung orientiert sich in weiten Teilen weiterhin an den alten Zielen und Grundsätzen der Datenschutzrichtlinie 95/46/EG[3] von 1995.[4] Sie übernimmt unter anderem in Art. 2 und 3 DSGVO weitgehend die Regelungen zum sachlichen und räumlichen

---

1 EU ABl. L 119 vom 4.5.2016, 1.

2 Zur besseren Lesbarkeit des Textes wird auf die Aufzählung mehrerer Geschlechter verzichtet. Der Begriff „Verbraucher" und ähnliche Begriffe umfassen immer auch alle Personen eines anderen Geschlechts.

3 EG ABl. L 281 vom 23.11.1995, 31.

4 S. Erwägungsgrund 9 DSGVO.

Anwendungsbereich, in Art. 5 DSGVO nahezu unverändert die Grundsätze der Datenverarbeitung, in Art. 6 Abs. 1 DSGVO wörtlich die Voraussetzungen für die Zulässigkeit der Datenverarbeitung und in Art. 9 DSGVO grundsätzlich die Regelungen zu besonderen Kategorien personenbezogener Daten. Hinsichtlich der Rechte der betroffenen Person orientiert sie sich in den Art. 12 bis 23 DSGVO ebenfalls stark an der Richtlinie. In Art. 28 und 29 DSGVO greift die Verordnung grundsätzlich auf die Vorgaben der Richtlinie zur Auftragsverarbeitung zurück. In Art. 32 DSGVO übernimmt sie weitgehend die Anforderungen an die Datensicherheit, in Art. 44 bis 50 DSGVO konzeptionell die Grundsätze zur Datenübermittlung in Drittländer und in Art. 51 bis 59 DSGVO die Konzeption der Stellung und Aufgaben der Aufsichtsbehörden. Diese Regelungen werden in der Verordnung präzisiert, neu gestaltet oder erweitert, aber konzeptionell nicht weiterentwickelt.

Allerdings enthält sie in wenigen Bereichen auch Innovationen, die in der Richtlinie nicht enthalten oder nur angedeutet waren. Diese neuen Instrumente betreffen vor allem die Pflichten der Verantwortlichen und deren Durchsetzung durch die Aufsichtsbehörden, die betroffenen Personen und ihre Verbände.[5] Diese Innovationen sind für Verbraucher mit großen Hoffnungen verbunden.[6] Innovativ ist z.B. in Art. 3 Abs. 2 DSGVO die Ausweitung des räumlichen Anwendungsbereichs durch das Aufenthaltsprinzip. Danach ist die Verordnung auch anwendbar, wenn ein Datenverarbeiter personenbezogene Daten von Personen verarbeitet, die sich in der Union aufhalten. Dies gilt allerdings nur, wenn der Verarbeiter entweder der betroffenen Person Waren oder Dienstleistungen anbietet oder die Datenverarbeitung der Beobachtung ihres Verhaltens in der Europäischen Union dient. Diese Erweiterung sorgt auf dem europäischen Markt für Wettbewerbsgleichheit zwischen Anbietern in der Union und Anbietern außerhalb der Union und vereinfacht die Wahrnehmung von Betroffenenrechten. Bisher unbekannt ist das Recht für betroffene Personen in Art. 20 DSGVO, ihre Daten, die sie einem Verantwortlichen bereitgestellt haben, auf einen anderen Datenverarbeiter zu übertragen. Innovativ sind auch die Anforderungen an den Verantwortlichen in Art. 25 DSGVO, Datenschutz durch Systemgestaltung und Voreinstellungen herzustellen. Neu ist auch seine Verpflichtung in Art. 35 DSGVO, vor riskanten Datenverarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen. Die engere Zusammenarbeit der Aufsichtsbehörden in der Union erforderte in Art. 60 bis 76 DSGVO eigene Regelungen zu deren Durchführung. Eine auffällige Veränderung bringt auch Art. 83 DSGVO, der für Verstöße gegen Vorgaben der Verordnung drastische Sanktionen ermöglicht. Nach Art. 83 Abs. 5 DSGVO können bei den dort aufgelisteten Verstößen Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist.

1.2 Herausforderungen für den Verbraucherdatenschutz

Die Datenschutz-Grundverordnung will das Datenschutzrecht der Mitgliedstaaten ablösen. Wo bisher die Mitgliedstaaten jeweils viele Hunderte von Vorschriften zum Datenschutz hatten, sollen nun die 99 Artikel der Datenschutz-Grundverordnung gelten. Von diesen befassen sich nur 50 Artikel mit materiellen Fragen des Datenschutzes und die anderen Artikel vor allem mit

5 S. zu den Innovationen ausführlich Roßnagel, DuD 2019, 467 ff. und das gesamte Heft 8 der DuD 2019.
6 S. z.B. vzbv, 2013; vzbv, 2018.

Aufgaben und Kompetenzen und Zusammenarbeit der Aufsichtsbehörden und sonstigen organisatorischen Fragen. Um alle vielfältigen Datenschutzprobleme in der gesamten Union in allen Gesellschafts-, Wirtschafts- und Verwaltungsbereichen in 50 Artikeln zu regeln, musste der Unionsgesetzgeber für die Datenschutz-Grundverordnung ein sehr hohes Abstraktionsniveau wählen.

Für den Datenschutz von Verbrauchern enthält die Datenschutz-Grundverordnung auf diesem Abstraktionsniveau eine Reihe von Verbesserungen – in der Regelung des Anwendungsbereichs, in der Anerkennung von Grundsätzen der Datenverarbeitung, in den Rechten für betroffene Personen, in neuen Pflichten für Verantwortliche, in drastischen Sanktionsdrohungen und in neuen Möglichkeiten für Verbraucher, die Aufsichtsbehörden anzurufen und Verbraucherverbände einzuschalten.

Sie hat aber auch die Verarbeitung personenbezogener Daten erleichtert, Zweckänderungen der Datenverarbeitung ermöglicht, eine Reihe von Pflichten der Verantwortlichen reduziert und zahlreiche Möglichkeiten geschaffen, Betroffenenrechte außer Kraft zu setzen. Vor allem hat sie keine einzige Regelung getroffen, die die modernsten Herausforderungen an den Datenschutz von Technikanwendungen spezifisch adressieren. Die Risiken von Big Data, Cloud Computing, smarten Informationstechniken im Alltag, Künstlicher Intelligenz, lernfähigen Systemen, Social Networks oder anderen datengetriebenen Geschäftsmodellen haben keine spezifische Regelung erfahren.

In der Praxis entscheidend ist, wie die vorteilhaft oder nachteilig klingenden Regelungen in ihrer hohen Abstraktheit konkretisiert werden. Hierfür ist entscheidend, dass zwar die Datenschutzaufsichtsbehörden eingreifen und irgendwann die Gerichte entscheiden können,[7] den ersten Zugriff auf das Verständnis und die Konkretisierung der Regelungen aber die Verantwortlichen haben. In jedem Interessenkonflikt nutzen sie jede Unklarheit, Ungenauigkeit, Regelungslücke – schlicht jeden Abstraktionsgrad für ihre Interessen.

Was dies für Verbraucher und ihren Datenschutz im Rahmen der Datenschutz-Grundverordnung bedeutet ist das Thema des Gutachtens.

1.3 Zentrale Forschungsfragen

Das Gutachten soll sich mit zwei Themenblöcken befassen:

Zum einen soll die derzeitige Ausgestaltung der Datenschutz-Grundverordnung aus Verbrauchersicht evaluiert werden. Hauptaugenmerk soll dabei auf die Frage gelegt werden, welche Defizite der Verordnung bei ihrer Anwendung bisher aufgetreten sind und wie die Verordnung nachgeschärft werden muss, um diesen Defiziten zu begegnen. Das Ziel dieses Teils sollte sein, konkrete Regelungsvorschläge zu formulieren, die in den laufenden Evaluationsprozess eingebracht werden können.

Zum anderen soll das Gutachten darstellen, wie eine längerfristige inhaltliche Konzeption für die Fortentwicklung der Datenschutz-Grundverordnung und des Datenschutzes aussehen

[7] S. hierzu skeptisch Kap. 3.3.1.

könnte. Ziel dieses Teils ist es, Ideen und Argumente für die laufenden Diskussionen zur zukünftigen Ausgestaltung des Datenschutzregulierungssystems zu erhalten.

Die Gliederung des Gutachtens leitet sich aus der Untersuchung der beiden Themen ab. Das dieser Einleitung folgende Kapitel 2 führt eine Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht durch. Das Unterkapitel 2.1 untersucht auf der Grundlage von Literatur, Rechtsprechung, Gutachten, Berichten der Datenschutzaufsichtsbehörden, Tagungsteilnahmen und Gesprächen einzelne aus Verbrauchersicht relevante Vorschriften der Datenschutz-Grundverordnung. Hierbei wird vor allem untersucht, wie diese Vorschriften ausgelegt und angewandt werden, ob sich inzwischen Rechtsicherheit durch eine einheitliche Meinung zur Interpretation von Tatbestandsmerkmalen ergeben hat oder ob die unklare Fassung einer Vorschrift zu Meinungsstreitigkeiten und Verunsicherung geführt hat. Das jeweilige Verständnis der Vorschrift wird danach bewertet, wie es sich auf die Interessen der Verbraucher oder Gruppen von Verbrauchern auswirkt. Das Unterkapitel 2.2 bewertet dann die Ergebnisse danach, ob die erkannten Defizite durch den Unionsgesetzgeber oder durch andere verantwortliche Stellen wie den Gesetzgebern der Mitgliedstaaten, den Europäischen Datenschutzausschuss oder Datenschutzaufsichtsbehörden beseitigt werden müssen. Soweit der Unionsgesetzgeber zuständig ist, untersucht das Unterkapitel weiter, ob die Defizite so klar sind, dass sie im Rahmen der Evaluation durch Textänderungen einer Vorschrift behoben werden können, oder ob sie Teil von konzeptionellen Problemen der Datenschutz-Grundverordnung sind, die einer umfassenderen Diskussion bedürfen. Das Unterkapitel 2.3 enthält schließlich 28 Formulierungsvorschläge zur Änderung der Datenschutz-Grundverordnung im Rahmen der anstehenden Evaluation.

Das Kapitel 3 widmet sich inhaltlich dem zweiten Themenkomplex und untersucht, wie eine längerfristige inhaltliche Konzeption für die Fortentwicklung der Datenschutz-Grundverordnung und des Datenschutzes aussehen könnte. Es greift dabei auch die konzeptionellen Defizite der Verordnung auf, die sich nicht durch eine einfache Textänderung beseitigen lassen, sondern die eine konzeptionelle Neuausrichtung des Datenschutzes benötigen. Das Kapitel 3 bietet zu dieser notwendigen inhaltlichen Diskussion Anregungen und Lösungsansätze.

Das Kapitel 4 greift den zweiten Themenkomplex prozedural auf und untersucht, in welchen Prozessen eine Fortentwicklung der Datenschutz-Grundverordnung und des Datenschutzes in der Europäischen Union und in den Mitgliedstaaten erfolgen kann und wer dafür zuständig sein sollte.

Kapitel 5 und 6 fassen die Ergebnisse des Gutachtens in deutscher und englischer Sprache zusammen.

2. Evaluation 2020

Das Europäische Parlament und der Rat haben nach Art. 97 Abs. 1 DSGVO der Europäischen Kommission vorgegeben, bis zum 25. Mai 2020 einen Bericht über die Bewertung und Überprüfung der Datenschutz-Grundverordnung vorzulegen und diesen Bericht auch zu veröffentlichen. Dabei sind nach Art. 97 Abs. 4 DSGVO die Standpunkte und Feststellungen des Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen zu berücksichtigen. Nach Art. 97 Abs. 5 DSGVO legt die Kommission erforderlichenfalls geeignete Vorschläge zur Änderung der Datenschutz-Grundverordnung vor und berücksichtigt dabei insbesondere die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft.

Vielfach liegen den angesprochenen Defiziten der Datenschutz-Grundverordnung unerwünschte Auswirkungen, Wertungswidersprüche, Inkonsistenzen oder Unklarheiten in der Textformulierung zu Grunde, die im Sinne des Gewollten beseitigt, klargestellt oder präzisiert werden sollten, damit die Datenschutz-Grundverordnung ihre Regelungsziele auch tatsächlich erreicht. Vielfach versuchen Rechtsprechung, Literatur und Aufsichtsbehörden diese Defizite durch entsprechende Rechtskonstruktionen oder Auslegungsversuche zu beseitigen. Dies führt jedoch immer zu interessengeleiteten Rechtsstreitigkeiten, die die Anwendung der Verordnung behindern. Bis der Europäische Gerichtshof in Einzelfällen für Rechtssicherheit sorgt, dürfte voraussichtlich noch eine geraume Zeit vergehen. Da er an den Text der Datenschutz-Grundverordnung gebunden ist, dürfte ihm in vielen Fällen die gebotene Korrektur auch gar nicht möglich sein. Daher sollten diese Defizite durch die Europäische Kommission in ihrem Evaluationsbericht aufgegriffen und vom europäischen Gesetzgeber möglichst bald behoben werden.

2.1 Die Datenschutz-Grundverordnung aus Verbrauchersicht

Vor diesem Hintergrund erfolgt eine nach einzelnen Artikeln der Datenschutz-Grundverordnung geordnete Evaluation der Regelungen der Verordnung aus Verbrauchersicht. Wo dies erforderlich ist, werden mitgliedstaatliche Umsetzungen und Ausgestaltungen der Datenschutz-Grundverordnung in Deutschland mitberücksichtigt.

2.1.1 Ausübung persönlicher oder familiärer Tätigkeiten

Die Regelung, den Anwendungsbereich der Datenschutz-Grundverordnung bei Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten auszuschließen, muss vor dem Hintergrund der Entwicklung der Datenverarbeitung kritisch hinterfragt werden.

Nach Art. 2 Abs. 2 lit. c DSGVO findet die Datenschutz-Grundverordnung keine Anwendung auf die Verarbeitung personenbezogener Daten, wenn diese durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten stattfindet. Erwägungsgrund 18 Satz 1 DSGVO präzisiert dies insofern, als kein Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden darf. Satz 2 des Erwägungsgrundes enthält Beispiele, für die die Anwendung der Datenschutz-Grundverordnung ausgeschlossen sein „könnte“. Dies ist das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten. Satz 3 stellt fest, dass der Ausschluss der Anwendung für den Verantwortlichen nicht für die Verantwortlichen oder Auftragsverarbeiter gilt, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen. Persönliche Tätigkeiten sind im Ergebnis Tätigkeiten, die der eigenen Selbstentfaltung und Freiheitsausübung in der Freizeit oder

im privaten Raum dienen, während familiäre Tätigkeiten solche Tätigkeiten sind, die der Pflege familiärer Beziehungen und des familiären Zusammenhalts dienen.[8]

Der vollständige Ausschluss des Anwendungsbereichs der Datenschutz-Grundverordnung gilt generell und auch dann, wenn besondere Kategorien personenbezogener Daten verarbeitet werden.[9] Eine Einzelfallabwägung findet auch bei hohen tatsächlichen Risiken durch die Datenverarbeitung nicht statt. Es wird deshalb eine enge Auslegung der Regelung gefordert.[10] Zu beachten ist, dass durch die Verwendung des Begriffs „ausschließlich" in der Vorschrift eine Verarbeitung, die zu einem Teil auch außerhalb des persönlichen oder familiären Bereichs liegt, trotz der teilweisen Verortung in der persönlichen oder familiären Sphäre der Datenschutz-Grundverordnung unterliegt.[11]

Nicht unter die Ausnahme des Art. 2 Abs. 2 lit. c DSGVO fällt der Austausch von Informationen mit und in einem größeren Kreis von Kommunikationsteilnehmern.[12] Problematisch ist es dabei festzustellen, wo die Grenze zwischen persönlicher Kommunikation und Kommunikation in einem größeren Teilnehmerkreis verläuft. Klar ist lediglich, dass der Anwendungsbereich der Datenschutz-Grundverordnung eröffnet ist, wenn der Empfängerkreis personenbezogener Daten eine unbestimmte Größe hat.[13] Dies hat in der Praxis zu Unsicherheiten geführt, die sich in Fällen von Ubiquitous Computing[14] künftig noch steigern werden. Findet etwa eine Datenverarbeitung im Smart Home statt, so ist im Zweifel, wenn eine Nutzungsbeschränkung auf den Wohnungsinhaber und seine Familie nicht sichergestellt ist, von der Anwendbarkeit der Datenschutz-Grundverordnung auszugehen.[15] Erfassen Wearables oder das Smart Car personenbezogene Daten im öffentlichen Raum, so ist die Verordnung ebenfalls anwendbar.[16] Unklar aber ist bei der gegenwärtigen Formulierung, wo die Grenzen liegen. Dadurch entstehen hohe Befolgungsrisiken bei den Personen, die Daten für persönliche und familiäre Zwecke verarbeiten.

---

8 Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 2 Rn. 25.

9 S. Ennöckl, in: Sydow, 2018, Art. 2 Rn. 11.

10 EuGH C-212/13, EuZW 2015, 234 Rn. 28 f. – Ryneš; Husemann, in: Roßnagel, Das neue Datenschutzrecht, 2018, § 3 Rn. 9; Kühling/Raab, in: Kühling/Buchner, 2018, Art. 2 Rn. 23; Zerdick, in: Ehmann/Selmayr, 2018, Art. 2 Rn. 10; zum Gebot der restriktiven Auslegung, um der Datenschutzkonvention des Europarats (Konvention 108, BGBl. II 1985, 538) zu genügen, die diese Ausnahme nicht kennt, s. Ennöckl, in: Sydow, 2018, Art. 2 Rn. 10; Dammann, in: Simitis, § 1 Rn. 148.

11 S. z.B. Dammann, in: Simitis, BDSG, 2014, § 1 Rn. 150; Simitis, in: Simitis, BDSG, 2014, § 27 Rn. 47 ff.; Buchner, in: Taeger/Gabel, BDSG, 2013, § 27 Rn. 19; a.A. Gola/Lepperhoff, ZD 2016, 9 (10).

12 Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 2 Rn. 29.

13 S. EuGH C-101/01, EuZW 2004, 245 Rn. 37 ff. – Lindquist, Anm. Roßnagel, MMR 2004, 99 f.; Dammann, RDV 2004, 19; s. auch Ernst, in: Paal/Pauly, 2018, Art. 2 Rn. 21; Ennöckl, in: Sydow, 2018, Art. 2 Rn. 13; Kühling/Raab, in: Kühling/Buchner, 2018, Art. 2 Rn. 25; Albrecht/Jotzo, Teil 3 Rn. 30; Gola, in: Gola, 2018, Art. 2 Rn. 16; Dammann, in: Simitis, BDSG, 2014, § 1 Rn. 151; a.A. von Lewinski, in: Auernhammer, 2018, Art. 2 Rn. 24; Buchner, FamRZ 2019, 665 (666 f.).

14 Für eine Einschränkung der Ausnahme argumentiert Roßnagel, 2007, 131, 192 f.

15 S. hierzu Geminn, DuD 2015, 575; von Lewinski, in: Auernhammer, 2018, Art. 2 Rn. 30; Skistims, Smart Homes, 2016, 393 ff. Werden Daten etwa an den Energieversorger oder Dienstleister weitergegeben oder werden von Gästen, Handwerkern, Postboten etc. erfasste Daten weitergegeben, entfällt der persönliche oder familiäre Zweck.

16 Dies aber z.B. umstritten mit Blick auf sog. Dashcams; s. z.B. Reibach, DuD 2015, 157; Kinast/Kühnl, NJW 2014, 3057; Greger NVZ 2015, 114. Zu Drohnen s. Bischof DuD 2017, 142 (144 f.). Zu Kamerasystemen s. Stöber, NJW 2016, 3681 (3682); EuGH C-212/13, EuZW 2015, 234, Rn. 34 f. – Ryneš. Zu Wearables s. Rose, DuD 2017, 137 (138 f.); Solmecke/Kocatepe, ZD 2014, 22; Schwenke, DuD 2015, 161. Zum Smart Car s. Roßnagel u.a., 2016, 59 f.; Roßnagel/Hornung, 2019.

2.1.1.1 Hohe Datenschutzrisiken

Auch jenseits von Abgrenzungsproblemen, denen durch Konkretisierungen durch den Europäischen Datenschutzausschuss jenseits der bereits erfolgten Rechtsprechung des Europäischen Gerichtshofs[17] abgeholfen werden sollte, liegen Probleme. So hat der einzelne Verbraucher heute Zugriff auf hochkomplexe Technik, die etwa über Aktivitätsberichte oder direkt über Video und Audio auch zur Überwachung von Kindern[18] oder des Lebenspartners eingesetzt werden kann.[19]

Soweit das Risiko der Datenverarbeitung über anerkannte Fallgruppen persönlicher und familiärer Tätigkeiten hinausgeht, ist zu fordern, dass die Ausnahme eingeschränkt wird – zumindest in Fällen, in denen eine deutliche Risikosteigerung vorliegt. Dies sollte in jedem Fall dann angenommen werden, wenn durch die Datenverarbeitung eine umfassende Überwachung ermöglicht wird. Eine vollständige Ausnahme auch dieser Art von Datenverarbeitung wird dem Schutzbedürfnis der betroffenen Personen, insbesondere Minderjähriger, nicht gerecht.[20] Deren Schutz ist aber gerade auch verfassungsrechtlich mit Blick auf Art. 7 und 8 GRCh geboten. Die Quantität der Datenverarbeitung sollte indes nicht entscheidend sein,[21] sondern es sollte auf die Zwecke der Verarbeitung abgestellt werden.

Bei Social Networks, Messengern und ähnlichen Diensten besteht überdies häufig das Problem, dass alle eingebrachten Daten dem Betreiber bekannt werden.[22] Damit besteht gleichzeitig das Risiko einer Weitergabe an Dritte – sowohl an befreundete Unternehmen des Anbieters, Werbetreibende und staatliche Stellen.[23]

Zusammenfassend ist zu konstatieren, dass die Ausnahme des Art. 2 Abs. 2 lit. c DSGVO ein Beispiel für die Unzulänglichkeiten der Datenschutz-Grundverordnung bei der Gewährleistung eines risikoadäquaten Schutzes der betroffenen Personen ist. Ihre Übernahme aus Art. 3 der Datenschutzlinie wird den seit den 1990er Jahren erfolgten enormen technischen Entwicklungen nicht gerecht. Diese Entwicklung betrifft nicht nur Rechenleistung, sondern auch Speicherkapazitäten und Möglichkeiten zur Datenübermittlung. Darüber hinaus wurde Sensorik verschiedenster Art auf dem Verbrauchermarkt verfügbar und kann im privaten und familiären Bereich eingesetzt werden.[24] Eine vollständige Ausnahme, wie sie Art. 2 Abs. 2 lit. c DSGVO darstellt, kann vor dem Hintergrund dieser Entwicklung und der damit verbundenen Risiken

---

17 EuGH C-101/01, EuZW 2004, 245 Rn. 37 ff. – Lindqvist, Anm. Roßnagel MMR 2004, 99 f.; Dammann, RDV 2004, 19; EuGH C-212/13, EuZW 2015, 234 Rn. 34 f. – Ryneš.

18 S. z.B. Buchner, FamRZ 2019, 665 (667 f.).

19 Gola/Lepperhoff, ZD 2016, 9 (12); Roßnagel/Kroschwald, ZD 2014, 495; s. Husemann, in: Roßnagel, 2018, § 3 Rn. 9.

20 In diese Richtung gehend auch Albrecht/Jotzo, Teil 3 Rn. 30; Buchner, FamRZ 2019, 665 (667 f.).

21 So aber z.B. Dammann, in: Dammann/Simitis, DSRL, 1997, Art. 2 Rn. 8; Dammann, in: Simitis, BDSG, 2014, § 1 Rn. 150.

22 Dies gilt z.B. nicht für die Inhalte der Kommunikation, wenn Messenger-Dienste diese Ende-zu-Ende-verschlüsseln.

23 Buchner, FamRZ 2019, 665 (666) weist zurecht darauf hin, dass sich z.B. Facebook in seinen Nutzungsbedingungen eine „nicht-exklusive, übertragbare, unterlizenzierbare und weltweite Lizenz“ einräumen lässt, die Inhalte seiner Nutzer „zu hosten, zu verwenden, zu verbreiten, zu modifizieren, auszuführen, zu kopieren, öffentlich vorzuführen oder anzuzeigen, zu übersetzen und abgeleitete Werke davon zu erstellen“ (Ziff. 3.1; https//de-de.facebook.com/legal/terms).

24 S. hierzu ausführlich Roßnagel, 2007, 192 ff.; Roßnagel u.a., 2016, 1 ff.

nicht gerechtfertigt werden.[25] Vielmehr ist auch bei persönlichen und familiären Tätigkeiten risikoadäquat zu differenzieren und nur bei – näher zu bestimmenden – geringen Risiken auf eine Anwendung des Datenschutzrechts zu verzichten.

2.1.1.2 Beschränkte Anwendung der Datenschutz-Grundverordnung

Umgekehrt ist festzustellen, dass Datenverarbeitungen im privaten Handlungskontext aufgrund der enormen technischen Möglichkeiten, die ein Nutzer bereits heute und erst recht künftig hat, zwar in den Geltungsbereich der Verordnung fallen, aber dennoch sozial üblich sind. Da die Datenschutz-Grundverordnung keine Differenzierungen kennt, sind auf diese Handlungen, wenn sie unter die Verordnung fallen, alle Anforderungen der Datenschutz-Grundverordnung anzuwenden. Diese sind den (privaten) Verantwortlichen gegenüber weder zu vermitteln noch effektiv durchzusetzen. Das in der Praxis vielleicht relevanteste Beispiel dürfte die Veröffentlichung von Gruppenbildern auf einer privat genutzten Webseite oder auf einem Social Network sein. Die Veröffentlichung im Internet gehört nach Ansicht des Europäische Gerichtshofs „offensichtlich nicht" zum Privat- und Familienleben von Einzelpersonen.[26] Doch selbst wenn eine Einwilligung der abgebildeten Personen eingeholt und dokumentiert wurde, fehlt es in der Regel an datenschutzkonformen Information, Dokumentation, Systemgestaltung, Sicherungsmaßnahmen. Diese millionenfach durch Aufsichtsmaßnahmen einzufordern und durch Sanktionen durchzusetzen, wäre sozial inadäquat und unverhältnismäßig.

Sowohl um bei der Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten unvertretbare Risiken für betroffene Personen zu vermeiden als auch um bei sozial üblichem und vertretbarem Verhalten außerhalb dieses Bereichs unverhältnismäßige Datenschutzmaßnahmen nicht ergreifen zu müssen, sollte die Datenschutz-Grundverordnung einen Handlungsbereich definieren, der bei erhöhten Risiken zwar Datenschutzpflichten begründet, aber die Verordnung nicht vollständig zur Anwendung kommen lässt. Für diesen Bereich sollten nur ausgewählte Regelungen gelten.[27] Denkbar wären etwa die Regelungen der Datenschutz-Grundverordnung zur Interessenabwägung, zum Schadensersatz, zur Datensicherung und zur Auftragsverarbeitung sowie angepasste Regelungen zur Signalisierung der Einwilligung und Identifizierung betroffener Personen sowie zur Auskunft.[28]

2.1.2 Aufenthaltsprinzip

Der räumliche Anwendungsbereich der Datenschutz-Grundverordnung wurde im Vergleich zur Datenschutzrichtlinie deutlich ausgeweitet. Die Ausweitung des Anwendungsbereichs der Datenschutz-Grundverordnung in Art. 3 Abs. 2 DSGVO gilt in zwei Fällen – wenn ein Datenverarbeiter personenbezogene Daten von Personen verarbeitet, die sich in der Union aufhalten, nämlich wenn er entweder der betroffenen Person Waren oder Dienstleistungen anbietet

---

25 Roßnagel/Nebel/Richter, ZD 2015, 455; Gola/Lepperhoff, ZD 2016, 9 (12).

26 EuGH C-101/01, EuZW 2004, Rn. 47; s. auch EuGH C-73/ 07. S. auch Kühlung/Raab, in: Kühling/Buchner, DSGVO, 2018, Art. 2 Rn. 25.

27 S. etwa Jandt/Roßnagel, ZD 2011, 160; Roßnagel/Richter/Nebel, ZD 2013, 104.

28 S. z.B. Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 2, Rn. 55.

(Marktort) oder die Datenverarbeitung der Beobachtung ihres Verhaltens dient (Beobachtungsort).[29] Dadurch will die Datenschutz-Grundverordnung auf dem europäischen Markt für Wettbewerbsgleichheit zwischen Anbietern in der Union und Anbietern außerhalb der Union sorgen und die Wahrnehmung von Betroffenenrechten vereinfachen. Mit der Ausweitung ist die Geltung des europäischen Datenschutzrechts nicht mehr an die Niederlassung des Verantwortlichen geknüpft, sondern hängt auch vom Aufenthaltsort der betroffenen Person in der Europäischen Union ab.

Möglich gewesen wäre indes auch eine Ausweitung des räumlichen Anwendungsbereichs, die sich nicht auf das Anbieten von Waren oder Dienstleistungen oder die Verhaltensbeobachtung beschränkt. Eine Erstreckung des Anwendungsbereichs auf jede Form der Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Europäischen Union aufhalten, hätte Abgrenzungsschwierigkeiten zwischen Art. 3 Abs. 2 lit. a und b DSGVO vermieden und eine weitere Steigerung des Schutzniveaus bedeutet.[30] Zudem bereitet auch die Frage, wann ein Angebot („anbieten“) an betroffene Personen in der Europäischen Union vorliegt, Schwierigkeiten.[31] Die Erwägungsgründe 23 und 24 DSGVO allein reichen zur Klarstellung dieser relevanten Abgrenzungsprobleme nicht aus. Problematisch gestaltet sich beispielsweise das Angebot von Waren oder Dienstleistungen auf einer Webseite in einer Sprache, die auch außerhalb der Europäischen Union Landessprache ist.[32] Sofern hier nicht direkt Personen in der Europäischen Union angesprochen werden, ist fraglich, ob „offensichtlich“ im Sinn von Erwägungsgrund 23 DSGVO betroffene Personen in einem oder mehreren Mitgliedstaaten adressiert werden.

In der Literatur wird ein Rückgriff auf Art. 57 Abs. 1 AEUV und Richtlinie 2006/123/EG (bezogen auf Dienstleistungen) sowie Art. 28 ff. AEUV (bezogen auf Waren) diskutiert.[33] Dies entspräche dem Gebot einer autonomen Auslegung der Datenschutz-Grundverordnung am Maßstab des europäischen Rechts, steht jedoch vor dem Problem, dass die dort befindlichen Definitionen nicht ohne Anpassungen übernommen werden können.[34] In jedem Fall ist eine weite Auslegung der Begriffe angezeigt, um Schutzlücken auszuschließen.

Den Abgrenzungsschwierigkeiten könnte zwar eine Klarstellung durch den Europäischen Datenschutzausschuss abhelfen, die insbesondere auf die Begriffe „Waren“, „Dienstleistungen“ und „anbieten“ konkretisierend eingeht.[35] Wirksamer und eindeutiger wäre jedoch die Einschränkung auf das Angebot von Waren und Dienstleistungen zu streichen.

Von besonderer Bedeutung ist für die Wahrnehmung des Datenschutzrechts in dem neu beschriebenen Anwendungsbereich, dass sich bei den Aufsichtsbehörden Praktiken herausbilden,

---

29 Die Bezeichnung Marktortprinzip trifft dementsprechend nur für Art. 3 Abs. 2 lit. a DSGVO zu, nicht aber für lit. b.

30 S. Husemann, in: Roßnagel, 2018, § 3 Rn. 17.

31 S. zur Problematik Klar, in: Kühling/Buchner, 2018, Art. 3 Rn. 80 ff.

32 S. Klar, in: Kühling/Buchner, 2018, Art. 3 Rn. 87.

33 So etwa Klar, in: Kühling/Buchner, 2018, Art. 3 Rn. 71 ff. bzw. 76 ff. S. auch Zerdick, in: Ehmann/Selmayr, 2018, Art. 3 Rn. 18.

34 So auch Klar, in: Kühling/Buchner, 2018, Art. 3 Rn. 73 bzw. 79.

35 S. Hornung, in: Simitis/Hornung/Spiecker, 2019, Art. 3 Rn. 48 ff.; Ennöckl, in: Sydow, EU-DSGVO, 2. Aufl. 2018, Art. 3 Rn. 13 f.

die eine effektive Rechtsdurchsetzung auch jenseits der Grenzen der Europäischen Union ermöglichen. Hier wird kritisiert, dass insbesondere ein Durchgriff auf kleine Anbieter Schwierigkeiten bereiten dürfte,[36] aber auch allgemein grundsätzliche Durchsetzungsprobleme außerhalb der Grenzen der Europäischen Union bestehen.[37] Eine Beschlagnahme etwa von in der Europäischen Union befindlichem Vermögen ist nicht möglich, wenn ein solches Vermögen gar nicht existiert. Auch eine Durchsetzung gegenüber dem Vertreter in der Europäischen Union[38] scheidet aus, wenn gar kein Vertreter bestellt wurde. Schon die Zustellung eines Bußgeldbescheides kann auf globaler Ebene leicht scheitern. Die Diskussion um Lösungsansätze steckt hier noch in den Anfängen.

2.1.3 Grundsätze der Datenverarbeitung

Die gesetzliche Festlegung der Datenschutzgrundsätze in Art. 5 DSGVO ist ein großer Fortschritt im Vergleich zu Art. 6 Abs. 1 DSRL. Sie sollte jedoch hinsichtlich des Grundsatzes „Treu und Glauben" präzisiert und um den Grundsatz der Datenvermeidung, der nicht im Grundsatz der Datenminimierung enthalten ist, ergänzt werden.

2.1.3.1 Grundsatz der Fairness

Nach Art. 5 Abs. 1 lit. a DSGVO und Art. 8 Abs. 2 Satz 1 GRCh müssen personenbezogene Daten nach Treu und Glauben verarbeitet werden. Der Grundsatz von Treu und Glauben ist in seiner Tragweite jedoch umstritten. Der Europäische Gerichtshof hat festgestellt, er verpflichte etwa „eine Verwaltungsbehörde, die betroffenen Personen davon zu unterrichten, dass die personenbezogenen Daten an eine andere Verwaltungsbehörde weitergeleitet werden, um von dieser […] weiterverarbeitet zu werden".[39] Dabei sind aber die Unterschiede zwischen Art. 5 Abs. 1 lit. a DSGVO und Art. 6 Abs. 1 DSRL zu beachten, zu dem die Entscheidung erging. Bezogen auf Art. 5 Abs. 1 lit. a DSGVO dürfte die vom Europäischen Gerichtshof formulierte Anforderung im Transparenzprinzip aufgehen. Dem Grundsatz von Treu und Glauben muss also ein darüberhinausgehender Gehalt zukommen. Im deutschen Recht ist der Begriff bereits zivilrechtlich besetzt, muss aber in der Datenschutz-Grundverordnung autonom ausgelegt werden. Um hier Missverständnisse zu vermeiden, sollte die deutsche Sprachfassung der Datenschutz-Grundverordnung Treu und Glauben durch Fairness übersetzen.[40] Der Begriff wird auch in der englischen Fassung verwendet und ist auch als deutscher Begriff im Duden zu finden.

Bezogen auf Gehalt und Tragweite des Grundsatzes von Treu und Glauben ist zu verhindern, dass er einerseits durch den Grundsatz der Transparenz, andererseits durch den Grundsatz der Rechtmäßigkeit der Verarbeitung überflüssig ist. Er könnte die Rolle einer Auffangklausel einnehmen, wenn eine Verarbeitung zwar formell und materiell rechtmäßig erfolgt, dies aber in

---

36 S. etwa Schwartmann, in: Schwartmann u.a., 2018, Art. 4 Rn. 38.

37 S. Klar, in: Kühling/Buchner, 2018, Art.3 Rn. 27, der darauf verweist, dass „Ermittlungs- und Rechtsdurchsetzungsbefugnisse im EU-Ausland nur nach Maßgabe bislang nicht existierender zwischenstaatlicher Verträge bestehen"; vgl. Geminn, DVBl. 2018, 1593 (1594).

38 S. Art 27 Abs. 1 DSGVO. Auch die faktische Möglichkeit der Überprüfung des Vorliegens der Ausschlusskriterien von Art. 27 Abs. 2 DSGVO ist von der Kooperation des nicht in der Europäischen Union niedergelassenen Verantwortlichen oder Auftragsverarbeiters abhängig.

39 EuGH, C-201/14, ZD 2015, 577 (578) Rn. 56 – Bara.

40 So Reimer, in: Sydow, 2018, Art. 5 Rn. 14; Wolff, in: Schantz/Wolff, 2018, Rn. 392; Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 5 Rn. 47.

einem bestimmten Fall als unbillig erscheint, etwa weil das Machtgefälle zwischen Anbieter und Verbraucher „unfair" zum Nachteil des Verbrauchers ausgenutzt wurde.[41] Der Europäische Datenschutzausschuss sieht im Grundsatz von Treu und Glauben eine Würdigung der „reasonable expectations" der betroffenen Person mit Blick auf die Machtasymmetrie zwischen dieser und dem Verantwortlichen.[42] Zusammenfassend ist der Gehalt des Grundsatzes von Treu und Glauben in der Datenschutz-Grundverordnung zu präzisieren, denn er ist in höchstem Maße ausfüllungsbedürftig. Dies könnte etwa in Erwägungsgrund 39 DSGVO geschehen, so wie es dort auch bezogen auf den Grundsatz der Transparenz geschehen ist. Zudem sollte seine Rolle in der Interessenabwägung und der Bewertung der Wirksamkeit der Einwilligung[43] gestärkt werden.

Aber auch die weiteren Grundsätze für die Verarbeitung personenbezogener Daten bedürfen der Präzisierung. Statt solche Präzisierungen vorzunehmen, ist die Datenschutz-Grundverordnung wie an vielen Stellen auch hier von der Verwendung unbestimmter Begriffe geprägt,[44] die äußerst interpretationsoffen sind.[45] Der Europäische Datenschutzausschuss sollte hier durch die Formulierung von entsprechenden Leitlinien tätig werden.

2.1.3.2 Grundsatz der Datenvermeidung

§ 3a BDSG a.F. enthielt das Gebot von Datenvermeidung und Datensparsamkeit. Obwohl es zu den allgemeinen Datenschutzprinzipien zählte, war es nicht sanktionsbewehrt und blieb unspezifisch; seine praktische Relevanz war denkbar gering. In Art. 5 Abs. 1 lit. c DSGVO spricht die Datenschutz-Grundverordnung nun von „Datenminimierung". Es handelt sich dabei um eine Fortführung des Grundsatzes der Erforderlichkeit der Verarbeitung aus Art. 6 Abs. 1 lit. c DSRL. Daten dürfen nur insoweit verarbeitet werden, als sie als Mittel zur Erreichung des Zwecks der Verarbeitung erforderlich sind; der Verantwortliche ist aber frei, den Zweck der Verarbeitung zu wählen und auszugestalten. Dieser Zweck wird vom Grundsatz der Datenminimierung nicht weiter hinterfragt. § 3a BDSG a.F. forderte hingegen, die Vermeidung von personenbezogenen Daten bereits bei der Zweckfestlegung zu berücksichtigen, mithin den Zweck so auszuwählen, dass möglichst wenige personenbezogene Daten erforderlich werden.[46] Geht es etwa um die Abrechnung der Nutzung eines Dienstes, so wäre ein Abrechnungsverfahren zu wählen, das möglichst wenige personenbezogene Daten erfordert.[47] Umgangssprachlich zwar nahe verwandt, sind Datenminimierung und Datensparsamkeit damit nicht gleichbedeutend.[48] Datenvermeidung kann als Gebot allenfalls aus Erwägungsgrund 78 Satz 3 DSGVO

---

41 So Dammann, in: Damann/Simitis, 1997, Art. 6 Rn. 3 für die Datenschutzrichtlinie; ebenso Reimer, in: Reimer, 2018, Art. 5 Rn. 14; Herbst, in: Kühling/Buchner, 2018, Art. 5 Rn. 17 für die DSGVO.

42 Draft Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version for public consultation, 9 April 2019, 5.

43 S. hierzu Kap. 2.1.4.

44 Z.B. „nachvollziehbar", „geeignet", „angemessen", „legitim", „vereinbar", „erheblich", „erforderlichenfalls".

45 S. Richter, DuD 2015, 735 (739); Roßnagel/Nebel/Richter, ZD 2015, 455 (457 f.); Frenzel, in: Paal/Pauly, 2018, Art. 5 Rn. 55.

46 Roßnagel, in: Eifert/Hoffmann-Riem, 2011, 41 ff. m.w.N.

47 So bereits Roßnagel/Pfitzmann/Garstka, 2001, 101.

48 Roßnagel, DuD 2016, 561 (562); Herbst, in: Kühling/Buchner, 2018, Art. 5 Rn. 55. Trotz anderslautender Stimmen in der deutschsprachigen Fachliteratur, z.B. Albrecht/Jotzo, 2017, 52; Buchner, DuD 2016, 155 (156); Heberlein, in: Ehmann/Selmayr, 2018, Art. 5 Rn. 22; Frenzel, in: Paal/Pauly, 2018, Art. 5 Rn. 53; Wolff, in: Schantz/Wolff, 2018, Rn. 427; Pötters, in: Gola, 2018, Art. 5 Rn. 21.

herausgelesen werden, der fordert als Teil von Art. 25 DSGVO die Verarbeitung personenbezogener Daten zu minimieren. Zudem kann er als Teil des Verhältnismäßigkeitsgrundsatzes in die Auslegung von Verarbeitungserlaubnissen der Datenschutz-Grundverordnung Eingang finden, wonach ein Eingriff in grundrechtlich geschützte Positionen so gering wie möglich gehalten werden muss.[49] Aus Gründen der Rechtssicherheit sollte ein § 3a BDSG a.F. entsprechendes Grundprinzip dennoch explizit Eingang in die Datenschutz-Grundverordnung finden. Hierzu böte sich vor allem Art. 5 Abs. 1 lit. c DSGVO an. Dann würden auch Verstöße gegen das Prinzip mit Sanktionen belegt werden können.

Abgesehen von den angesprochenen Problemen im Einzelfall ist den Grundsätzen der Datenverarbeitung gemein, dass sie mit moderner, insbesondere mit smarter Informationstechnik in Konflikt geraten. Sie müssen deshalb modernisiert und risikoadäquat weiterentwickelt werden.[50]

2.1.4 Einwilligung und andere Erlaubnistatbestände

Nach dem Geltungsbeginn der Datenschutz-Grundverordnung im Mai 2018 waren die E-Mail-Postfächer vieler Verbraucher voll von Nachrichten, die vor dem Hintergrund der Verordnung zur Abgabe einer Einwilligung aufforderten. Diese Aufforderungen erfolgten oftmals, obwohl bereits eine Verarbeitungserlaubnis nach Art. 6 Abs. 1 UAbs. 1 lit. b oder lit. f DSGVO bestand.[51] Dies führte durch die bürokratische Aufforderung und die notwendige Zusatzarbeit nicht nur zu einem Prestigeverlust des Datenschutzes; lange gehegte Vorurteile sahen sich bestätigt. Vielmehr führt die Inanspruchnahme einer Einwilligung nach Art. 6 Abs. 1 lit. a oder 9 Abs. 2 lit. a DSGVO neben einem weiteren gesetzlichen Erlaubnistatbestand zu einer Verwirrung über die Voraussetzungen und Rechtsfolgen der Datenverarbeitung.

Einerseits suggeriert Art. 6 Abs. 1 UAbs. 1 DSGVO durch die Verwendung des Begriffs „mindestens“, dass mehrere Erlaubnistatbestände nebeneinander Anwendung finden können.[52] Dies wird unterstützt durch die Regelung des Art. 17 Abs. 1 lit. b DSGVO, nach der ein Widerruf der Einwilligung nur dann einen Anspruch auf Datenlöschung begründet, wenn es „an einer anderweitigen Rechtsgrundlage für die Verarbeitung“ fehlt.[53] Dieser Vorbehalt betrifft nicht die Verpflichtung zur Datenverarbeitung gemäß Art. 6 Abs. 1 lit. c DSGVO. Denn bei einer solchen Verpflichtung gelten nach Art. 17 Abs. 3 lit. b DSGVO die Abs. 1 und 2 dieser Vorschrift überhaupt nicht. Der Löschanspruch nach Art. 17 Abs. 1 lit. b DSGVO ist somit dann ausgeschlossen, wenn eine Datenverarbeitung auf die Erlaubnistatbestände des Art. 6 Abs. 1 UAbs. 1 lit. b oder lit. f DSGVO gestützt wird.

---

49 S. bezogen auf die Verarbeitung personenbezogener Daten EuGH, C-293/12 und C-594/12, NJW 2014, 2169 – Digital Rights Ireland; EuGH, C-362/14, NJW 2015, 3151 – Schrems; EuGH, C-203/15 und C-698/15, NJW 2017, 717 – Tele2 Sverige; BVerfGE 65, 1 (43, 46).

50 S. hierzu näher Kap. 3.3.

51 S. hierzu und zum Folgenden auch Roßnagel, DuD 2018, 741 (745).

52 So auch Schulz, in: Gola, 2018, Art. 6 Rn. 11 f.; Buchner/Kühling, in: Kühling/Buchner, 2018, Art. 7 Rn. 17; Schantz, in: Simitis/Hornung/Spiecker, 2019, Art. 6 Abs. 1 Rn. 12.

53 S. Dix, in: Simitis/Hornung/Spiecker, 2019, Art. 17 Rn. 13; Herbst, in: Kühling/Buchner, 2018, Art. 17 Rn. 24 f.

Dennoch verstößt bezogen auf die Einwilligung die Nutzung mehrerer Tatbestände gegen den Grundsatz von Treu und Glauben, da der Verantwortliche hier das Vertrauen der betroffenen Person missbraucht.[54] Ähnlich hat sich auch die Artikel 29-Datenschutzgruppe geäußert. In den Leitlinien zur Einwilligung nach der Datenschutz-Grundverordnung weist sie darauf hin, dass der Verantwortliche, der seine Verarbeitung auf eine Einwilligung stützt, bereit sein müsse, „die Entscheidung zu respektieren und den Teil der Verarbeitung zu beenden, wenn eine Einzelperson ihre Einwilligung widerruft".[55] Die Artikel 29-Datenschutzgruppe beruft sich dabei zumindest indirekt auf den Grundsatz von Treu und Glauben, indem sie feststellt, es „wäre gegenüber Einzelpersonen ein in höchstem Maß missbräuchliches Verhalten, ihnen zu sagen, dass die Daten auf der Grundlage der Einwilligung verarbeitet werden, wenn tatsächlich eine andere Rechtsgrundlage zugrunde gelegt wird".[56] Die Datenschutzgruppe erwartet, dass der Verantwortliche sich vor Datenerhebung auf eine Rechtsgrundlage festlegen muss.[57] Zudem hat die Artikel 29-Datenschutzgruppe klargestellt, dass die Formulierung des Art. 17 Abs. 1 lit. b DSGVO, wonach personenbezogene Daten unverzüglich zu löschen sind, wenn die betroffene Person ihre Einwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt, auf Fälle abzielt, in denen ein Datensatz zu unterschiedlichen Zwecken aufgrund unterschiedlicher Rechtsgrundlagen verarbeitet wird.[58] Dies dürfte auch für die Formulierung von Art. 6 Abs. 1 UAbs. 1 DSGVO zutreffen.

Die Regelung der Datenschutz-Grundverordnung ist derzeit widersprüchlich. Sie sieht für die Einwilligung andere Voraussetzungen, Einwirkungsmöglichkeiten und Rechtsfolgen vor, wie für eine Datenverarbeitung, die auf die Erforderlichkeit einer Vertragserfüllung oder eines überwiegenden berechtigten Interesses gestützt wird. Es geht jeweils um die gleiche Datenverarbeitung. Diese kann nicht zugleich unterschiedlichen Regelungskomplexen unterliegen. Auch sieht die Datenschutz-Grundverordnung keine Wahlfreiheit des Verantwortlichen darüber vor, welche Regelungen für die Datenverarbeitung gelten sollen.

Mit der Einwilligung oder der Berufung auf einen gesetzlichen Erlaubnistatbestand sind unterschiedliche Informationspflichten verbunden. So muss der Verantwortliche nach Art. 13 Abs. 1 lit. c und 14 Abs. 1 lit. d DSGVO über die Rechtsgrundlagen der Datenverarbeitung informieren, ob er sich also auf Einwilligung, Vertrag oder überwiegende berechtigte Interessen beruft. Bei einer Berufung auf eine für ihn günstige Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO muss er nach Art. 13 Abs. 1 lit. d und 14 Abs. 2 lit. b DSGVO über seine berechtigten Interessen informieren. Er muss bei einer Einwilligung nach Art. 13 Abs. 2 lit. c DSGVO und nach Art. 14 Abs. 2 lit. d DSGVO auf die Möglichkeit und die Folgen eines Widerrufs hinweisen. Bei einer Datenverarbeitung, die auf eine Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO gestützt wird, muss er dagegen nach Art. 13 Abs. 2 lit. b und Art.

---

54 S. Erwägungsgrund 43 DSGVO. S. auch Brink/Hertfelder, in: Roßnagel/Hornung, 2019, 75 ff.; Wolff, in: Schatz/Wolff 2017, Rn. 475; Buchner/Petri, in: Kühling/Buchner, 2018, Art. 6 Rn. 22; Buchner/Kühling, in: Kühling/Buchner, 2018, Art. 7 Rn. 18, 21; Uecker, ZD 2019, 248; a.A. z.B. Schulz, in: Gola, 2018, Art. 6 Rn. 11 f.

55 Artikel 29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung, WP 259 rev.01, 27.

56 Leitlinien in Bezug auf die Einwilligung, WP 259 rev.01, 27.

57 Leitlinien in Bezug auf die Einwilligung, WP 259 rev.01, 28.

58 Artikel 29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung, WP 259 rev.01, 26.

14 Abs. 2 lit. c DSGVO über die Möglichkeit eines Widerspruchs nach Art. 21 DSGVO informieren. Widerruf und Widerspruch haben jedoch unterschiedliche Voraussetzungen und Wirkungen.

Informiert der Verantwortliche darüber, dass seine Datenverarbeitung sowohl durch eine Einwilligung als auch durch eine Interessenabwägung legitimiert ist, muss er also der betroffenen Person widersprüchliche Informationen zur gleichen Datenverarbeitung präsentieren. Lässt er sich nur eine Einwilligung geben und informiert über die durch Einwilligung gerechtfertigte Datenverarbeitung korrekt und beruft sich später auf eine Interessenabwägung, hat er die betroffene Person über ihre Rechte aus der Einwilligung getäuscht und ihr die notwendigen Informationen zur Datenverarbeitung aufgrund einer Interessenabwägung vorenthalten.

Wenn ein Verantwortlicher seine Datenverarbeitung bereits auf die Erlaubnistatbestände der Art. 6 Abs. 1 UAbs. 1 lit. b oder f DSGVO stützen kann, missbraucht er das Vertrauen des Verbrauchers, wenn er zusätzlich eine Einwilligung verlangt. Dies wird dem Prinzip von Treu und Glauben aus Art. 5 Abs. 1 lit. a DSGVO nicht gerecht. Obwohl er ihn nach Art. 7 Abs. 3 Satz 3 DSGVO auf sein Widerrufsrecht hinweisen muss, wird er nach einem Widerruf die weitere Datenverarbeitung trotzdem auf der Grundlage des gesetzlichen Erlaubnistatbestands fortführen.

Schließlich könnte für bestimmte Formen der Datenverarbeitung – wie z.B. Profilbildung oder personalisierte Werbung – der Verantwortliche dem Verbraucher mit der Bitte um eine Einwilligung das Recht vorgaukeln, dass er mit diesen Verarbeitungsformen nur nach einem Opt-in rechnen muss. Dieses mindert sich für ihn aber nachträglich zu einem Recht auf Opt-out, wenn der Verantwortliche auf den gesetzlichen Erlaubnistatbestand des überwiegenden berechtigten Interesses wechselt.

Informiert der Verantwortliche den Verbraucher von Anfang an über beide Erlaubnistatbestände – Einwilligung einerseits und Vertragserfüllung oder berechtigte Interessen andererseits – und die mit ihnen verbundenen unterschiedlichen Regelungsregime, gibt er ihm widersprüchliche Informationen und behält sich die Wahl des Erlaubnistatbestands, auf den er sich später berufen will, vor. Dies wäre ein unzulässiges perplexes Verhalten, das nur dazu führen kann, den Verbraucher zu verwirren.

Schließlich haben beide Rechtfertigungen der Datenverarbeitung unterschiedliche Rechtsfolgen. Mit der Einwilligung ist das Recht der betroffenen Person verbunden, eine Datenübertragung nach Art. 20 DSGVO einzufordern. Dies kann für die Entscheidung einzuwilligen bedeutsam sein. Wenn der Verantwortliche die Datenverarbeitung aber auch auf eine Interessenabwägung stützen kann, ist er in der Lage, dem Verbraucher dieses Recht zu nehmen, indem er sich auf den gesetzlichen Erlaubnistatbestand des überwiegenden berechtigten Interesses beruft. Für diesen Anspruch der betroffenen Person sieht Art. 20 DSGVO aber kein Wahlrecht des Verantwortlichen vor.

Alle diese Ungereimtheiten erfordern eine Klarstellung in der Verordnung. Diese kann nur darin bestehen, dass ein Verantwortlicher sich neben einer Einwilligung nicht zusätzlich auf einen gesetzlichen Erlaubnistatbestand berufen kann. Wenn er von der betroffenen Person eine Einwilligung einfordert, muss er sich auch auf die Regeln zu einer Einwilligung einlassen. Er muss

dann vor allem einen Widerruf der Einwilligung gegen sich gelten lassen und kann nicht trotz des Widerrufs die Datenverarbeitung unter Berufung auf einen anderen gesetzlichen Erlaubnistatbestand fortsetzen. Ansonsten suggeriert er dem Verbraucher durch den durch Art. 7 Abs. 3 Satz 3 DSGVO geforderten Hinweis auf das Widerrufsrecht, er könne durch Widerruf die weitere Datenverarbeitung verhindern, obwohl dies aber bei einem bestehenden weiteren gesetzlichen Erlaubnistatbestand faktisch nicht der Fall ist.

Der notwendige Vorrang der Einwilligung sollte nicht nur aus Art. 5 Abs. 1 lit. a DSGVO als einzig faire Form der Datenverarbeitung abgeleitet werden müssen,[59] sondern – zur Rechtssicherheit für alle Beteiligten – in den Text des Art. 6 Abs. 1 UAbs. 1 DSGVO aufgenommen werden.[60] Eine Klarstellung der Formulierung in Art. 6 Abs. 1 UAbs. 1 DSGVO könnte Unsicherheiten abbauen und Missbrauch verhindern.

2.1.5 Bestimmung des Vertragszwecks

Die extrem weite Fassung des Erlaubnistatbestands der „Erfüllung eines Vertrags" kann so genutzt werden, dass der vom Anbieter definierte Vertragszweck auf umfassende Verarbeitungen seiner personenbezogenen Daten im Rahmen eines Persönlichkeitsprofils zielt und die Erhebung einer großen Zahl von Daten erforderlich macht.[61] Hier ist eine Präzisierung des Erlaubnistatbestands zu empfehlen.[62]

Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO erklärt die Verarbeitung personenbezogener Daten für rechtmäßig, die zur Erfüllung eines Vertrages erfolgt, dessen Vertragspartei die betroffene Person ist. Dies schließt auch vorvertragliche Maßnahmen ein, die auf Anfrage der betroffenen Person erfolgen. Der Europäische Datenschutzausschuss weist darauf hin, dass eine Verarbeitung, die nicht zur Erfüllung des Vertrages notwendig ist, auf eine andere Grundlage gestellt werden kann, insbesondere auf lit. a und f, die dem Betroffenen dann auch mitzuteilen ist.[63] Zugleich müsse streng zwischen Einwilligung und Vertragserfüllung differenziert werden, da für diese unterschiedliche Voraussetzungen und Rechtsfolgen gelten. Der Bereich notwendiger Einwilligungen darf nicht durch die Ausweitung des Erlaubnistatbestands des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO eingeschränkt werden.

Die notwendige datenschutzrechtliche Eingrenzung des Erlaubnistatbestands des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO kann nicht allein durch die Kontrolle der Allgemeinen Geschäftsbedingungen (AGB)[64] erreicht werden.[65] Die AGB-Kontrolle schützt den Verbraucher lediglich vor unfairen allgemeinen für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen,

---

59 S. hierzu Kap. 2.1.3.

60 S. hierzu vzbv, 2013, 7.

61 Dieses Problem sieht auch der Europäische Datenschutzausschuss; s. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, v2.0, 8. October 2019, 6 f.

62 S. auch Wendehorst/Graf v. Westphalen, NJW 2016, 3745 (3749 f.), die sich mit einer teleologischen Reduktion behelfen.

63 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, v2.0, 8 October 2019, 7.

64 S. RL 93/13/EWG.

65 So aber Engeler, ZD 2018, 55 (57 f.). Über „erprobte zivilrechtliche Werkzeuge wie die Prüfung von Treuwidrigkeit, Verstoß gegen die guten Sitten und die AGB-Kontrolle" könne eine ausreichende Präzisierung erfolgen (ebd., 60); s. auch Wendehorst/Graf v. Westphalen, NJW 2016, 3745.

die eine überraschende Regelung enthalten (§ 305c BGB) oder den Verbraucher entgegen den Geboten von Treu und Glauben unangemessen benachteiligen (§ 307 Abs. 1 BGB). Dies gilt nach § 307 Abs. 2 Nr. 1 BGB insbesondere, wenn eine AGB-Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren sind. Die AGB-Kontrolle erfasst nach § 305 Abs. 1 Satz 3 BGB jedoch gerade nicht die Bestimmung des individuellen Vertragszwecks – wie weit und wie gezielt auf die Verarbeitung personenbezogene Daten er auch immer ausgerichtet sein mag.

Die notwendige datenschutzrechtliche Eingrenzung verstößt auch nicht gegen den Grundsatz der Privatautonomie und insbesondere den Grundsatz der Vertragsfreiheit. Zwar hat der Verbraucher grundsätzlich die Freiheit, auch in für ihn nachteilige Verträge einzutreten. Daher wird argumentiert, dass das Datenschutzrecht ihm diese Freiheit nicht nehmen dürfe. Das Argument der Freiheit der Vertragsparteien unterliegt jedoch dem Gesetzesvorbehalt. Das Datenschutzrecht schützt die Grundrechte und Freiheiten der betroffenen Person gegen übergroße Machtasymmetrien – vor allem aus Wissensmacht. Insbesondere dann, wenn soziale, rechtliche und sonstige Zwänge zur Nutzung bestimmter Angebote bestehen, bei denen ein weit definierter Vertragszweck den Verbraucher in eine umfassende Verarbeitung seiner personenbezogenen Daten drängen würde, muss die staatliche Schutzpflicht für machtausgleichende Regelungen sorgen. Dieser Schutz fordert eine eingrenzende Bestimmung des Erlaubnistatbestands des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO.

Zur Frage, was für die Erfüllung eines Vertrages erforderlich ist, darf nicht auf die Vertragsformulierung oder auf den Willen des Verantwortlichen abgestellt werden. Ansonsten könnte der Verantwortliche den Vertragstext so formulieren oder den Vertragsgegenstand und den Vertragszweck so bestimmen, dass er jede von ihm gewünschte Datenverarbeitung durchführen kann – z.B. auch Datenverarbeitungen zu Werbemaßnahmen, zur Profilbildung, zur Weitergabe von Daten an Dritte, zur Durchführung von Sicherungsmaßnahmen, zur Erhebung der Kundenzufriedenheit, zur Verbesserung der Waren und Dienste und vieles mehr. Diese Zusatzzwecke sollen nur nach einer Einwilligung der betroffenen Person oder nach der umfassenden und dokumentierten Abwägung der berechtigten Interessen der Verantwortlichen mit den Interessen und Freiheiten der betroffenen Person eine Datenverarbeitung rechtfertigen können. Daher fordert der Ausschuss, für die Zulässigkeit der Datenverarbeitung nach lit. b auf die objektive Erforderlichkeit der Datenverarbeitung für den Hauptzweck des Vertrags abzustellen.[66] Es kann nicht auf das bloße Vorhandensein einer Vertragsklausel ankommen, die der betroffenen Person unilateral auferlegt wird.[67] Entscheidend muss sein, dass die Vertragsleistung funktional ohne die Verarbeitung der relevanten personenbezogenen Daten nicht erbracht werden kann.[68]

Dies sollte zur Rechtssicherheit für alle Beteiligten im Text des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO klargestellt werden. Ohne Klarstellung, dass die funktional objektive Erforderlichkeit der Datenverarbeitung für den zentralen Vertragszweck entscheidend ist, wird es über die Reichweite des Erlaubnistatbestands des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO immer wieder zu

---

66 Draft Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version for public consultation, 9.4.2019, 7 f.

67 Unter Verweis auf Stellungnahme 6/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 21 f.

68 S. hierzu auch Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2019, 8.

interessengeleiteten Streitereien kommen. Die dadurch verursachte Rechtsunsicherheit wird den Vollzug des Datenschutzes erheblich behindern.

2.1.6 Verarbeitung der Daten von Kindern

Sehr oft wenden sich Verantwortliche direkt an Kinder und verarbeiten deren Daten auf vielfältige Weise und speichern diese für lange Zeit. Die gilt insbesondere für die Nutzung von Social Networks und Angebote im E-Commerce, die sich an Kinder richten. Z.B. nutzten in der Altersgruppe der 6- bis 13-jährigen im Jahr 2016 57% der Kinder WhatsApp, 50% YouTube und 30% Facebook mehrmals in der Woche oder am Tag.[69] Das durchschnittliche Alter der Erstanmeldung bei Facebook lag 2016 bei 10 Jahren.[70] 2018 nutzten z.B. 73% der 14- bis 17-Jährigen Instagram.[71] Die Datenverarbeitung von Kindern ist somit im Internet keine Ausnahme sondern ein Massenphänomen.[72] Kinder sind aber in einer spezifischen Situation: Sie verstehen die meist langfristigen Nachteile der Verarbeitung ihrer personenbezogenen Daten noch unzureichend, sind aber für die meist kurzfristigen positiven Effekte der Nutzung von Internet-Diensten sehr offen und für Verführungen zu ihrer Nutzung leicht zugänglich. Diese jungen Verbraucher bedürfen daher eines besonderen Schutzes.

Diese besondere Schutzpflicht berücksichtigt auch die Datenschutz-Grundverordnung in vielen Zusammenhängen – allerdings nicht in allen notwendigen Aspekten.

Berücksichtigt hat die Datenschutz-Grundverordnung die besondere Schutzbedürftigkeit von Kindern z.B. in folgenden Zusammenhängen:

- Nach Art. 8 Abs. 1 Satz 1 DSGVO gilt die Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, schon als rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Nach Art. 8 Abs. 1 Satz 1 DSGVO dürfen Mitgliedstaaten diese Grenze sogar auf das dreizehnte vollendete Lebensjahr senken. In anderen Fällen ist das Kind erst mit Volljährigkeit einwilligungsfähig.
- Nach Art. 6 Abs. 1 UAbs. 1 Satz 1 lit. f DSGVO muss eine Interessenabwägung die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person in besonderer Weise berücksichtigen, „wenn es sich bei der betroffenen Person um ein Kind handelt".[73]
- Nach Art. 12 Abs. 1 Satz 1 DSGVO sind Informationen nach Art. 13 und 14 DSGVO sowie Mitteilungen nach Art. 15 DSGVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln". Dies soll umso mehr für Informationen gelten, die sich speziell an Kinder richten.[74]
- Eine Löschung personenbezogener Daten hat nach Art. 17 Abs. 1 lit. f. DSGVO zu erfolgen, wenn die Daten aufgrund einer Einwilligung von einem Kind nach Art. 8 Abs. 1 DSGVO erhoben worden sind.

---

69 MPFS, KIM-Studie 2016, 33.
70 MPFS, KIM-Studie 2016, 41.
71 MPFS, KIM-Studie 2018,39.
72 S. ähnliche Zahlen in BITKOM, 2017, 8.
73 Hier sieht die Bundesregierung einen Bedarf an Konkretisierung – Bundesregierung, 2019, 12.
74 Hier verweist die Artikel 29-Datenschutzgruppe auf die Konvention über die Rechte des Kindes – Für Kinder erklärt des Kinderhilfswerks der Vereinten Nationen als gelungenes Beispiel für kindgerechte Sprache; Leitlinien für Transparenz, WP 260 rev.01, 12.

- Für Verhaltensregeln sind nach Art. 40 Abs. 2 lit. g DSGVO „Unterrichtung und Schutz von Kindern“ ein möglicher Regelungsgegenstand.

Das sind allerdings nicht alle Situationen, in den der besondere Schutz von Kindern erforderlich ist oder ihre besonderen Interessen zu berücksichtigen sind. Daher sollte der Wortlaut der Verordnung z.B. in folgenden Vorschriften diesen besonderen Aspekt zusätzlich und ausdrücklich berücksichtigen:

- Die Prüfung der Vereinbarkeit eines neuen Verarbeitungszwecks mit dem bisherigen Verarbeitungszweck nach Art. 6 Abs. 4 DSGVO sollte auch berücksichtigen, wenn die Daten eines Kindes für einen anderen Zweck verwendet werden sollen.
- In den Normtext des Art. 8 DSGVO sollte die Wertung des Erwägungsgrunds 38 Satz 2 DSGVO übernommen werden: „Ein solch besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen.“
- Von der Ausnahme des Verbots der Verarbeitung besonderer Kategorien von personenbezogenen Daten bei einer Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO sollte die Einwilligung eines Kindes ausgenommen werden.
- Nicht nur bei der Forderung nach Löschung, sondern auch beim Widerspruch nach Art. 21 Abs. 1 DSGVO sollte es in besonderer Weise berücksichtigt werden, wenn die personenbezogenen Daten im Kindesalter erhoben worden sind.
- Von der Ausnahme des Verbots der Verarbeitung personenbezogener Daten bei einer automatisierten Entscheidung aufgrund einer Einwilligung nach Art. 22 Abs. 2 lit. c DSGVO sollte die Einwilligung eines Kindes ausgenommen werden.[75] Die Wertung von Erwägungsgrund 71 Satz 5 DSGVO („Diese Maßnahme sollte kein Kind betreffen“) sollte sich im Normtext wiederfinden. Die Einwilligung des Erziehungsberechtigten bleibt allerdings weiterhin möglich.
- Bei der datenschutzgerechten Systemgestaltung nach Art. 25 Abs. 1 DSGVO[76] sollte der Schutz der Grundrechte und Interessen von Kindern in besonderer Weise gefordert werden. Gerade bei der Systemgestaltung wäre ein grundlegender Schutz von Kindern - vor allem in Social Networks – besonders wichtig- und meist leicht zu realisieren.
- Auch bei der datenschutzfreundlichen Voreinstellung nach Art. 25 Abs. 2 DSGVO[77] sollte der Schutz von Kindern in besonderer Weise gefordert werden. Sie übernehmen – mehr noch als Erwachsene – die voreingestellten Werte und konzentrieren sich allein auf die Nutzung des Geräts oder des Dienstes. Diese spezifische Voreinstellung für Kinder ist vor allem für Social Networks wichtig.

---

75 Noch weitergehender vzbv, 2013, 17.
76 S. hierzu allgemein Kap. 2.1.12.
77 S. hierzu allgemein Kap. 2.1.13.

- In der Datenschutzfolgenabschätzung nach Art. 35 DSGVO sollte sowohl bei der Risikoanalyse als auch bei den Schutzmaßnahmen dem Schutz der Grundrechte und Interessen von Kindern eine besondere Aufmerksamkeit entgegengebracht werden.[78]

Diese Schutzregelungen können mit geringem Aufwand aber hoher Wirkung in den Text der jeweiligen Vorschrift aufgenommen werden. Über die besondere Schutzbedürftigkeit von Kindern dürfte auch kein politischer Streit entstehen.

2.1.7 Informationspräsentation

Die Informationspflichten wurden in Art. 13 und 14 DSGVO im Vergleich zu den Vorgängerregelungen der Datenschutzrichtlinie zwar inhaltlich ausgeweitet, aber an vielen Stellen sehr unscharf umschrieben. Vom Zweck der Informationspflichten, dem Verbraucher die Wahrnehmung seiner Rechte zu ermöglichen, sollten in der Form weiterentwickelt und im Inhalt präzisiert werden. Eine intensivere Überarbeitung ist für den Text der Informationspflichten nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO erforderlich.

2.1.7.1 Interessengerechte und an der Aufnahmekapazität ausgerichtete Information

Aus Verbrauchersicht von besonderer Relevanz ist zunächst die Form der Informationsvermittlung. Die Ausgestaltung der Information stellt für Verbraucher regelmäßig eine signifikante Hürde dar, tatsächlich Umfang und Tragweite einer Datenverarbeitung zu erfassen. Nach Art. 12 Abs. 1 Satz 1 DSGVO sind Informationen nach Art. 13 und 14 DSGVO sowie Mitteilungen nach Art. 15 DSGVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“. Dies soll umso mehr für Informationen gelten, die sich speziell an Kinder richten.[79] In der Praxis ergeben sich hier zwei Problemkreise. Einerseits werden entsprechende Erklärungen unter Umständen in Sprache und Form bewusst so gestaltet, dass sie beschwichtigend auf aktive oder potenzielle Nutzer wirken. Andererseits ist die Datenverarbeitung auch bei bestem Willen des Verantwortlichen, die betroffenen Personen bestmöglich zu informieren, unter Umständen so komplex, dass eine leicht zu erfassende Darstellung nicht gelingt. Um den Zweck des Grundrechtsschutzes durch Information zu erreichen, müssten die Informationen so angeboten werden, dass sie den jeweiligen Interessen und der jeweiligen Aufnahmekapazität der betroffenen Person entsprechen. Sie müssten daher in unterschiedlichem Umfang und unterschiedlichen Konkretisierungsstufen (z.B. Icon, Informationen auf einer einzigen Seite oder umfangreiche Darstellung), die die betroffene Person wählen kann, präsentiert werden. Sie müsste somit der Nutzungssituation angemessen in unterschiedlichen Modi zur Verfügung gestellt werden. Dies wird so von Art. 12 DSGVO nicht ausdrücklich gefordert.

2.1.7.2 Mediengerechte Information

Die Übermittlung der Information sollte praktikabel sein. Sie soll zwar grundsätzlich im gleichen Medium übermittelt werden, wie die Datenerhebung erfolgt. Ein Medienbruch bei der Information sollte jedoch dann zulässig sein, wenn das Ausgangsmedium keinen Raum für eine

---

78 Anders noch der Kommissionsentwurf in Art. 32 Abs. 2 lit. d.

79 Hier verweist die Artikel 29-Datenschutzgruppe als auf die Konvention über die Rechte des Kindes – Für Kinder erklärt des Kinderhilfswerks der Vereinten Nationen als gelungenes Beispiel für kindgerechte Sprache; Leitlinien für Transparenz, WP 260 rev.01, 12.

ausreichende Information lässt oder keine geeignete Information ermöglicht. Dies kann etwa der Fall sein, wenn auf einem analogen Datenträger nicht alle notwendigen Informationen Platz haben und daher ergänzend ein Weblink auf die fehlenden Informationen verweist. Gleichzeitig darf der Medienbruch nicht zu einer Umgehung von Informationspflichten missbraucht werden oder dem Verbraucher die Informationserlangung erschweren. Dabei ist auch die jeweilige Adressatengruppe und deren Technikaffinität zu berücksichtigen. Ein Medienbruch wäre damit nur unter engen Voraussetzungen zulässig und entsprechend begründungspflichtig.

2.1.7.3 Situationsadäquate Information

Um ihren gesetzlichen Zweck zu erfüllen, müssten die Informationen situationsadäquat, also dann gegeben werden, wenn der Verbraucher eine Entscheidung zu treffen hat – z.B. unmittelbar vor einer Einwilligung, vor der Nutzung eines Dienstes oder vor der Übertragung von Daten. Nach Art. 13 Abs. 1 DSGVO müssen die Daten „zum Zeitpunkt der Erhebung" mitgeteilt werden. In der bisherigen Praxis erfolgt die Mitteilung meist bei Vertragsabschluss oder beim ersten Kontakt mit der betroffenen Person. Dabei werden in Form von Datenschutzerklärungen oder Allgemeinen Geschäftsbedingungen alle Eventualitäten künftiger Datenverarbeitungen beschrieben.[80] Die Mitteilung kann dadurch Jahre vor der Datenerhebung liegen. Keine betroffene Person wird sich an die umfassenden Inhalte dieser Mitteilung erinnern, wenn die Daten tatsächlich erhoben werden. Diese Praxis entspricht nicht der Forderung, die Informationen „zum Zeitpunkt der Erhebung" mitzuteilen. Die Mitteilung muss vielmehr zum richtigen Zeitpunkt erfolgen: zum Zeitpunkt der Datenerhebung und – aus dem Blickwinkel der Selbstbestimmung – vor einer notwendigen oder möglichen Entscheidung der betroffenen Person. Dies sollte im Normtext dadurch zum Ausdruck gebracht werden, dass die *relevante* Information *jeweils* zum Zeitpunkt der Erhebung dieser Daten" erfolgt.

Eng mit dem Zweck der Information für den Grundrechtsschutz hängt die Frage zusammen, wie gesichert werden kann, dass die Informationen für die betroffene Person handlungsrelevant sind. Dies ist die für die Selbstbestimmung letztlich die entscheidende Frage. In einer Situation extremer Machtasymmetrie oder in einem Anschluss an eine Infrastruktur (Take it or Leave it) gibt es für die betroffene Person keine Selbstbestimmung hinsichtlich der Datenverarbeitung, wenn sie auf die Leistung der anderen Seite angewiesen ist. Daher kommt es darauf an, künftige Datenverarbeitungssysteme so zu gestalten, dass für die betroffene Person ein hohes Maß an Auswahlmöglichkeiten besteht. Dies ist eine zentrale Aufgabe der von Art. 25 Abs. 1 DSGVO geforderten Gestaltung der Funktion des Datenverarbeitungssystems.[81]

Die Leitlinien der Artikel 29-Datenschutzgruppe für Transparenz[82] geben zwar wertvolle Hilfestellungen zur Auslegung der Art. 12 ff. DSGVO, jedoch ist die Befolgung der dort formulierten Praxis noch deutlich verbesserungsbedürftig. Präzision und Redlichkeit bei der Information sind aber zentral, da der Verbraucher sonst nur schwer abschätzen kann, welche Reichweite seine Einwilligung hat, welche Datenverarbeitung ihn betrifft und welche Rechte er geltend machen kann. Bleibt der Verantwortliche hier vage, indem er beispielhaft verkürzt, anstatt vollständige Angaben zu machen, oder angibt, dass „möglicherweise" mit bestimmten Handlungen

---

80 S. z.B. Dorfleitner/Hornuf 2018, 2, 4 für die FinTech-Unternehmen in Deutschland.

81 S. hierzu Kap. 2.1.12.

82 Artikel 29-Datenschutzgruppe, Leitlinien für Transparenz, WP 260 rev.01.

seinerseits zu rechnen ist, anstatt definitive Angaben zu präsentieren, so können die mit den Transparenzpflichten der Grundverordnung verfolgten Ziele nicht erreicht werden. Es sollte im Text des Art. 12 DGSVO festgehalten werden, dass sich die Information auf die gegenwärtig vorgesehene Datenverarbeitung beziehen muss. Künftige Änderungen in der Datenverarbeitung sollten zu neuen, dann wiederum aktuellen, Informationen führen. Es sollte ausdrücklich nicht zulässig sein, seine Informationspflicht zu erfüllen, indem alle denkbaren künftigen Datenverarbeitungen mit vagen Hinweisen auf künftige Möglichkeiten in eine einmalige Information aufgenommen werden.

2.1.7.4 Information durch Bildsymbole

Art. 12 Abs. 7 DSGVO sieht die Möglichkeit vor, die bereitzustellenden Informationen mit standardisierten Bildsymbolen zu kombinieren. Trotz initialer Rückschläge bei der Frage der konkreten Gestaltung dieser Bildsymbole stellt diese Neuerung einen äußerst begrüßenswerten Ansatz dar, in dem großes Potential steckt. Er sollte deshalb konsequent weiterverfolgt werden. In die gleiche Richtung geht letztlich die Etablierung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen.[83] Hier geht es darum, den Verbraucher zu entlasten, der sich eine eigene Überprüfung der durch den Verantwortlichen bereitgestellten Informationen ersparen kann, wenn diese nachgewiesener Weise bereits durch einen vertrauenswürdigen Dritten erfolgt ist.

2.1.7.5 Technik- und bereichsspezifische Informationen

Außerdem sollte die Information für spezielle Anwendungsbereiche und Technologien bereichsspezifisch geregelt werden. Dies könnte im Rahmen von Verordnungen geschehen, die bereichsspezifisch etwa die Datenverarbeitung im intelligenten Fahrzeug regeln.[84] Der technologieneutrale Ansatz der Datenschutz-Grundverordnung gerät hier an seine Grenzen.

2.1.8 Informationspflichten des Verantwortlichen

Bezogen auf konkrete Informationspflichten des Verantwortlichen zu Beginn der Datenverarbeitung sind einige Kritikpunkte zu erörtern.

2.1.8.1 Informationen über Empfänger

In Art. 13 Abs. 1 lit. e und Art. 14 Abs. 1 lit. e DSGVO sollte die Formulierung aufgenommen werden, dass über „die Empfänger, *soweit sie bestimmbar sind*, oder Kategorien von Empfängern der personenbezogenen Daten“ zu informieren ist. Da die personenbezogenen Daten sehr oft weitergegeben werden, kann die betroffene Person ihre Rechte nur dann effektiv geltend machen, wenn sie die Empfänger kennt.[85] Soweit der Verantwortliche die Empfänger, denen er die Daten der betroffenen Person weitergibt, kennen kann, sollte er diese der betroffenen Person mitteilen, damit diese auch den Datenempfängern gegenüber ihre Rechte geltend machen kann. Für den Verantwortlichen ist dies ein geringer Mehraufwand, für die betroffenen Personen aber

---

83 S. zum Stand der Einführung solcher Verfahren Maier/Bile, DuD 2019, 478.

84 S. hierzu Husemann, in: Roßnagel/Hornung, 2019, 367 ff.

85 Dies findet in Deutschland selten statt – s. z.B. Dorfleitner/Hornuf 2018, 2, 26 ff. für die FinTech-Unternehmen in Deutschland.

die Grundvoraussetzung, um von ihren Rechten nach der Datenschutz-Grundverordnung überhaupt Gebrauch machen zu können.

2.1.8.2 Konflikt zwischen rechtlich geschützten Geheimnissen und Informationspflicht

Probleme bereitet auch die Information im Kontext von automatisierter Entscheidungsfindung im Einzelfall gemäß Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO. Die Reichweite der Informationspflicht wie auch des Auskunftsrechts nach Art. 15 Abs. 1 lit. h DSGVO bezogen auf Art. 22 Abs. 1 und 4 DSGVO umfasst dabei „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person". Diese zunächst weit erscheinende Formulierung erfährt durch Erwägungsgrund 63 Satz 5 DSGVO jedoch eine einschränkende Auslegung. So sollen insbesondere Geschäftsgeheimnisse und Rechte des geistigen Eigentums nicht dem Auskunftsrecht unterfallen. Zwar stellt Erwägungsgrund 63 Satz 6 DSGVO klar, dass das Vorliegen eines Geschäftsgeheimnisses oder geistigen Eigentums nicht dazu führen darf, dass der betroffenen Person jegliche Auskunft verweigert wird. Dies beinhaltet jedoch nur eine Grenzziehung nach unten, dass eine Information der betroffenen Person nicht vollständig entfallen darf. Wie der Konflikt zwischen Informationsanspruch und Geheimnisschutz oberhalb dieser Grenze gelöst werden soll, lässt die Datenschutz-Grundverordnung offen und gibt die Entscheidung damit in die Hand des Verantwortlichen. Hier ist eine Abwägung des Gesetzgebers notwendig, der zumindest eine Grundregel für die Auflösung des Konflikts festlegen müsste. Diese könnte zum Beispiel so lauten, dass – unter Wahrung des Geschäftsgeheimnisses oder des geistigen Eigentums – dennoch ein möglichst hohes Maß an Information bereitgestellt werden muss. Hier könnten Überlegungen ansetzen, in der Praxis die bereitzustellenden Informationen im Bereich des Geheimnisses zu „verrauschen" und so etwa geheim zu haltende Bestandteile des Entscheidungsverfahrens zu schützen, gleichzeitig aber ein Maximum an Information zu ermöglichen.[86]

2.1.8.3 Informationen über automatisierte Entscheidungsverfahren

Der Verantwortliche hat „aussagekräftige" Informationen „über die involvierte Logik sowie die Tragweite" für die betroffene Person zu geben. Über den Umfang und die Tiefe dieser Information ist großer Streit entbrannt. Hier sollte in einer Überarbeitung der Vorschrift klargestellt werden, dass die Information über die Tragweite auch die rechtlichen und tatsächlichen Auswirkungen auf die betroffene Person umfasst. Hinsichtlich der Information über die „involvierte Logik" müssen auch die abstrakten Kriterien[87] für die Entscheidung und ihre Gewichtung enthalten sein.[88] Die betroffene Person muss nach der Information in der Lage sein, ihr Verhalten so anzupassen, dass sie die entscheidenden Kriterien erfüllt oder zumindest konkret nachvollziehen kann, warum die Entscheidung nicht zu ihren Gunsten ausfällt.[89] Nur so kann verhindert

---

86 S. z.B. Bäcker, in: Kühling/Buchner, 2018, Art. 13 Rn. 54 unter Verweis auf Kugelmann, DuD 2016, 566 (568).

87 Im Gegensatz zur Auskunft nach Art. 15 Abs. 1 lit. h DSGVO – s. Kap. 2.1.9.2.

88 Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 30; vzbv, 2013, 13; vzbv, Algorithmenkontrolle, 2019, 13.

89 Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 28.

werden, dass sie als Persönlichkeit einem für sie unverständlichen algorithmenbasierten System unterworfen wird.

Aussagekräftig sind die Informationen, wenn sie in der Lage sind, bei der betroffenen Person das genannte Verständnis hervorzurufen. Dies fordert vom Verantwortlichen, „einfache Möglichkeiten [zu] finden, die betroffene Person über die der Entscheidungsfindung zugrunde liegenden Überlegungen bzw. Kriterien zu informieren".[90] Komplexität ist „keine Entschuldigung" für mangelhafte Information. Dies dürfte gerade bei selbstlernenden Systemen eine Herausforderung für den Verantwortlichen darstellen. Gerade deshalb sollte diese Klarstellung zumindest in einen Erwägungsgrund aufgenommen werden.

An dem Eingriff in das Datenschutzrecht und die informationelle Selbstbestimmung der betroffenen Person ändert sich gar nichts, wenn die automatisierte Entscheidung arbeitsteilig getroffen wird. Daher darf eine Arbeitsteilung nicht dazu führen, dass die Information unterbleibt oder verkürzt erfolgt. Findet das arbeitsteilige automatisierte Entscheidungsverfahren in einem Auftragsverhältnis nach Art. 28 DSGVO statt, hat der Auftraggeber die umfassende Information zu geben. Findet das arbeitsteilige automatisierte Entscheidungsverfahren durch mehrere Kooperationspartner statt, sollte jeder über den Teil samt den Schnittstellen zu allen anderen Teilen informieren, den er verantwortet. Dies sollte in der Vorschrift festgehalten werden.

Im Ergebnis darf eine arbeitsteilige Durchführung der automatisierten Entscheidung etwa in der Form, dass die Auskunftei A ein Verbraucherprofil erstellt, aus dem der Bonitätsprüfer B einen Score-Wert errechnet, der im Kreditvergabesystem des Online-Händlers C zu einem Verbraucherkredit oder einer bestimmten Bezahlweise führt,[91] nicht dazu führen, dass Informationslücken für die betroffene Person entstehen. In diesem Fall muss es so sein, dass alle drei Verantwortlichen die betroffene Person über ihren jeweiligen Beitrag zum automatisierten Entscheidungsverfahren informieren müssen, ganz gleich ob sie die eigentliche Entscheidung treffen oder diese lediglich vorbereiten. Dies muss die Vorschrift klarstellen.

Inhaltliche Erweiterungen würde die Vorschrift indirekt erfahren, wenn das Verbot des Art. 22 Abs. 1 den Vorschlägen dieses Gutachtens entsprechend erweitert würde.[92]

2.1.8.4 Information über Profiling

Profiling ist in Art. 4 Nr. 4 DSGVO definiert und in Art. 22 Abs. 1 DSGVO sowie in Art. 13 Abs. 2 lit. f, 14 Abs. 2 lit. g und 15 Abs. 12 lit. h DSGVO in der eigentümlichen Form „einschließlich Profiling" erwähnt. Profiling hat in der Datenschutz-Grundverordnung jedoch keine eigenständige Regelung erfahren, obwohl dies nach dem risikobasierten Absatz der Verordnung erforderlich gewesen wäre. Profiling als automatisierte Sammlung von Persönlichkeitsmerkmalen zur Bewertung einer betroffenen Person ist ein tiefer Eingriff in die Grundrechte auf Datenschutz und informationelle Selbstbestimmung. Von solchen Bewertungsprofilen gehen insbesondere für Verbraucher besondere, über die normale Verarbeitung personenbezogener

---

90 Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 28.

91 S. ähnlich Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 28.

92 S. näher Kap. 2.1.11.

Daten hinausgehende Risiken für die freie Entfaltung und Entscheidung und die gerechte Beurteilung aus. Daher sollte die betroffene Person zumindest über jedes Profiling informiert werden, auch wenn dieses nicht unmittelbar mit einer automatisierten Entscheidung verbunden ist, sondern für andere Bewertungszwecke verwendet wird.[93] Daher sollten die Vorschriften der Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g dahingehend ausgeweitet werden, dass über jede automatisierte Entscheidung und über jedes Profiling informiert werden muss.[94]

2.1.9 Das Auskunftsrecht der betroffenen Person

Ähnlich wie für die Informationspflichten sind die Informationen, die zur Erfüllung des Auskunftsrechts nach Art. 15 DSGVO zu geben sind, zu präzisieren, um die grundrechtsschützende Funktion des Auskunftsrechts zu wahren.

2.1.9.1 Auskunft über Empfänger

Das Gleiche, wie zu Art. 13 Abs. 1 lit. e und Art. 14 Abs. 1 lit. e DSGVO hinsichtlich der Empfänger von personenbezogenen Daten aufgeführt, gilt erst recht bei einem Auskunftsanspruch nach Art. 15 Abs. 1 lit. c DSGVO.[95] Die Auskunft soll der betroffenen Person die Informationen verschaffen, um ihre Rechte nach der Datenschutz-Grundverordnung wahrnehmen zu können.[96] Hierzu gehört in erster Linie die Identität aller Verantwortlichen, um ihnen gegenüber ihr Recht gelten machen zu können. Wenn der Verantwortliche, gegenüber dem die betroffene Person ihr Auskunftsrecht geltend macht, durch die Weitergabe der Daten dafür verantwortlich ist, dass die Empfänger auch zu Verantwortlichen geworden sind, die Daten der betroffenen Person verarbeiten, dann ist es auch gerechtfertigt, von ihm die Mitteilung zu verlangen, an wen er die Daten weitergeleitet hat. Denn diese Weiterleitung ist ein gesonderter Eingriff in das Grundrecht auf Datenschutz der betroffenen Person. Dieser Eingriff mag gerechtfertigt sein, eventuell auch die weitere Datenverarbeitung durch den Empfänger. Aber die betroffene Person sollte in der Lage sein, dies zu überprüfen. Der Verantwortliche sollte daher verpflichtet sein, alle Empfänger der personenbezogenen Daten zu protokollieren und der betroffenen Person das sie betreffende Protokoll bekanntzugeben.

2.1.9.2 Auskunft über automatisierte Entscheidungsverfahren

Nach Art. 15 Abs. 1 lit. h DSGVO hat die betroffene Person einen Anspruch auf „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“. Im Gegensatz zur Information nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO,[97] die die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen nur abstrakt beschreiben muss, ist die Auskunft über diese Themen personenspezifisch zu erteilen. Diese Auskunft muss um die relevanten Merkmale und deren Bedeutung für die automatisierte oder automatisiert vorbereitete

93 S. z.B. auch Martini, 2019, 10.
94 Zu weiteren Regelungsvorschlägen hinsichtlich algorithmenbasierter Systeme s. Kap. 2.1.11.
95 S. hierzu auch vzbv, 2013, 12.
96 S. z.B. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit 2019, 76.
97 S. Kap. 2.1.8.3.

Entscheidung ergänzt werden. Nur mit dieser Information kann die betroffene Person ihr Verhalten so einrichten, dass sie Chancen hat, die gewünschte Entscheidung zu erreichen.[98]

Eine gesonderte Information sollte nach einem geänderten Art. 15 Abs. 1 lit. h DSGVO der betroffenen Person auch für jedes Profiling, dessen Umfang, Inhalt, Zielsetzung und Verwendungszweck gegeben werden müssen.[99]

2.1.9.3 Recht auf Erhalt einer Kopie

Nach Art. 15 Abs. 3 Satz 1 DSGVO hat der Verantwortliche der betroffenen Person auf Antrag „eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung" zu stellen.[100] Kaum eine Regelung in der Datenschutz-Grundverordnung ist so misslungen und daher umstritten.[101] Dies beginnt schon mit der Frage, ob das „Recht auf Erhalt einer Kopie" (Art. 15 Abs. 4 DSGVO) ein eigenständiger Anspruch der betroffenen Person ist[102] oder nur eine Form der Auskunft nach Art. 15 Abs. 1 DSGVO.[103] Der Streit geht weiter mit der Frage, was eine Kopie ist,[104] ob diese eine umfassende Wiedergabe aller zu einer betroffenen Person vorhandenen Datensätze beinhalten muss,[105] welcher „Gegenstand der Verarbeitung" kopiert werden muss[106] und endet nicht in den Problemen, ob der Anspruch auf eine Kopie eigens geltend gemacht werden muss[107] oder nicht[108] sowie in welcher Form die Kopie übergeben werden muss.[109]

Dieses „Recht auf Erhalt einer Kopie" ist vom Ansatz her eine sinnvolle Lösung:[110] Der Verantwortliche wird durch eine schlichte Kopie eines Datensatzes nur wenig belastet.[111] Eine Mitteilung aller verarbeiteten Daten ist dann nicht notwendig. Für die betroffene Person gibt die „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind," eine geeignete

98 S. auch Kap. 2.1.9.

99 S. hierzu auch Kap. 2.1.11.

100 Hier sieht auch die Bundesregierung einen Konkretisierungsbedarf – Bundesregierung, 2019, 13.

101 S. z.B. Zikesch/Sörup, ZD 2019, 239 (239, 243); Wybitul, ZD 2019, 278; Lapp, NJW 2019, 345 (347); Härting, CR 2019, 219 (221 ff.); Engeler/Quiel, NJW 2019, 2201.

102 So z.B. Bäcker, in Kühling/Buchner, 2018, Art. 15 Rn. 39; Schwartmann/Klein, in: Schwartmann u.a., 2018, Art. 15 Rn. 34; Spindler, DB 2016, 937 (944); Härting, CR 2019, 219 (220); Engeler/Quiel, NJW 2019, 2201 (2202).

103 So z.B. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 77 f.; Bayerisches Landesamt für Datenschutz, 2019, 46; Raith 2019, 223 f.; Paal, in: Paal/Pauly, 2018, Art. 15 Rn. 33; Franck, in: Gola, 2018, Art. 15 Rn. 27; Specht, in: Sydow, 2018, Art. 15 Rn. 18; Veil, in: Gierschmann/Schlender/Stenzel, 2018, Art. 15 Rn. 209; Zikesch/Sörup, ZD 2019, 239 (240); Wybitul, ZD 2019, 278 (279).

104 S. z.B. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 77 f.; Härting, CR 2019, 219 (221 ff.); Engeler/Quiel, NJW 2019, 2201 (2202 f.).

105 So z.B. Dix, in: Simitis/Hornung/Spiecker, 2019, Art. 15 Rn. 36; Engeler/Quiel, NJW 2019, 2201 (2203); a.A. Dausend, ZD 2019, 103; Zikesch/Sörup, ZD 2019, 239 (243); Specht, in: Sydow, 2018, Art. 15 Rn. 18; Wybitul 2016, Kap. IV, Rn. 166.

106 S. z.B. Härting, CR 2019, 219 (222).

107 S. z.B. Bäcker, in Kühling/Buchner, 2018, Art. 15 Rn. 39.

108 S. z.B. Dix, in: Simitis/Hornung/Spiecker, 2019, Art. 15 Rn. 29; Ehmann, in: Ehmann/Selmayr, 2018, Art. 15 Rn. 25; Engeler/Quiel, NJW 2019, 2201 (2205).

109 S. z.B. z.B. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 78. Engeler/Quiel, NJW 2019, 2201 (2204).

110 A.A. IHK München und Oberbayern, 2019, 1.

111 S. den Hinweis des Erwägungsgrunds 63 DSGVO auf die Verwendung von Datendownloadtools. Diese werden von Social-Media-Anbieter überwiegend angewendet – s. zu den unzureichenden Ergebnissen jedoch Scheibel/Horn/Öksüz, 2018, 13 ff.

Prüfgrundlage für die Fragen, welche Daten von ihr in welchem Verarbeitungszusammenhang verarbeitet werden und ob diese Datenverarbeitung rechtmäßig ist. Allerdings kann eine Kopie der verarbeiteten Daten eine Erläuterung erforderlich machen, wenn sie für die betroffene Person ansonsten nicht verständlich wäre.

Umstritten ist jedoch, was eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind," sein kann. Dies ist leicht zu beantworten, soweit die Daten der betroffenen Person in einem Datensatz oder in einem Dateiordner gespeichert sind, wie dies etwa ein Account, eine Personalakte, eine Kunden- oder eine Krankenakte, ein Persönlichkeitsprofil oder ähnlich geschlossene Datensammlungen sind. Schwierig ist es jedoch die „personenbezogenen Daten, die Gegenstand der Verarbeitung sind", von anderen Daten, auf deren Kenntnis die betroffene Person kein Recht hat, abzugrenzen, wenn sie mit anderen Daten in Geschäftsvorgängen, Protokollen, Logdateien, Backup-Dateien, Kommunikationsverläufen, Infrastruktur- oder Geräteprozessen verarbeitet werden, die nicht nach betroffenen Personen geordnet sind und auch nicht nach diesen strukturiert werden können.[112] Dass ein Datum der betroffenen Person in einem Geschäftsvorgang vorkommt, kann nicht dazu führen, ihr den gesamten – unter Umständen sehr umfangreichen – Geschäftsvorgang in Kopie zur Kenntnis zu geben. Die Rechtsunsicherheit, wo die Grenze des berechtigten Anspruchs auf eine Kopie liegt, führt dazu, dass betroffene Personen davor zurückschrecken, dieses Recht in Anspruch zu nehmen, und dass Verantwortliche sich weigern, diesen Anspruch zu erfüllen. Daher ist es notwendig, dass das Recht auf eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind", in einer Weise präzisiert wird, dass es in der Praxis handhabbar wird, und der Verbraucher in die Lage versetzt wird, es gezielt in Anspruch zu nehmen.

Kann der Verantwortliche keine Kopie zur Verfügung stellen, ist eine strukturierte, aufgearbeitete Liste aller verarbeiteten Daten notwendig, damit die betroffene Person überprüfen kann, ob die über sie gespeicherten Daten korrekt sind und ihre Verarbeitung durch den angegebenen Erlaubnistatbestand erlaubt ist. Die Angabe der Kategorien personenbezogener Daten, die verarbeitet werden, nach Art. 15 Abs. 1 lit. b DSGVO kann dann nicht ausreichen. Für diese Fälle ist Abs. 1 um die Angabe der verarbeiteten Daten zu ergänzen. In bestimmten Fällen, in denen die Kopie eines Dokuments oder eines Auszugs aus einem komplexen Datensatzes notwendig ist, um die Rechtmäßigkeit der Datenverarbeitung zu überprüfen, ist eine solche Kopie oder ein solcher Auszug vorzulegen.[113]

Durch diese Klarstellung sowie die im folgenden Kapitel vorgeschlagene Klarstellung zum Anwendungsbereich des Rechts auf Datenübertragung nach Art. 20 DSGVO würde auch den Unterschied zwischen der Übermittlung einer Kopie und der Übertragung von Daten der betroffenen Person verdeutlichen:[114] Die Kopie würde die der betroffenen Person zugeordnete Datensammlung betreffen, unabhängig davon, ob die betroffene Person die Daten „bereitgestellt" hat und unabhängig davon, auf welcher Rechtsgrundlage die Daten verarbeitet werden. Dagegen besteht das Recht auf Datenübertragung nur unter zwei Voraussetzungen, die für das Recht auf

---

112 S. z.B. Zikesch/Sörup, ZD 2019, 239

113 Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 78; Zikesch/Sörup, ZD 2019, 239 (243).

114 Dies übersehen z.B. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 77 f.; Zikesch/Sörup, ZD 2019, 239 (241).

eine Kopie nicht gelten: Zum einen kann die Datenübertragung nur gefordert werden, wenn die Verarbeitung personenbezogener Daten „auf einer Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a oder Art. 9 Abs. 2 lit. a oder auf einem Vertrag gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO beruht". Zum anderen gilt sie nur für alle die Datensammlungen, die die betroffene Person verursacht oder veranlasst hat, auch wenn dies Daten von Dritten mit umfasst, die die betroffene Person rechtmäßig verarbeitet hat. Außerdem muss die Kopie nicht in einer weiterverarbeitbaren Form übermittelt werden, während die Datenübertragung nur dann Sinn macht, wenn sie vom Empfänger weiterverarbeitet werden kann.

2.1.10 Das Recht auf Datenübertragung

Während die Rechte der betroffenen Personen aus dem Katalog der Datenschutz-Grundverordnung im Wesentlichen dem entsprechen, was auch bereits unter dem Regime der Datenschutzrichtlinie galt, stellt das Recht auf Datenübertragung eine der prominentesten Neuerungen des neuen Datenschutzrechts dar.[115] Es gibt der betroffenen Person das Recht, Daten, die sie dem Verantwortlichen bereitgestellt hat, auf einen anderen Datenverarbeiter zu übertragen. Diese nicht zuletzt auf soziale Netzwerke abzielende Regelung soll sog. Lock-in-Effekte reduzieren helfen und den Wettbewerb zwischen Anbietern steigern.[116]

Die Bezeichnung des Rechts ist missglückt. Art. 20 DSGVO regelt einen Anspruch auf eine Handlung und eine Pflicht zu einer Handlung, nämlich die Bereitstellung personenbezogener Daten (Abs. 1) und deren Übertragung durch die betroffene Person (Abs. 1) oder den Verantwortlichen (Abs. 2), nicht ein Recht zur Herstellung einer Möglichkeit. Wie die anderen Rechte der betroffenen Person nicht mit Informierbarkeit, Korrigierbarkeit, Löschbarkeit oder Einschränkbarkeit überschrieben sind, sondern mit Auskunft, Berichtigung, Löschung und Einschränkung die geforderte Handlung nennen, sollte auch Art. 20 DSGVO mit „Recht auf Übertragung" überschrieben werden.

Die Nutzung dieses Rechts ist für Verbraucher jedoch durch drei Probleme, die der Normtext verursacht, gefährdet: erstens durch den zu engen Anwendungsbereich des Rechts auf Datenübertragung und zweitens durch die zu geringe Bestimmtheit über das Format, in dem die Daten übergeben werden sollen. Schließlich ist die Regelung zu eng, weil sie eine bestehende Einwilligung oder einen bestehenden Vertrag voraussetzt.

2.1.10.1 Anwendungsbereich der Vorschrift

Das Recht auf Datenübertragung sollte nicht nur für die von der betroffenen Person „bereitgestellten" personenbezogenen Daten gelten, sondern auch für die von der betroffenen Person verursachten Daten. Zwar könnte mit einer umstrittenen[117] Auslegung vertreten werden, „bereitgestellten" Daten seien nicht nur die aktiv in das Dienstangebot eingestellten Daten, sondern auch personenbezogene Daten, die das Ergebnis der Beobachtung der Tätigkeit der betroffenen

115 Roßnagel, DuD 2019, 467 (468).
116 S. Kühling/Sackmann, 2018, 21; Stiftung Datenschutz, 2018, 10, 13 ff.
117 S. a.A. z.B. Piltz, in: Gola, 2018, Art. 20 Rn. 14; Richter, PinG 2017, 231; Kamann/Braun, in: Ehmann/Selmayr, 2018, Art. 20 Rn. 13; Westphal/Wichtermann, ZD 2019, 191 (192);

Person sind.[118] Die Bereitstellung durch den Nutzer erfolge dabei durch die Nutzung des Dienstes oder Geräts.[119] Beispiele sind Suchverläufe, Playlists, Verkehrs- und Standortdaten, Fitnessdaten oder ähnliche Daten.[120] Als eingegeben sollten auf jeden Fall auch Daten gelten, die der Verbraucher mittels eines Trackers erhebt und über eine Schnittstelle in das System des Verantwortlichen eingibt. Als nicht bereitgestellt sollen dagegen Daten gelten, die der Verantwortliche aus der Analyse und Zusammenführung der bereitgestellten Daten gewonnen hat – wie etwa Bonitäts-Scores und andere Profiling-Ergebnisse.[121]

Dieses Verständnis überzeugt vor dem Hintergrund des Normzwecks, der in einer Stärkung des Wettbewerbs und dem Schutz der Verbraucher liegt.[122] Letztlich geht es darum, Einflusssphären zwischen Verantwortlichem und betroffener Person abzugrenzen und den Beitrag zum Entstehen der Daten zu würdigen. Aus ihrem Beitrag zum Entstehen der Daten leitet sich die Verfügungsbefugnis der betroffenen Person ab. Soweit die betroffene Person das Entstehen der Daten verursacht hat, der Verantwortliche aber hierzu wenig beigetragen hat, indem er etwa lediglich die Infrastruktur bereitstellt, sollen die entstandenen Daten auch unter der Verfügungs- und Nutzungsgewalt der betroffenen Person stehen. Aus dieser Logik heraus wird klar, dass eine Erstreckung von Art. 20 DSGVO auch auf Rohdaten erfolgen muss, die vom Verhalten der betroffenen Person verursacht werden.[123]

Auch für Daten Dritter, die die betroffene Person in ihrem Bereich auf der Plattform verarbeitet hat, soll sie ein Recht auf Datenübertragung haben, wenn sie diese Daten rechtmäßig verarbeitet. Dies gilt etwa für ihre Kontaktdaten[124] oder ihre Bilder, auf denen auch andere Personen zu sehen sind. Gerade Daten, die von anderen Personen an die betroffene Person übermittelt worden sind, werden vom Wortlaut der Vorschrift nicht erfasst, müssten aber von der Zielsetzung der Vorschrift erfasst sein. Dies gilt insbesondere bei Kommunikationsvorgängen. Zumindest sollten alle die Daten von der Vorschrift erfasst werden, die sich ausschließlich in der Sphäre der betroffenen Person befinden, wie z.B. E-Mails im Eingangspostfach. Dass die Nachrichten im Ausgangspostfach – weil von der betroffenen Person eingegeben – übertragen werden können, die Nachrichten im Eingangspostfach aber nicht, wäre widersinnig. Das Gleiche muss aber auch für Chats oder Messenger-Dienste gelten, auf die auch andere Personen zugreifen können. Wenn sich Beitrag an Beitrag reiht und die betroffene Person zur Kommunikation beigetragen hat, wäre es unverständlich, wenn sie nur ihre Beiträge übertragen könnte, nicht aber die Beiträge anderer, auf die sich ihre Beiträge beziehen. Bei beiden Gruppen handelt es sich um nachträglich nicht mehr veränderbare Nachrichten einer Person an die betroffene Person als Empfänger. Der Empfänger muss davon ausgehen können, dass eine persönliche Nachricht (auch)

---

118 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 11; Kühling/Sackmann, 2018, 21.

119 S. vzbv, 2016, 6; Scheibel/Horn/Öksüz 2018, 4.

120 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 11; Dix, in Simitis/Hornung/Spiecker, 2019, Art. 20 Rn. 8; Herbst, in: Kühling/Buchner, 2018, Art. 20 Rn. 11.

121 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 11 nennen diese „abgeleitete" Daten. S. hierzu auch Westphal/Wichtermann, ZD 2019, 191.

122 S. Roßnagel/Richter/Nebel, ZD 2013, 103 (107); Nebel/Richter, ZD 2012, 407 (413); Schantz, NJW 2016, 1841 (1845).

123 S. zum Streit Kamann/Braun, in: Ehmann/Selmayr, 2018, Art. 20 Rn. 13.

124 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 10 f.

an ihn zu seiner freien Verfügung steht.[125] Im Ergebnis muss dies auch für Geschäftsvorgänge gelten, die die betroffene Person betreffen, wie etwa Einzahlungen oder Belastungen auf ihren Konten. So würde einer Lösung jede Plausibilität fehlen, wenn sie nur die von ihr veranlassten Überweisungen oder Einzahlungen übertragen könnte, nicht aber die Überweisungen Dritter auf ihr Konto oder die Abbuchungen Dritter von ihrem Konto. Der Begriff „bereitgestellt" ist daher zu eng und sollte, um sinnvolle Ergebnisse zu erzielen durch „verursacht oder veranlasst" ersetzt werden.

2.1.10.2 Beschränkung auf geltende Einwilligungen oder Verträge

Das Recht auf Datenübertragung besteht nach Art. 20 Abs. 1 DSGVO nur, wenn die Verarbeitung auf einer Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO oder auf einem Vertrag gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO beruht. Ungeklärt ist die Frage, ob dieser Anspruch auch noch zu dem Zeitpunkt besteht, wenn die Einwilligung widerrufen oder der Vertrag beendet worden ist.[126] Für diesen Fall wird vertreten, dass eine Übertragung der Daten nicht mehr gefordert werden kann, weil die Datenverarbeitung nach dem Widerruf oder der Vertragsbeendigung nicht mehr auf einer Einwilligung oder einem Vertrag beruht.[127] Gerade nach einem Widerruf oder einer Beendigung des Vertrags besteht aber in besonderer Weise der Bedarf der Übertragung der Daten an die betroffenen Person oder an den neuen Provider. Der Zielsetzung der Vorschrift des Art. 20 DSGVO würde ein solcher Anspruch erst recht entsprechen. Für sie kann es keinen Unterschied machen, ob die betroffene Person zuerst die Einwilligung wiederrufen oder den Vertrag beendet hat und dann ihren Anspruch auf Datenübertragung geltend gemacht hat oder umgekehrt. Den Anspruch der betroffenen Person zu versagen, nur weil der Wortlaut des Art. 20 Abs. 1 DSGVO unpassend formuliert ist, wäre ungerechtfertigt. Daher sollte der Text dieser Vorschrift dahingehend verbessert werden, dass er die Datenübertragung auch noch nach Beendigung der Verarbeitungserlaubnis ermöglicht. Allerdings sollte dieser Anspruch in einem angemessenen zeitlichen Zusammenhand zum Widerruf oder zur Vertragsbeendigung geltend gemacht werden.

Ohne Einwilligung oder ohne Vertrag müssen die Daten nach Art. 17 Abs. 1 lit. a, b oder d DSGVO gelöscht werden. Dies wird in der Praxis aber nicht sofort nach dem Widerruf oder der Vertragsbeendigung geschehen, sondern entsprechend dem jeweiligen Löschkonzept in einer angemessenen darauffolgenden Zeitspanne. Der Anspruch auf Datenübertragung kann nur geltend gemacht werden, solange die Daten noch im System des Verantwortlichen gespeichert sind. Daher wäre die Zeitspanne bis zur Löschung der Daten auch der notwendige und zugleich ein angemessener Zeitraum, um die Datenübertragung einfordern zu können.[128] Der Verantwortliche hätte es dann in der Hand, durch eine baldige Löschung der Daten auch von seiner Pflicht zur Datenübertragung frei zu werden.

---

125 Ähnlich auch Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 11; Schantz, NJW 2016, 1841 (1845).

126 Die Datenübertragung ist keine nachvertragliche Pflicht und dient nicht der Vertragserfüllung – s. Westphal/Wichtermann, ZD 2019, 191 (192).

127 S. z.B. Westphal/Wichtermann, ZD 2019, 191 (192).

128 S. hierzu auch Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, Anhang, Frage 5; Westphal/Wichtermann, ZD 2019, 191 (193 f.), die allerdings eine Datenübertragung nach Widerruf der Einwilligung ausschließen wollen.

2.1.10.3 Form der Datenübertragung

Besteht ein Recht auf Datenübertragung aus Art. 20 Abs. 1 DSGVO, ist unklar, welche Form der Datenübertragung und welches Format der Daten der Verbraucher fordern darf. Das Recht auf Datenübertagung ist durch die Verwendung unbestimmter Rechtsbegriffe (z.B. „strukturiertes gängiges und maschinenlesbares Format", „ohne Behinderung", „technisch machbar"), gekennzeichnet,[129] die von Anbietern höchst unterschiedlich und oft zum Nachteil der Verbraucher ausgelegt werden.[130] So gibt die Datenschutz-Grundverordnung keine konkreten Formate vor. Der Begriff „ohne Behinderung" lässt offen, ob lediglich ein Unterlassen von Behinderung gemeint oder eine weite Auslegung vorzunehmen ist.[131] Bei einer weiten Auslegung dürfte die aktuelle Bereitstellungspraxis überwiegend einen Verstoß gegen Art. 20 DSGVO darstellen. Die Datenschutz-Grundverordnung bestimmt auch nicht, was gängige Formate sind. So wären E-Mails, die als PDF-Datei übergeben werden, oder Chats, die als Screenshots in einem gängigen Bildformat herausgegeben werden, wohl nicht sachgerecht, obwohl es gängige Formate sind. Für welche spätere Funktion, die herauszugebenden Daten geeignet sein müssen, lässt die Verordnung jedoch offen. Die technische Machbarkeit soll etwa auch bei der Möglichkeit einer Bereitstellung der Daten auf einem physischen Medium „unter Umständen" nicht entfallen,[132] was wiederum Kosten beim Verarbeiter verursacht. Gerade für dieses Betroffenenrecht bleiben alle die Problembereiche im Streit, die der europäische Gesetzgeber nicht gelöst, sondern nur vertuscht hat. Vorschläge zur Verankerung von Interoperabilität im Normtext sowie zur Verpflichtung des Verantwortlichen zur Bereitstellung in einem von der betroffenen Person weiter verwendbaren Format[133] wurden im Trilog nicht akzeptiert. Die mit der Einführung dieser rechtlichen Innovation bezweckten Regelungsziele werden durch die bestehenden Unsicherheiten gefährdet und durch die Anbieter von Social Networks weitgehend unterlaufen.[134]

Die Lösung dieser Problembereiche kann nur in der rechtlichen Forderung nach Interoperabilität der verwendeten Formate liegen.[135] Der Aufruf des Erwägungsgrundes 68 DSGVO, Verantwortliche zur Entwicklung interoperabler Formate für die Datenübertragung aufzufordern, hat bislang indes kaum Nachhall gefunden. Interoperabilität der Formate benötigt klare und verbindliche Vorgaben. Diese sollten in der Verordnung gefordert und deren bestimmte Festlegung als verbindliche Pflichtaufgabe des Europäischen Datenschutzausschuss gewährleistet werden.

---

129 S. z.B. Strubel, ZD 2017, 355; Jülicher/Röttgen/Schönfeld, ZD 2016, 358.

130 Sie sind nach EG 68 nicht verpflichtet, „technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten". Sie „sollten dazu aufgefordert werden interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen". S. zur Praxis von Social-Media-Anbieter Scheibel/Horn/Öksüz, 2018, 15 ff.

131 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 18: „jedwede rechtliche, technische oder finanzielle Hürde […], durch die ein Verantwortlicher den Datenzugriff, die Datenübertragung oder die Datenwiederverwendung vonseiten der betroffenen Person oder eines anderen Verantwortlichen verlangsamen oder verhindern möchte.

132 So die vagen Vorgaben der Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 17.

133 „In einem interoperablen gängigen elektronischen Format […], das sie weiterverwenden kann", Art. 15 Abs. 2a Parl-E; „in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format", Art. 18 Abs. 1 KOM-E.

134 S. z.B. Scheibel/Horn/Öksüz, 2018, 15 ff.

135 So auch vzbv, 2013, 15; Kühling/Sackmann, 2018, 21.

Dieser sollte aufgefordert werden, verbindliche Formatvorgaben für die Übergabe der Daten zu bestimmen.

Hilfreich hierfür könnten die Leitlinien zum Recht auf Datenübertragbarkeit der Artikel 29-Datenschutzgruppe vom Dezember 2016 sein. Interoperabilität wird dort als „gewünschte[s] Ergebnis" der sich aus den Begriffen „strukturiert", „gängig" und „maschinenlesbar" ergebenden „Leistungsvorgaben" bezeichnet. Das erwartete Dateiformat, in dem Daten der betroffenen Person bereitzustellen sind, muss „mit einer Weiterverwendung vereinbar" sein.[136] Der dem Verbraucher bereitgestellte Datensatz soll mit Standardsoftware kompatibel sein.

Neben Interoperabilität der Formate fordert das Recht auf Datenübertragung weitere gesetzlich Klärungen: So sollte festgelegt werden, dass die Daten durch den Verantwortlichen in der deutschen oder englischen Sprache bereitgestellt werden sollen.

Rechtspolitisch besteht demnach Klärungs- und Präzisierungsbedarf bezüglich des Rechts auf Datenübertragung, um sicherzustellen, dass es die ihm zugedachten verbraucher- und wettbewerbsstärkenden Funktionen tatsächlich erfüllen kann. Daher sollte der Unionsgesetzgeber die vorgeschlagenen Änderungen in den Normtext der Datenschutz-Grundverordnung aufnehmen.

2.1.11 Automatisierte Entscheidungen im Einzelfall

Für Art. 22 DSGVO ist weniger entscheidend, was die Vorschrift verbietet, sondern was sie erlaubt.[137] Ihre geltende Fassung verursacht für Verbraucher folgende Probleme, die eine Anpassung erfordern: Zum einen ist das Verbot automatisierter Entscheidungen im Einzelfall zu eng gefasst. Zum anderen erwähnt sie zwar das Problem des Profiling, ohne dessen spezifische Risiken zu regeln. Drittens rechtfertigt sie in Abs. 2 eine automatisierte Entscheidung im Einzelfall, wenn sie für den Abschluss oder eines Vertrags erforderlich ist, ohne dass die betroffene Person dem zustimmen muss.

2.1.11.1 Ausweitung des Anwendungsbereichs der Vorschrift

Art. 22 Abs. 1 DSGVO enthält das „Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie ähnlicher Weise erheblich beeinträchtigt". Auch hier handelt es sich um eine Übernahme aus dem alten Datenschutzrecht; hier wurde der über 20 Jahre alte Art. 15 der Datenschutzrichtlinie fast wörtlich in die Datenschutz-Grundverordnung überführt. Diese Regelung wird ca. 25 Jahre nach ihrem Entstehungsprozess den Grundrechtsrisiken algorithmenbasierter Entscheidungen nicht ausreichend gerecht.

Ihr Anwendungsbereich ist in dreifacher Weise eingeschränkt: Zunächst ist er begrenzt auf Entscheidungen und erstreckt sich nicht auf Verarbeitungen personenbezogener Daten, die den Entscheidungen zugrunde liegen, sodann ist er beschränkt auf „ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidungen" und schließlich ist er begrenzt auf Entscheidungen mit einer rechtlichen Wirkung oder einer ähnlichen erheblichen Beeinträchtigung.

---

136 Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, 19.

137 S. Roßnagel, in: Baule u.a., 2019, i.E.

Durch diese Einschränkungen erfasst die Vorschrift nur einen Bruchteil der Grundrechtsbeeinträchtigungen von Verbrauchern und wird daher der Schutzpflicht des Gesetzgebers für die Grundrechte der Verbraucher nicht gerecht.

Beispiele für automatisierte Entscheidungsverfahren sind die personalisierte Preissetzung von Gütern und Diensten, KI-basierte Gesundheitsratgeber, die Bestimmung individueller Kreditausfallrisiken, Smart-Home-Anwendungen, digitale Assistenzsysteme, Portfoliomanagement für Finanzanleger sowie das autonome Fahren.[138] Alle diese Entscheidungsverfahren berühren die Grundrechte und Interessen der betroffenen Person in beträchtlicher Weise.

Nicht erfasst von Art. 22 Abs. 1 DSGVO ist die auf einer automatisierten Verarbeitung beruhende Vorbereitung einer Entscheidung, sondern lediglich die Entscheidung selbst.[139] Die vorausgehende Verarbeitung personenbezogener Daten richtet sich in ihrer Rechtmäßigkeit nach den risikoneutralen Erlaubnistatbeständen des Art. 6 Abs. 1 und 4 DSGVO. Das damit verbundene Problem einer adäquaten Regulierung der Risiken des Profiling wird im folgenden Unterkapitel aufgegriffen.[140]

Nicht erfasst sind zum anderen alle Entscheidungen, die nicht „ausschließlich" auf einer automatisierten Verarbeitung beruhen. Die Vorschrift erfasst damit nicht die Risiken, die durch eine teilautomatisierte Entscheidung oder eine arbeitsteilig durchgeführte automatisierte Entscheidung entstehen. Möglich bleiben dadurch Entscheidungen im Einzelfall, die in mehreren Stufen automatisiert vorbereitet werden, die am Ende zwar ein Mensch trifft, der aber die automatische Entscheidungsvorbereitung nicht zu verantworten hat, eventuell nicht einmal ihre Kriterien kennt, aber ihr Ergebnis übernimmt. Dadurch entstehen erhebliche Schutzlücken gegenüber den Risiken automatisierter Entscheidungen für die Grundrechte.[141] Die Vorschrift des Art. 22 Abs. 1 DSGVO sollte daher auf die Einschränkung „ausschließlich" verzichten, um eine Erstreckung auch auf teilautomatisierte Entscheidungen zu erreichen.

Auch innerhalb einer Organisation ist die Beschränkung auf automatisierte Entscheidungen aus Verbrauchersicht problematisch. Das Recht nach Art. 22 Abs. 1 DSGVO gilt nicht, wenn am Ende ein Mensch entscheidet. Dieser wird in der Praxis die Vorgabe des Systems ungeprüft übernehmen. Zudem wird ihm zumeist das Fachwissen fehlen, diese Vorgabe kritisch zu hinterfragen. Der Mensch ist in solchen Fällen nur formal der Entscheider; die tatsächliche Entscheidung wird vom automatisierten System getroffen.

Nicht erfasst werden schließlich die automatisiert entstandenen Entscheidungen im Einzelfall, die keine Rechtswirkung entfalten oder den Betroffenen auf ähnliche Weise erheblich beeinträchtigen. Laut Erwägungsgrund 71 DSGVO sollen die automatische Ablehnung eines Online-Kreditantrags oder eines Online-Einstellungsverfahrens ohne jegliches menschliche Eingreifen erfasst sein. Aufgrund dieser Beschränkung soll die Vorschrift aber keine Anwendung finden etwa auf die automatisierte Beschränkung von Zahlungsmöglichkeiten im E-Commerce oder

138 S. vzbv, Algorithmenkontrolle, 2019, 7 f. m.w.N.
139 Kritisch Martini, 2018, 19 f.; vzbv, Algorithmenkontrolle, 2019, 12.
140 S. Kap. 2.1.12.
141 S. zu dem damit verbundenen Anspruch auf aussagekräftige Informationen s. Kap. 2.1.8.

die Verweigerung bestimmter Vertragskonditionen.[142] Umstritten ist die Anwendbarkeit auf verhaltensbedingte Werbung und individualisierte Preise.[143]

Notwendig wäre in Art. 22 Abs. 1 DSGVO eine Ergänzung um ein Verbot, automatisiert vorbereiteten Entscheidungen ausgeliefert zu sein, die der menschliche Entscheider im Regelfall unbesehen übernimmt, ohne dass die betroffene Person *vor* der Entscheidung eine Möglichkeit hat, ihren Standpunkt vorzutragen.[144] Hierzu benötigt sie zuvor eine aussagekräftige Information gemäß Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO aufgeführt oder eine Auskunft gemäß Art. 15 Abs. 1 lit. h DSGVO „über die involvierte Logik, die einzelnen Profilmerkmale und deren Bedeutung sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person".[145]

Schließlich sollte Abs. 1 auf die Einschränkung verzichten, dass die Entscheidung der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie „*in ähnlicher Weise erheblich*" beeinträchtigt. Für die Geltung des Art. 22 Abs. 1 DSGVO sollte genügen, dass die betroffene Person in ihren Grundrechten und Freiheiten beeinträchtigt wird.[146] Wenn von ihr höhere Preise verlangt werden oder wenn sie durch personalisierte Werbung belästigt wird, sollte dies als Beeinträchtigung ausreichen. Eine Benachteiligung wie bei einer negativen rechtlichen Wirkung zu verlangen, bevorzugt den Verantwortlichen und benachteiligt die Verbraucher in ungerechtfertigter Weise.

2.1.11.2 Automatisierte Entscheidungen Dritter als Bedingung

Zudem soll Art. 22 Abs. 1 DSGVO nach Abs. 2 lit. a DSGVO nicht greifen, wenn automatisierte Entscheidungen Dritter zur Bedingung der Entscheidung eines Anbieters werden. Dies ist etwa dann der Fall, wenn eine Bonitätsprüfung eingeholt wird, die dann über die Vergabe eines Kredits entscheidet. Art. 22 Abs. 2 lit. b DSGVO ermöglicht die Festsetzung weitere Ausnahmen durch mitgliedstaatliches Recht, was in Deutschland in Form von § 37 BDSG geschehen ist.

Art. 22 Abs. 2 lit. a DSGVO sollte entweder vollständig entfallen oder zumindest um die Formulierung „mit Einwilligung der betroffenen Person" ergänzt werden. Dass eine Bank, ein Vermieter oder ein Verkäufer mit einer Auskunftei vereinbart haben, dass ein Scoring Voraussetzung für einen Vertragsabschluss oder die Erfüllung eines Vertrags mit der betroffenen Person sein soll, kann nicht dafür genügen, dass Abs. 1 zu Lasten der betroffenen Person ersatzlos

---

142 Buchner, in: Kühling/Buchner, 2018, Art. 22 DSGVO, Rn 26; Born, ZD 2015, 66; Abel, ZD 2018, 304; s. auch Atzert, in: Schwartmann u.a., 2018, Art. 22 Rn. 51.

143 Dagegen Martini, in: Paal/Pauly, 2018, Art. 22 Rn. 23; Artikel 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling, WP 251 rev.01, 24; dafür Hladjk, in: Ehmann/Selmayr, 2018, Art. 22 Rn. 9.

144 Im Unterschied dazu zielt Art. 22 Abs. 3 DSGVO nur auf eine nachträgliche nochmalige Überprüfung wenn die vollautomatisierte Entscheidung im Einzelfall auf den Erlaubnistatbeständen des Abs. 2 lit. a oder c beruht – s. z.B. Scholz, in: Simitis/Hornung/Spiecker, 2019, Art. 22 Rn. 56 und 59; Hladjk, in: Ehmann/Selmayr, 2019, Art. 22 Rn. 15.

145 S. hierzu Kap. 2.1.8 und 2.1.9.

146 S. auch vzbv, Modernisierung des europäischen Datenschutzrechts, 2013, 17; vzbv, Algorithmenkontrolle, 2019, 3 f., 12.

ausfällt. Vielmehr sollte die betroffene Person auch in diesen Fällen das genannte Auskunfts- und Reklamationsrecht haben.

2.1.11.3 Qualitative Anforderungen

Jede auf einer automatisierten Verarbeitung beruhende Entscheidung sollte immer qualitativen Anforderungen unterliegen. Diese Anforderungen könnten sich an den Bedingungen des Erwägungsgrunds 71 DSGVO und des § 31 BDSG für Scoring und Bonitätsauskünften orientieren.[147] Zumindest sollte gefordert werden, dass die Entscheidung unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Entscheidungsfindung erheblich ist und dass die Prognosetauglichkeit für das Verhalten einer Person, die Validität und Reliabilität des verwendeten mathematisch-statistischen Verfahren wissenschaftlich nachgewiesen werden kann.[148]

2.1.11.4 Pflicht zur Erläuterung der Entscheidung

Nach Abs. 3 des Art. 22 DSGVO hat der Verantwortliche in den Fällen des Abs. 2 lit. a oder c „angemessene Maßnahmen“ zu treffen, „um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren.“ Zu diesen Maßnahmen gehören „mindestens“ die Rechte „auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung“. Diese Vorschrift gewährleistet der betroffenen Person ein Recht auf Reklamation und auf nochmalige Überprüfung der automatisiert getroffenen Entscheidung durch einen Menschen. Der Wortlaut fordert keine Begründungen, Erklärungen oder Erläuterungen der automatisiert getroffenen Entscheidung. In der Kommentarliteratur wird dies zwar als Inhalt des Abs. 3 gefordert,[149] aber auch bestritten.[150]

Um hier für Klarheit zu sorgen und einen Interessenausgleich sicherzustellen, sollte der Text des Abs. 3 eindeutig feststellen, dass der Verantwortliche im Fall einer Reklamation die wesentlichen Gründe der automatisiert getroffenen Entscheidung und deren Auswirkungen erläutern muss. Der betroffenen Person muss deutlich werden, welche Beurteilungsmaßstäbe der Entscheidung zugrunde lagen und welche Gesichtspunkte und Erkenntnisse in ihrem Fall ausschlaggebend waren.[151] Soweit dies möglich ist, sollte er auch verpflichtet sein, anzugeben unter welchen Voraussetzungen die Entscheidung für die betroffene Person positiv ausgegangen wäre.

2.1.12 Anforderungen an Profiling

Ein großes Manko der Datenschutz-Grundverordnung ist, dass sie das Profiling zwar in Art. 4 Nr. 5 DSGVO definiert als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen

147 S. auch Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2019, 8.
148 S. auch vzbv, Algorithmenkontrolle, 2019, 21.
149 S. z.B. Scholz, in: Simitis/Hornung/Spiecker, 2019, Art. 22 Rn. 57 f.; Schulz, in: Gola 2019, Art. 22 Rn. 42 - jeweils unter Berufung auf Erwägungsgrund 71 UAbs. 1 Satz 4.
150 S. z.B. nicht erwähnt in der Kommentierung von Helfrich, in: Sydow, 2019, Art. 22 Rn. 69 bis 73.
151 S. z.B. Scholz, in: Simitis/Hornung/Spiecker, 2019, Art. 22 Rn. 57 f.

Person zu analysieren oder vorherzusagen“. Diese Definition ist deswegen notwendig, um durch sie besonders hohe Risiken für die Grundrechte der betroffenen Personen zu erfassen.

Trotz seiner besonderen Risiken regelt die Datenschutz-Grundverordnung Profiling nur punktuell. Gegen Profiling kann nach Art. 21 Abs. 1 und 2 DSGVO Widerspruch angemeldet werden, wenn es der Wahrung berechtigter Interessen, insbesondere dem Direktmarketing, dient. Es ist außerdem nach Art. 22 Abs. 1 DSGVO verboten, wenn es für eine ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung dient, es sei denn eine der Ausnahmen des Art. 22 Abs. 2 DSGVO erlaubt dies. Alle anderen Formen und Gründe für Profiling sowie deren Risiken regelt die Datenschutz-Grundverordnung nirgendwo in einer adäquaten Weise. Auch die allgemeinen Zulässigkeitsregelungen in Art. 6 DSGVO enthalten keine Anforderungen zur Bekämpfung dieser Risiken.

Profiling von Verbrauchern ist jedoch immer ein starker Eingriff in deren Grundrechte, der über die normale Verarbeitung von personenbezogenen Daten hinausgeht. So kann es in Folge einer automatisierten Entscheidung auf Grundlage eines Profils zu einer Preisdiskriminierung im Internet kommen, wenn etwa Kunden, bei denen aufgrund ihres Profils (Einkommen, Interessen, Präferenzen) eine höhere Zahlungsbereitschaft angenommen wird und daher ein höherer Preis verlangt wird, als dies ohne Profil der Fall wäre. Daher bedarf die Datenschutz-Grundverordnung einer risikoadäquaten Regelung, die Datenschutz und Entscheidungsfreiheit schützt und Diskriminierung verhindert.[152] Eine solche Regelung ist nicht nur dann notwendig, wenn das Profil die Grundlage für eine automatisierten Entscheidungsfindung ist, sondern immer dann, wenn die Risiken üblicher Datenverarbeitung durch die Risiken einer Merkmalssammlung in Profilen deutlich gesteigert werden.

Um den spezifischen Risiken zu begegnen, die mit Profiling für die Grundrechte der Verbraucher einhergehen, sind risikoadäquate Regelungen notwendig. Die Datenschutz-Grundverordnung könnte gesetzlich festlegen, für welche Zwecke Profiling zulässig ist und für welche nicht. Vergleichbar mit der Regelung in Art. 9 DSGVO für besondere Kategorien personenbezogener Daten könnte die Regelung festlegen, dass Profiling grundsätzlich nicht erlaubt ist und nur in ausdrücklich vorgesehenen Fällen zugelassen ist. Außerdem sollte die Sammlung von Persönlichkeitsmerkmalen immer qualitativen Anforderungen unterliegen. Zu fordern ist, dass die verwendeten Merkmale für den Verarbeitungszweck tatsächlich aussagekräftig sind, dass sie nicht unzulässig diskriminieren, dass die zugrundeliegenden und genutzten Daten für die Zweckerreichung erforderlich und erheblich sind und dass die Schlussfolgerungen, die aus den Daten gezogen werden, wissenschaftlich nachweisbar mit den Merkmalen, die durch die Daten belegt werden sollen, zusammenhängen.

2.1.13 Datenschutz durch Systemgestaltung

Eine besondere Innovation der Datenschutz-Grundverordnung[153] ist die in Art. 25 Abs. 1 DSGVO geforderte datenschutzgerechte Systemgestaltung. Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen, sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung

[152] S. auch Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2019, 8.
[153] S. hierzu Roßnagel, DuD 2019, 467 (468 f.).

als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu ergreifen, die die Datenschutzgrundsätze wirksam umsetzen und den Schutz der Rechte der betroffenen Personen garantieren. Die Forderung einer datenschutzgerechten Systemgestaltung ist indes nicht neu[154] und dennoch zentral für die Verwirklichung von Datenschutz in einem technisierten Alltag.

2.1.13.1 Unbestimmtheit der Gestaltungspflicht

Die Pflicht ist allerdings sehr weich formuliert („trifft der Verantwortliche"). Ergänzt wird sie in Erwägungsgrund 78 DSGVO dadurch, dass der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen „sollte", die den Grundsätzen des Datenschutzes durch Technik sowie dem Datenschutz durch datenschutzfreundliche Voreinstellungen Genüge tun. Zur Konkretisierung enthält Erwägungsgrund 78 DSGVO in Satz 3 lediglich die sehr abstrakten Beispiele Datenminimierung, Pseudonymisierung, Transparenz, Möglichkeit der Überwachung durch die betroffene Person sowie Schaffung und Verbesserung von Sicherheitsfunktionen durch den Verantwortlichen. Die konkrete Umsetzung bleibt offen.[155]

Zur Problematik hochgradiger Unbestimmtheit treten die zahlreichen Einschränkungen, die Art. 25 Abs. 1 DSGVO enthält. So sollen der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und der Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen Berücksichtigung finden. Die Bestimmung und Abwägung dieser Faktoren gestalten sich jedoch äußerst schwierig und geben dem Verantwortlichen einen sehr großen Entscheidungs- und Gestaltungsspielraum.[156] Beide Problemkreise – unbestimmte Pflicht und weite Einschränkungsmöglichkeiten – gemeinsam führen in der Praxis dazu, dass die Verpflichtung zur Systemgestaltung nach Art. 25 Abs. 1 DSGVO beim Verantwortlichen meist auf der Strecke bleibt.[157]

2.1.13.2 Fehlende Verpflichtung der Hersteller

Die Pflicht nach Art. 25 Abs. 1 DSGVO trifft überdies nur den Verantwortlichen. Dieser ist häufig darauf angewiesen, dass der Markt geeignete Techniken zur Verfügung stellt und Hersteller von Informationstechnik geeignete Produkte anbieten, die es dem Verantwortlichen erlauben, den Anforderungen der Datenschutz-Grundverordnung gerecht zu werden. Dies ist jedoch oft nicht der Fall: „Diejenigen, die es richtig machen wollten, waren auch nicht glücklich, weil sie feststellten, dass Hersteller von Produkten und Anbieter von Dienstleistungen ihnen oft keine Hilfe waren und es damit schwierig war, die eigene Rechenschaftspflicht zu erfüllen."[158] Gleiches gilt auch für die Verbraucher, wenn sie Software verwenden, die zwischen ihnen und dritten Datenverarbeitern steht, wie beispielsweise Webbrowser oder Betriebssysteme.

---

154 S. etwa Roßnagel, 1993, 241 ff.

155 S. Hartung, in: Kühling/Buchner, 2018, Art. 25 Rn. 17.

156 S. z.B. Hansen, in: Simitis/Hornung/Spiecker, 2019, Art. 25 Rn. 37 f.

157 S. hierzu Roßnagel, DuD 2018, 741 (745). Bereichsspezifische risikobezogene Konkretisierungen fordert auch die Bundesregierung, 2019, 15.

158 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2019, 10.

Diese werden von der Verordnung aber nicht direkt adressiert, sondern durch Erwägungsgrund 78 Satz 4 DSGVO lediglich „ermutigt“, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.[159]

Die Vorschrift wird allein aus diesem Grund nicht die beabsichtigte Wirkung erzielen, eine Marktdurchdringung möglichst datenschutzfreundlicher Technologien zu erreichen. Konkrete Forderungen können aus der geltenden Fassung der Vorschrift des Art. 25 DSGVO nicht abgeleitet werden. Dies führt dazu, dass sich letztlich stets derjenige durchsetzt, der die Technikgestaltung durchführt, ohne dass Art. 25 DSGVO den Verbrauchern einen Anspruch verleiht, mehr zu verlangen. Eine verpflichtende und bußgeldbewehrte Adressierung der Hersteller wäre weitaus effektiver und würde die Vorschrift nicht lediglich auf einen wohlgemeinten Programmsatz reduzieren.

Für Anbieter von Social Networks ist die Unterscheidung zwischen Hersteller und Anwender weitgehend bedeutungslos. Der Verantwortliche ist auch der Hersteller oder hat auf die Hersteller einen so starken Einfluss, dass er sie zwingen kann, das von ihm gewünschte Maß an Datenschutz zu realisieren. Bei ihnen könnte die Pflicht zur datenschutzgerechten Systemgestaltung theoretisch greifen, sie wird aber von ihnen bisher praktisch ignoriert.

2.1.13.3 Gestaltungsmacht der Verantwortlichen

Zusammenfassend kann also festgehalten werden, dass bezogen auf Datenschutz durch Technikgestaltung vornehmlich Konkretisierungen dieser Verpflichtungen und eine Ausweitung des Adressatenkreises notwendig sind. Die Pflicht zur Systemgestaltung als zentrale Neuerung des Datenschutzrechts kann nur dann volle Wirkung entfalten, wenn auch die Hersteller rechtlich bindend verpflichtet werden. Eine Präzisierung dessen, was Datenschutz durch Technikgestaltung konkret bedeutet, kann auf Unionsebene durch den Europäischen Datenschutzausschuss, auf mitgliedstaatlicher Ebene durch die Aufsichtsbehörden erfolgen.[160] Zudem sind Verbänderegulierung und Normung als Instrumente denkbar. Eine Verpflichtung der Hersteller könnten sowohl die mitgliedstaatlichen Gesetzgeber,[161] besser aber der Unionsgesetzgeber vorsehen.

Eine abstrakte Regelung, wie sie Art. 25 Abs. 1 DSGVO enthält, zeichnet sich zwar durch Offenheit für technische Neuerungen aus, hat jedoch auch den handfesten Nachteil, zu Auseinandersetzungen von Interessenvertretern über ihren Bedeutungsgehalt einzuladen.[162] Hier besteht die Gefahr, dass die Interessen der Verarbeiter und Hersteller sich im Diskurs gegenüber den Interessen der betroffenen Person und insbesondere der Verbraucher durchsetzen. Machtasymmetrien spielen auch innerhalb der Verantwortlichen eine Rolle. Mahnt die Datenschutzabteilung eines Unternehmens zu bestimmten Maßnahmen zur Sicherstellung von Datenschutz

159 S. Husemann, in: Roßnagel, 2018, § 5 Rn. 56.
160 S. hierzu Roßnagel, 2017, 122 ff. So etwa geschehen durch die spanische Datenschutzaufsichtsbehörde: Agencia Española de Protección de Datos, Guía de Privacidad desde el Diseño, Oktober 2019.
161 S. Hansen, in: Simitis/Hornung/Spiecker, 2019, Art. 25 Rn. 21.
162 S. Roßnagel, DuD 2018, 741 (745).

durch Technikgestaltung, so kann die Gegenseite sich leicht auf den Katalog der Einschränkungen aus Art. 25 Abs. 1 DSGVO zurückziehen und die geforderten Maßnahmen ablehnen. Auch dies gerät dem Verbraucher letztlich zum Nachteil.

2.1.14 Datenschutz durch datenschutzfreundliche Voreinstellungen

Das Prinzip des „Privacy by Default" nach Art. 25 Abs. 2 DSGVO unterliegt nicht den fünf Einschränkungen des Abs. 1.[163] Jedoch sollen sich die Voreinstellungen für den Nutzer nach der Erforderlichkeit der Verarbeitung für den jeweiligen Verarbeitungszweck richten. Dies lässt dem Verantwortlichen sehr große Freiheiten, durch die Bestimmung des Zwecks die Voreinstellungen so zu wählen, dass er durch diese die gewünschten Daten erhalten kann. Auch hier sind Präzisierungen erforderlich, wenn die Vorschrift ihr rechtspolitisches Ziel erreichen soll. Diese können durch die Aufsichtsbehörden, den mitgliedstaatlichen Gesetzgeber (für einzelne Technikbereiche),[164] den Europäischen Datenschutzausschuss, aber auch durch Verbänderegulierung erfolgen.

Außerdem sollte der mögliche Zweck auf die Funktionalität des jeweiligen Dienstes beschränkt werden. Art. 25 Abs. 2 DSGVO nimmt eine solche Beschränkung nicht vor, sondern richtet die Voreinstellungen an der Erforderlichkeit für den jeweiligen Verarbeitungszweck aus. Diesen aber bestimmt allein der Verantwortliche – nach seinen Verarbeitungsinteressen. Setzt er seine Zwecke großzügig, so läuft letztlich der als Beschränkung vorgesehene Art. 25 Abs. 2 DSGVO weitgehend leer.

Hier könnte das Prinzip der Datenvermeidung, das auch den Zweck unter das Gebot, mit möglichst wenigen personenbezogenen Daten auszukommen, nimmt, in einer Ergänzung des Art. 5 Abs. 1 DSGVO helfen.[165] Bei der Zweckbestimmung müsste eine vergleichbare Einschränkung erfolgen wie sie zur Bestimmung des Vertragszwecks ihm Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO vorgeschlagen wurde.[166]

2.1.15 Effektive Datenschutzaufsicht

Ein in der Praxis effektives Datenschutzregime ist auf eine funktionierende Datenschutzaufsicht angewiesen. Die Datenschutz-Grundverordnung hat mit ihren Regelungen zu Aufgaben und Befugnissen der Aufsichtsbehörden zur Zusammenarbeit und Kohärenz sowie mit den Entwicklungen in den Bereichen Rechtsbehelfe, Rechtsmittel, Haftung und Schadensersatz sowie Sanktionen eine deutliche Verbesserung bewirkt. Das Funktionieren des Kohärenzmechanismus muss sich in der Praxis indes noch beweisen. Zudem bleibt trotz personeller Anpassungen das Problem einer unzureichenden personellen wie auch finanziellen Ausstattung des Europäischen Datenschutzausschusses[167] und der nationalen Aufsichtsbehörden. Ergänzende Regelungen könnten hilfreich sein.

---

163 S. Hartung, in: Kühling/Buchner, 2018, Art. 25 Rn. 29; Hansen, in: Simitis/Hornung/Spiecker, 2019, Art. 25 Rn. 45.

164 Barlag, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, § 3 Rn. 247.

165 S. hierzu Kap. 2.1.3.

166 S. hierzu Kap. 2.1.5.

167 Zur Überforderung des EDSA s. Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg, 2019, 11; Roßnagel, DuD 2019, 467 (472).

Die Aufsichtsbehörden sind die Instanzen, für die die Datenschutz-Grundverordnung die größten Veränderungen bewirkt und den größten Zuwachs an neuen Aufgaben bewirkt hat.[168] Ihre Ausstattung ist angesichts dieser neuen Aufgaben zwar in den meisten Fällen verbessert worden. Dennoch sind sie vom Umfang und der Größe der zusätzlichen Aufgaben durch die Datenschutz-Grundverordnung weiterhin überfordert.[169] Die Beanspruchung durch Beschwerden, Beratungsanforderungen und Meldungen von Datenschutzverstößen haben sich um ein Vielfaches erhöht und binden in beträchtlichem Umfang Personal.[170] Die Herstellung von Vollzugsgleichheit in den Bundesländern und in den Mitgliedstaaten ist für den Erfolg der Datenschutz-Grundverordnung zentral.[171] Um alle praktisch relevanten Fragen der Datenschutz-Grundverordnung beantworten und um alle notwendigen Vorbedingungen für die Durchsetzung der Datenschutzregelungen zu gewährleisten, sind noch weitere Personalaufstockungen erforderlich.[172]

2.1.16 Sanktionen

Eine wichtige Stärkung des Datenschutzes liegt in der Möglichkeit, drastische Sanktionen zu verhängen. Die Unsicherheit bezogen auf die zu abstrakten Bußgeldtatbestände des Art. 83 Abs. 4 und 5 DSGVO behindert jedoch die Nutzung dieses Instruments. Diese sind daher zur Gewährleistung ihrer Praktikabilität zu präzisieren.

Bei dem im Vergleich zum alten Bundesdatenschutzgesetz deutlich erweiterten Spielraum zur Sanktionierung von Rechtsbrüchen handelt es sich um die wahrscheinlich meistbeachtete Innovation der Datenschutz-Grundverordnung.[173] Die Datenschutzrichtlinie hatte die Ausgestaltung solcher Sanktionen noch den Mitgliedstaaten überlassen. Das Bundesdatenschutzgesetz sah in seiner alten Fassung eine Höchstbuße von 300.000 Euro vor.[174] Die in der aufsichtsbehördlichen Praxis verhängten Bußgelder lagen indes zumeist im vierstelligen Bereich. Art. 83 Abs. 4, 5 und 6 DSGVO ermöglichen nun, Geldbußen in Höhe von bis zu 10 Millionen Euro oder bei Unternehmen von bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorausgegangenen Geschäftsjahres bzw. 20 Millionen Euro oder 4 % des Jahresumsatzes zu verhängen.

Art. 83 Abs. 1 und 2 DSGVO enthalten die Maßstäbe, die bei der Verhängung von Geldbußen anzulegen sind. Hier sind General- und Spezialprävention wesentliche Aspekte, wobei insbesondere die Negativprävention durch die Verwendung des Begriffs „abschreckend“ in Art. 83 Abs. 1 DSGVO hervorgehoben wird. Ebenso hervorgehoben werden die Effektivität der verhängten Geldbußen („wirksam“) sowie der Grundsatz der Verhältnismäßigkeit. Art. 83 Abs. 2

168 S. hierzu ausführlich Roßnagel, 2017.

169 S. z.B. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 18; Bayerisches Landesamt für Datenschutzaufsicht, 2019, 2; Sachsen-Anhalt, 2019, 6.

170 S. Schulzki-Haddouti, Implodierende Aufsichtsbehörden, PinG-Blog vom 29.3.2019; Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg, 2019, 11; Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, 2019, 10.

171 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 2019, 22.

172 S. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit 2019, 18; Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, 2019, 10; Roßnagel, DuD 2019, 467 (471 f.).

173 S. hierzu Rost, DuD 2019, 467 (471 f.).

174 § 43 Abs. 3 Satz 1 BDSG a.F.

Satz 2 DSGVO enthält eine Auflistung von Faktoren, die sich verschärfend oder mildernd auf die Geldbuße auswirken sollen.

Es ist zu konstatieren, dass die Möglichkeiten zur Sanktionierung von Verstößen, die die Datenschutz-Grundverordnung bietet, bislang noch eher zurückhaltend ausgenutzt werden,[175] auch wenn einzelne Bußgelder herausstechen.[176] Ein Grund hierfür dürfte in der Spannbreite der möglichen Sanktionen liegen, die durch die abstrakten Vorgaben des Art. 83 Abs. 2 Satz 2 DSGVO nur unzureichend eingeengt wird. Hier wird zurecht kritisiert, die Bußgeldtatbestände in Art. 83 Abs. 4 und 5 DSGVO seien zu unbestimmt, um rechtssicher Bußgelder in Millionenhöhe verhängen zu können.[177] In der Praxis sicher handhabbar dürfte allein das Bußgeld nach Art. 83 Abs. 6 DSGVO sein, das bei Nichtbefolgung einer Anweisung einer Aufsichtsbehörde nach Art. 58 Abs. 2 DSGVO verhängt werden kann. Die Anweisung der Aufsichtsbehörde muss dabei allerdings auch vollziehbar sein. Dabei ist davon auszugehen, dass insbesondere finanzstarke Verarbeiter eine gerichtliche Überprüfung des Bußgelds anstreben werden. Diese Prozesse auch über mehrere Instanzen binden wiederum Ressourcen der Aufsichtsbehörden. Der Vollzug der Datenschutz-Grundverordnung hätte deshalb von Anfang an durch eine Präzisierung der Bußgeldtatbestände gestärkt werden müssen.[178] Diese könnte nachträglich durch eine Leitlinie des Europäischen Datenschutz-Ausschusses nach Art. 70 Abs. 1 Satz 2 lit. k DSGVO erreicht werden. Eine erste Leitlinie zu den Kriterien des Art. 83 Abs. 2 Satz 2 DSGVO hat die Artikel 29-Datenschutzgruppe zwar bereits 2017 vorgenommen,[179] es verbleibt jedoch weiterer Präzisierungsbedarf.[180] Die notwendige Präzisierung könnte indes auch auf mitgliedstaatlicher Ebene von der Konferenz der Datenschutzaufsichtsbehörden geleistet werden, indem diese einen unverbindlichen Bußgeldkatalog erstellt.[181] Als Beispiel können die Feststellungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden in Deutschland vom Oktober 2019 gelten.[182] Nur so kann dem sowohl im primären Unionsrecht als auch mitgliedstaatlich verankerten Bestimmtheitsgebot Genüge getan und eine einheitliche Anwendung der Bußgeldvorschriften in der gesamten Union erreicht werden. Hierfür wäre auch eine Verpflichtung der Aufsichtsbehörden hilfreich, eine jährliche Statistik ihrer Bußgeldpraxis zu veröffentlichen. Jedenfalls sind alle sinnvollen Maßnahmen zu ergreifen, um hinsichtlich der Sanktionen keinen Anreiz zu einem Forum Shopping zu bieten.

Denkbar wäre auch eine Reform des Umgangs mit erfolgreich verhängten Bußgeldern. Die so erlangten Geldmittel fließen in Deutschland überwiegend in die allgemeinen Haushalte des

---

175 S. näher Martin/Friedewald, DuD 2019, 493 ff.; Rost, DuD 2019, 488 (491 f.).

176 Z.B. gegen ein dänisches Taxiunternehmen im April 2019 in Höhe von etwa 2,8% des Jahresumsatzes des Unternehmens; gegen Google in Höhe von 50 Millionen Euro durch die französische CNIL im Januar 2019; in Italien im Kontext des Telemarketing (Newsletter des italienischen Datenschutzbeauftragten Nr. 453 vom 30. Mai 2019); im Juli 2019 in Großbritannien 183,4 Millionen GBP (ca. 1,5% des weltweiten Jahresumsatzes) gegen British Airways und 99.2 Millionen GBP gegen Marriott.

177 S. etwa Bergt, DuD 2017, 555; Eckhardt/Menz, DuD 2018, 139; Faust/Spittka/Wybitul, ZD 2016, 120.

178 S. Roßnagel, 2017, 131 ff.

179 Artikel 29-Datensachutzausschuss, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, WP 253.

180 So auch Bundesregierung, 2019, 18.

181 Braun/Hohmann, in: Roßnagel, 2018, § 6 Rn. 152.

182 Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen vom 14.10.2019.

Bundes und der Länder. Hier wäre mit Blick auf andere Mitgliedstaaten wie Frankreich auch eine Ausgestaltung denkbar, bei der Bußgelder direkt in den Haushalt der jeweiligen Aufsichtsbehörde fließen. Wird dieser Weg aus Angst vor einem überschießenden Gebrauch des Instruments nicht gegangen, so ist zumindest eine weitere personelle und finanzielle Aufstockung der Aufsichtsbehörden angezeigt[183] – verbunden mit einer Übernahme anfallender Prozesskosten durch den Bund und die Länder.[184]

2.2 Handlungsbedarf

Die Untersuchung zeigt, dass an zahlreichen Stellen rechtspolitischer Handlungsbedarf besteht. Dieser zielt nicht immer auf eine Umformulierung des Normtextes der Datenschutz-Grundverordnung. Vielmehr reicht der politische Handlungsbedarf von Erläuterungen des geltenden Rechts oder verbindlichen Festlegungen durch die Aufsichtsbehörden und den Europäischen Ausschuss über kleinere und größere Anpassungen oder Konkretisierungen durch die Gesetzgeber der Mitgliedstaaten im Rahmen der Ko-Regulierung des europäischen Datenschutzrechts sowie Änderungen einzelner Vorschriften der Datenschutz-Grundverordnung bis hin zu konzeptionellen Veränderungen und Modernisierungen des Datenschutzrechts in der Europäischen Union. Letztere betreffen nicht nur einzelne Vorschriften, sondern sind umfangreicher und langfristiger angelegt. Sie erfordern weitere Untersuchungen und Diskussionen. Konzeptionelle Überlegungen zu ihnen stehen im dritten Kapitel des Gutachtens im Fokus. Formulierungsvorschläge zu einzelnen Vorschriften der Datenschutz-Grundverordnung – ohne Änderung ihrer Gesamtkonzeption – werden im folgenden Unterkapitel vorgestellt. In diesem Unterkapitel erfolgt ein Zwischenfazit zum rechtspolitischen Handlungsbedarf, das diesen in drei Gruppen teilt:

- Sonstige rechtspolitische Maßnahmen, die keine Änderungen im Normtext der Datenschutz-Grundverordnung erfordern. Für diese Maßnahmen sind in der Regel andere Instanzen der Union oder der Mitgliedstaaten verantwortlich. Sie werden im Gutachten nicht weiterverfolgt.
- Änderungen einzelner Vorschriften der Datenschutz-Grundverordnung. Diese stehen im Mittelpunkt der Evaluation der Datenschutz-Grundverordnung und daher auch im Mittelpunkt des Gutachtens. Soweit das Regelungsproblem allein durch eine Änderung des Normtextes gelöst werden kann, werden hierfür in Unterkapitel 2.3 Formulierungsvorschläge empfohlen.
- Weiterreichender konzeptioneller Handlungsbedarf. Soweit Änderungen in der grundlegenden Konzeption der Datenschutz-Grundverordnung in Frage stehen, um die Effektivität des Grundrechtsschutzes zu verbessern, oder Fortentwicklungen des europäischen Datenschutzrechts bedacht werden müssen, um dieses gegenüber den künftigen Herausforderungen der Digitalisierung zu wappnen, werden Diskussionsvorschläge in Kapitel 3 präsentiert.

Der rechtspolitische Handlungsbedarf wird im Folgenden nach Kapiteln der Datenschutz-Grundverordnung zusammengefasst, um Zusammenhänge über einzelne Vorschriften oder Problembereiche hinaus, die in Unterkapitel 2.1 diskutiert wurden, erkennen zu können.

---

183 S. Roßnagel, 2017, 191 ff.

184 Miedzianowski, in: Roßnagel, 2018, § 4 Rn. 75; Dieterich, ZD 2016, 266.

2.2.1 Handlungsbedarf zum ersten Kapitel der Datenschutz-Grundverordnung

Bezogen auf die Verarbeitung im persönlichen oder familiären Kontext ist eine Rücknahme der vollständigen Ausnahme invasiver Datenverarbeitung aus dem Anwendungsbereich der Datenschutz-Grundverordnung zu fordern. Dadurch würde eine Schutzlücke geschlossen, die bei bestimmten Formen der Datenverarbeitung bei der Ausübung persönlicher oder familiärer Tätigkeiten entsteht, die ein hohes Risiko für die betroffenen Personen mit sich bringt. Wo daher die Grenze der Ausnahme schon nach geltendem Text zu ziehen ist, sollte der Europäische Datenschutzausschuss durch geeignete Richtlinien deutlich machen.

Im Sinne eines risikoadäquaten Ansatzes sollten nur solche Verarbeitungen vollständig aus dem Anwendungsbereich der Datenschutz-Grundverordnung herausgenommen werden, bei denen nur geringe Risiken für die Rechte und Freiheiten der betroffenen Personen bestehen.[185] Um selbst bei risikoreichen Datenverarbeitungen zu verhindern, dass der persönliche und familiäre Bereich mit Datenschutzregeln überfrachtet und die privaten Verarbeiter personenbezogener Daten damit überfordert werden, sollten bei erhöhten Risiken nur ausgewählte Regelungen der Datenschutz-Grundverordnung zur Anwendung kommen. Bezogen auf die Veröffentlichung von personenbezogenen Daten Dritter aus dem persönlichen und familiären Bereich in Social Media-Plattformen oder auf selbstbetriebenen Webseiten sollte trotz der Übermittlung personenbezogener Daten an den Betreiber der Plattform der Verantwortliche von bestimmten Pflichten ausgenommen werden. Damit soll verhindert werden, dass es zu regelmäßigen Rechtsbrüchen bei der Verwendung von sozialen Medien kommt, für die kein Verständnis bei den Nutzern besteht.[186] Diese Einschränkung der Ausnahme in Art. 2 Abs. 2 lit. c DSGVO ist mit den umfassenden risikobezogenen Änderungen der Regelungen zur Zulässigkeit der Verarbeitung personenbezogener Daten zu verknüpfen und bedarf daher weiterer konzeptioneller Überlegungen.[187]

Der räumliche Anwendungsbereich der Datenschutz-Grundverordnung sollte ausgeweitet werden. Er sollte jede Form der Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Europäischen Union aufhalten und die nicht die Datenverarbeitung initiiert haben, erfassen.[188] Hierfür wird eine Formulierung für Art. 2 Abs. 2 lit. a DSGVO vorgeschlagen.[189]

2.2.2 Handlungsbedarf zum zweiten Kapitel der Datenschutz-Grundverordnung

Die deutsche Sprachfassung von Art. 5 Abs. 1 lit. a DSGVO sollte angepasst werden. Das Begriffspaar „Treu und Glauben“ ist zur Vermeidung von falschen Assoziationen und zur Angleichung an die anderen Sprachfassungen der Datenschutz-Grundverordnung durch den Begriff „Fairness“ zu ersetzen.[190] Zudem sollte eine Präzisierung der Begriffe mittels Erwägungsgrund 39 DSGVO und eine klare Abgrenzung von Transparenz und Rechtmäßigkeit der Verarbeitung

185 S. Kap. 2.1.1.1.
186 S. Kap. 2.1.1.2.
187 S. zu diesen Kap. 3.3.1.
188 S. Kap. 2.1.2.
189 S. hierzu Kap. 2.3.1.
190 S. Kap. 2.1.3.1.

erfolgen. Der Erwägungsgrund sollte deutlich machen, dass das Begriffspaar eine Auffangklausel ist, die ungerechte Praxisergebnisse verhindert. Ein Vorschlag zur Änderung des Textes von Art. 5 Abs. 1 lit. a DSGVO findet sich im nächsten Unterkapitel.[191]

Der Gestaltungsgrundsatz der Datenminimierung fordert nur, die personenbezogenen Daten auf den jeweils vom Verantwortlichen bestimmten Zweck erforderlichen Umfang zu reduzieren. Er sollte um den Grundsatz der Datenvermeidung ergänzt werden. Dieser fordert eine datensparsame Gestaltung des sozio-technischen Gesamtsystems, das den Zweck einbezieht, und wird daher dem Ausgleich der beteiligten Grundrechte nach dem Grundsatz der Verhältnismäßigkeit gerechter.[192] Hierfür bietet das nächste Unterkapitel einen Formulierungsvorschlag für Art. 5 Abs. 1 lit. c DSGVO.[193]

Die weiteren Grundsätze für die Verarbeitung personenbezogener Daten bedürfen der Präzisierung. Art. 5 DSGVO ist an vielen Stellen von unbestimmten Begriffen geprägt, die äußerst interpretationsoffen sind.[194] Dies ist bei Grundsätzen schwer zu vermeiden. Daher sollte nicht der Unionsgesetzgeber, sondern der Europäische Datenschutzausschuss sie durch die Formulierung von geeigneten Leitlinien präzisieren und so die Vollziehbarkeit der Grundsätze unterstützen.

Darüber hinaus bedürfen die Regelungen zur Zulässigkeit von Verarbeitungen personenbezogener Daten der Präzisierung und der risikoadäquaten Weiterentwicklung. Die Präzisierung durch Textänderung wird im Folgenden weiterbehandelt, die risikoadäquaten Weiterentwicklung ist Thema der konzeptionellen Überlegungen im nächsten Kapitel.[195]

In Art. 6 Abs. 1 UAbs. 1 DSGVO sollte klargestellt werden, dass neben einer Einwilligung kein weiterer gesetzlicher Erlaubnistatbestand in Anspruch genommen werden kann und dass in der Konkurrenz mehrerer Erlaubnistatbestände die Regelungen zur Einwilligung den Regelungen zu anderen gesetzlichen Erlaubnistatbestand vorgehen.[196] Hierzu bietet das nächste Unterkapitel einen Formulierungsvorschlag.[197]

Der Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO sollte präzisiert werden. Notwendig ist eine objektive (funktionale) Bestimmung der zur Erfüllung eines Vertrages notwendigen Verarbeitung personenbezogener Daten unabhängig von der Vertragsformulierung und dem Willen des Verantwortlichen.[198] Das nächste Unterkapitel unterbreitet hierzu einen Formulierungsvorschlag.[199]

Zudem ist die Aufnahme eines Erlaubnistatbestands für die Sammlung von Persönlichkeitsmerkmalen in Form von Profiling in die Datenschutz-Grundverordnung zu fordern, der festlegt,

---

191 S. hierzu Kap. 2.3.2.
192 S. Kap. 2.1.3.2.
193 S. hierzu Kap. 2.3.2.
194 S. Kap. 2.1.3.1.
195 S. Kap. 3.3.1.
196 S. hierzu Kap. 2.1.4.
197 S. hierzu Kap. 2.3.3.
198 S. hierzu Kap. 2.1.5.
199 S. hierzu Kap. 2.3.4.

für welche Zwecke Profiling zulässig ist und für welche nicht.[200] Ein solcher risikobezogener spezifischer Erlaubnistatbestand ist allerdings in die Diskussion über die Risikoorientierung der Datenschutz-Grundverordnung einzubeziehen und bedarf weiterer Diskussionen, die im nächsten Kapitel aufgegriffen werden.[201] Außerdem sind die Voraussetzungen eines solchen Erlaubnistatbestands und deren bereichsspezifische Auswirkungen ebenso intensiv zu diskutieren wie deren branchenspezifischen Auswirkungen.

Art. 6 Abs. 4 DSGVO sollte bei der Prüfung der Vereinbarkeit eines neuen Verarbeitungszwecks mit dem bisherigen Verarbeitungszweck berücksichtigen, wenn die Daten eines Kindes für einen anderen Zweck verwendet werden sollen.[202] Hierzu ist der Text des Art. 6 Abs. 4 DSGVO in lit. d zu ergänzen. Einen Formulierungsvorschlag enthält das nächste Unterkapitel.[203]

Ebenfalls um der besonderen Schutzbedürftigkeit von Kindern gerecht zu werden, sollte in Artikel 8 DSGVO die Zielsetzung des Erwägungsgrunds 38 Satz 2 DSGVO in den Normtext übernommen werden.[204] Hierzu bietet das nächste Unterkapitel einen Formulierungsvorschlag.[205]

Schließlich sollte bei der Ausnahme des Verbots der Verarbeitung besonderer Kategorien von personenbezogenen Daten durch eine Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO, die Einwilligung eines Kindes ausgeschlossen werden.[206] Auch hierzu enthält das nächste Unterkapitel einen Formulierungsvorschlag.[207]

2.2.3 Handlungsbedarf zum dritten Kapitel der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung erfordert insbesondere in ihrem dritten Kapitel, das die Rechte der betroffenen Person regelt, Klarstellungen im Normtext, um unnötige Rechtsstreitigkeiten zwischen Verantwortlichen und betroffenen Personen zu vermeiden und den Vollzug des neuen Datenschutzrechts zu unterstützen.

Statt die betroffene Person mit nur einer Information zu Beginn der Datenverarbeitung zu überfordern, die alle denkbaren künftigen Formen und Phasen der Datenverarbeitung in einer zu umfangreichen Erklärung zusammenfasst, sollte das Konzept der Information der betroffenen Person neu aufgegriffen werden. Es sollte aus dem Blickwinkel der betroffenen Person, nicht nur aus der Perspektive des Verantwortlichen neu konzipiert werden.[208] Die Information sollte in der Situation in dem Umfang in der Form erfolgen, die dem Interesse der betroffenen Person und ihren Entscheidungsmöglichkeiten oder ihrer Betroffenheit entspricht. Außerdem sollten die Pflichten zur Information der betroffenen Person und zur Kommunikation mit dieser risikoadäquat gestalten werden. Daher sollten die allgemeinen Informationspflichten um bereichs-

200 S. hierzu Kap. 2.1.12.
201 S. Kap. 3.3.1.
202 S. hierzu Kap. 2.1.6.
203 S. hierzu Kap. 2.3.5.
204 S. hierzu Kap. 2.1.6.
205 S. hierzu Kap. 2.3.6.
206 S. hierzu Kap. 2.1.6.
207 S. hierzu Kap. 2.3.7.
208 S. hierzu Kap. 2.1.7.1.

und technologiespezifische Regelungen für spezielle Anwendungsbereiche und Technologien ergänzt werden. Dieses neue Konzept einer betroffenenorientierten Information statt einer die Informationslast des Verantwortlichen reduzierenden Konzeption muss insgesamt noch näher erörtert werden. Es wird in Grundzügen im nächsten Kapitel im Rahmen der Fortentwicklung des Datenschutzrechts wieder aufgegriffen.[209]

Einige kleinere Verbesserungen in den allgemeinen Regelungen zur Information der betroffenen Person könnten aber unmittelbar in Art. 12, 13 und 14 DSGVO vorgenommen werden.

Um vage, verkürzte, unvollständige, unklare und nur beispielhafte Angaben über die Datenverarbeitung auszuschließen, sollte der Text des Art. 12 DGSVO festhalten, dass sich die Information auf die gegenwärtig vorgesehene Datenverarbeitung beziehen muss. Künftige Änderungen in der Datenverarbeitung sollten zu neuen, dann wiederum aktuellen, Informationen führen. Es sollte ausdrücklich nicht zulässig sein, seine Informationspflicht zu erfüllen, indem unter Verweis auf eine allgemeine Datenschutzerklärung alle denkbaren künftigen Datenverarbeitungen mit vagen Hinweisen auf künftige Möglichkeiten in eine einmalige Information aufgenommen werden.[210] Hierzu enthält das nächste Unterkapitel einen Formulierungsvorschlag.[211]

Der Konflikt zwischen den Informationspflichten des Verantwortlichen, dem Informationsanspruch der betroffenen Person und dem Schutz rechtlich anerkannter Geheimnisse und Rechte des geistigen Eigentums ist durch eine Verfahrensregel in Art. 12 DSGVO zu reduzieren: Der Verantwortliche sollte jeweils das höchstmögliche Maß an Information bereitstellen müssen, das er unter gleichzeitiger Wahrung von rechtlich anerkannten Geheimnissen ermöglichen kann. Das Geheimnis sollte kein Grund sein, Informationen zu der Datenverarbeitung vollständig zu verweigern oder stark einzugrenzen. Vielmehr muss er nach Wegen suchen, wie er das vertretbare Maximum an Informationen zur Verfügung stellen kann.[212] Im nächsten Unterkapitel findet sich ein Vorschlag, wie eine solche Ergänzung des Art. 12 DSGVO formuliert werden kann.[213]

Um der betroffenen Person eine einfache und schnelle Information über die Datenverarbeitung zu ermöglichen, sieht Art. 12 Abs. 7 DSGVO die Möglichkeit vor, die bereitzustellenden Informationen mit standardisierten Bildsymbolen zu kombinieren. Diese mögliche Entlastung des Verbrauchers sollte möglichst bald umgesetzt werden.[214] Diese rechtpolitische Handlungsempfehlung fällt allerdings nicht in die Verantwortung des Unionsgesetzgebers, sondern der Europäischen Kommission.

Um ihren gesetzlichen Zweck zu erfüllen, müssten die Informationen situationsadäquat, also dann gegeben werden, wenn der Verbraucher eine Entscheidung zu treffen hat oder wenn eine ihn belastende Handlung erfolgt. Daher fordert Art. 13 Abs. 1 DSGVO, dass der Verantwortliche die betroffene Person „zum Zeitpunkt der Erhebung“ informieren muss. Damit dies auch tatsächlich geschieht und nicht weit – eventuell Jahre – vor der Datenerhebung Informationen

209 S. Kap. 3.3.3.
210 S. hierzu Kap. 2.1.7.3.
211 S. hierzu Kap. 2.3.8.
212 S. hierzu Kap. 2.1.7.3.
213 S. hierzu Kap. 2.3.9.
214 S. Kap. 2.1.7.4.

erfolgen,[215] sollte im Normtext zur Klarstellung festgelegt werden, dass die *relevante* Information *jeweils* zum Zeitpunkt der Erhebung dieser Daten erfolgt. Hierzu erfolgt im nächsten Unterkapitel ein Vorschlag zur Ergänzung des Eingangs zu Art. 13 Abs. 1 DSGVO.[216]

Um der betroffenen Person tatsächlich zu ermöglichen, ihre Rechte auch dann effektiv geltend zu machen, wenn die personenbezogenen Daten – bisweilen sehr oft – weitergegeben werden, sollte der Verantwortliche ihr die Empfänger personenbezogener Daten mitteilen, wenn er sie kennt. Nur wenn er sie noch nicht kennt, soll die Angabe von Kategorien von Empfängern genügen.[217] Zu diesem Zweck sollte die Regelung in Art. 13 Abs. 1 lit. e und Art. 14 Abs. 1 lit. e DSGVO angepasst werden. Hierzu erfolgt ein Formulierungsvorschlag im nächsten Unterkapitel.[218]

Die bisherige Pflicht des Verantwortlichen, die betroffene Person über das Bestehen einer automatisierten Entscheidungsfindung zu informieren, sollte durch Präzisierung der Informationsinhalte im Gesetzestext klargestellt werden.[219] Die Informationen sollten sich hinsichtlich der Tragweite der Entscheidung auch auf die rechtlichen und tatsächlichen Auswirkungen auf die betroffene Person erstrecken. Bezogen auf die Information über die „involvierte Logik" sollten auch die Kriterien für die Entscheidung und ihre Gewichtung mitgeteilt werden müssen. Ein Formulierungsvorschlag für diese Änderungen wird im nächsten Unterkapitel dargestellt.[220]

Bei automatisierten Entscheidungen im Einzelfall – insbesondere bei selbstlernenden Systemen – dürfte es nicht immer einfach sein, bei der betroffenen Person ein ausreichendes Verständnis der sie betreffenden Schritte der Datenverarbeitung hervorzurufen.[221] Dennoch darf Komplexität keine Entschuldigung für mangelhafte Informationen sein. Dies sollte in Erwägungsgrund 58 DSGVO klargestellt werden.

Der Anwendungsbereich der Informationspflichten aus Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO wird sich erweitern, wenn der Anwendungsbereich der Vorschrift des Art. 22 DSGVO, auf den diese Informationspflichten verweisen, ausgeweitet wird.[222]

Zur Verpflichtung gemeinsam Verantwortlicher, diese Informationsplicht umfassend und lückenlos zu erfüllen, wird auf die vorgeschlagene Ergänzung des Art. 26 Abs. 1 DSGVO verwiesen.[223]

Um den Risiken des Profiling für die Grundrechte der betroffenen Person[224] gerecht zu werden, sollte in Art. 13 Abs. 2 DSGVO über den Hinweis in Erwägungsgrund 60 Satz 3 DSGVO hinaus in einem zusätzlichen lit. g und in 14 Abs. 2 DSGVO in einem zusätzlichen lit. h gleichlau-

215 S. S. hierzu Kap. 2.1.7.3.
216 S. hierzu Kap. 2.3.10.
217 S. hierzu näher Kap. 2.1.8.
218 S. hierzu Kap. 2.3.11.
219 S. hierzu Kap. 2.1.8.3.
220 S. Kap. 2.3.12.
221 S. Kap. 2.1.8.3.
222 S. hierzu Kap. 2.3.20.
223 S. hierzu Kap. 2.1.8.3 und 2.3.24.
224 S. zu diesen Kap. 2.1.8.4.

tend eine Informationspflicht bei jedem Profiling vorgesehen werden. Dadurch wird die betroffene Person auf diese besonderen Risiken aufmerksam gemacht und kann für sich noch einmal prüfen, ob sie eine solche, eventuell tiefgreifende automatisierte Sammlung ihrer Persönlichkeitsmerkmale zu ihrer Bewertung durch andere zulassen will. Im nächsten Unterkapitel findet sich ein Vorschlag, wie eine solche Ergänzung der Art. 13 und 14 DSGVO formuliert werden kann.[225]

Das Auskunftsrecht der betroffenen Person sollte um eine Verpflichtung des Verantwortlichen zur Protokollierung aller Empfänger personenbezogener Daten ergänzt werden. Damit einhergehen sollte eine Pflicht zur Bekanntgabe des Protokolls gegenüber der betroffenen Person statuiert werden.[226] Einen Formulierungsvorschlag für eine Protokollierungspflicht in einem neuen Art. 24 Abs. 1 Satz 2 DSGVO und einen Auskunftsanspruch nach Art. 15 Abs. 1 lit. c DSGVO enthält das nächste Unterkapitel.[227]

Nach Art. 15 Abs. 1 lit. h DSGVO hat die betroffene Person einen Anspruch auf „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“. Diese Auskunft muss um die relevanten Merkmale und deren Bedeutung für die automatisierte oder automatisiert vorbereitete Entscheidung ergänzt werden. Nur mit dieser Information kann die betroffene Person ihr Verhalten so einrichten, dass sie Chancen hat, die gewünschte Entscheidung zu erreichen.[228]

Art. 15 Abs. 2 DSGVO sollte um eine Verpflichtung des Verantwortlichen zu einer gesonderten Information für jedes Profiling sowie dessen Umfang, Inhalt, Zielsetzung und Verwendungszweck erweitert werden.[229] Hierzu erfolgt ein Formulierungsvorschlag im nächsten Unterkapitel.[230]

Eine Präzisierung sollte auch das Recht auf eine Kopie erfahren. Es sollte als eigenständiges Recht der betroffenen Person ausgestaltet sein, das sie zusätzlich oder – sofern dadurch alle personenbezogene Daten mitgeteilt werden – ersatzweise zum Anspruch über eine Auskunft über die Daten geltend machen kann. Sollte die Kopie nicht alle Daten der betroffenen Person enthalten, gilt weiterhin die Pflicht zur Mitteilung aller verarbeiteten Daten. Das Recht auf eine Kopie sollte alle personenbezogenen Daten erfassen, die Gegenstand der Verarbeitung sind und in einem Datensatz zusammengefasst sind oder zusammengefasst werden können. Dadurch werden personenbezogene Daten von diesem Anspruch ausgenommen, die nicht nach betroffenen Personen geordnet sind und auch nicht nach diesen strukturiert werden können.[231] Im nächsten Unterkapitel findet sich ein Vorschlag, wie eine solche Präzisierung des Art. 15 Abs. 3 DSGVO formuliert werden kann.[232]

---

225 S. Kap. 2.3.13.
226 S. näher Kap. 2.1.9.1.
227 S. Kap. 2.3.14 und 2.3.21.
228 S. auch Kap. 2.1.9.
229 S. Kap. 2.1.9.2.
230 S. hierzu Kap. 2.3.16.
231 S. Kap. 2.1.9.3.
232 S. Kap. 2.3.17.

Das Recht auf Datenübertragung aus Art. 20 Abs. 1 DSGVO sollte auf alle von der betroffenen Person verursachten Daten ausgeweitet werden.[233] Dies kann durch die Ersetzung des Begriffs „bereitgestellt" durch „verursacht" erfolgen. Zudem sollten Klarstellungen zur Form der Datenübertragung und zum Format, in dem die Daten übergeben werden sollen, erfolgen. Statt unbestimmter Rechtsbegriffe zum Format der Übertragung, sollte festgelegt werden, dass dieses interoperabel sein muss. Die Anforderungen an die Interoperabilität kann aber nicht in der Verordnung selbst erfolgen, sondern sollte dem Europäischen Datenschutzausschuss übertragen werden. Die Norm ist außerdem durch eine Verpflichtung zur Bereitstellung der Daten in der jeweiligen Landessprache des Mitgliedstaates oder in englischer Sprache zu ergänzen.[234] Das Recht auf Datenübertragung sollte auch dann gelten, wenn die Einwilligung oder der Vertrag nicht mehr bestehen, die Daten aber während des Bestehens der Einwilligung oder des Vertrags vom Verantwortlichen erhoben worden sind.[235] Soweit der Unionsgesetzgeber die Vorschrift ändern sollte, ist ein Formulierungsvorschlag für eine Neufassung des Art. 20 Abs. 1 DSGVO im nächsten Unterkapitel zu finden.[236]

Zum Schutz von Kindern sollte bei der Beurteilung eines Widerspruchs nach Art. 21 Abs. 1 DSGVO die Tatsache besonders berücksichtigt werden, dass personenbezogene Daten im Kindesalter erhoben worden sind.[237] Eine entsprechende Ergänzung im Verordnungstext wird im nächsten Unterkapitel vorgeschlagen.[238]

Das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, erfordert mehrere Anpassungen des Normtextes. Zum einen ist das Verbot automatisierter Entscheidungen im Einzelfall zu eng gefasst.[239] Die Einschränkung „ausschließlich" in Art. 22 Abs. 1 DSGVO ist zu streichen. Gleiches gilt für die Einschränkung, dass die Entscheidung der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie „in ähnlicher Weise erheblich" beeinträchtigt. Eine benachteiligende Beeinträchtigung sollte ausreichen. Gleichzeitig ist Art. 22 Abs. 1 DSGVO um ein Verbot zu ergänzen, automatisiert vorbereiteten Entscheidungen ausgeliefert zu sein, die der menschliche Entscheider im Regelfall unbesehen übernimmt, ohne dass die betroffene Person vor der Entscheidung eine Möglichkeit hatte, ihren Standpunkt vorzutragen.[240] Zweitens rechtfertigt sie in Abs. 2 eine automatisierte Entscheidung im Einzelfall, wenn sie für den Abschluss oder eines Vertrags erforderlich ist, ohne dass die betroffene Person dem zustimmen muss. Art. 22 Abs. 2 lit. a DSGVO sollte daher gestrichen werden. Es genügt, wenn der Verantwortliche die betroffene Person um ihre Einwilligung nach Abs. 2 lit. c bitten kann.[241] Außerdem sollte

233 S. hierzu Kap. 2.1.10.1.
234 S. hierzu Kap. 2.1.10.3.
235 S. hierzu Kap. 2.1.10.2.
236 S. Kap. 2.3.18.
237 S. hierzu Kap. 2.1.6.
238 S. Kap. 2.3.19.
239 Zur fehlenden Regulierung der Vorbereitung der automatisierten Entscheidung durch Profiling s. Kap. 2.1.12 und 2.2.2.
240 S. Kap. 2.11.1.1.
241 S. kap. 2.1.11.3.

in Art. 22 Abs. 2 lit. c DSGVO zum Schutz der Kinder die Einwilligung eines Kindes ausgeschlossen werden.[242] Weiterhin sollten gemäß Erwägungsgrund 71 DSGVO und nach dem Vorbild von § 31 BDSG in Art. 22 DSGVO qualitative Anforderungen an eine auf einer automatisierten Verarbeitung beruhenden Entscheidung aufgenommen werden.[243] Schließlich sollte Art. 22 Abs. 3 DSGVO um die Verpflichtung des Verantwortlichen ergänzt werden, bei einer Reklamation die wesentlichen Gründe für die automatisierte Entscheidung zu erläutern.[244] Formulierungsvorschläge für diese Anpassungen des Art. 22 DSGVO werden im nächsten Unterkapitel vorgestellt.[245]

2.2.4 Handlungsbedarf zum vierten Kapitel der Datenschutz-Grundverordnung

Die Vorschrift zum Datenschutz durch Systemgestaltung in Art. 25 Abs. 1 DSGVO erfordert Konkretisierungen dieser Verpflichtungen und eine Ausweitung des Adressatenkreises auf die Hersteller der Technik zur Datenverarbeitung.[246] Die Pflicht zur Systemgestaltung als zentrale Neuerung des Datenschutzrechts kann nur dann volle Wirkung entfalten, wenn klar ist, welche Gestaltungsmaßnahmen in der jeweiligen Branche und für die jeweilige Technikfunktion von den Verantwortlichen gefordert werden können und wenn auch die Hersteller zu diesen gestaltungsmaßnahmen rechtlich bindend verpflichtet werden. Eine die Chancen der Systemgestaltung richtig ausnutzende Umsetzung dieser Forderungen setzt allerdings eine umfassende Neukonzeption eines risikoorientierten Datenschutzes voraus. Erste Überlegungen zu diesen notwendigen Diskussionen werden im nächsten Kapitel vorgestellt.[247] Bis zu einer entsprechenden grundlegenden Überarbeitung der Datenschutz-Grundverordnung kann die Aufgabe zu präzisieren, was bereichs- und technikbezogen Datenschutz durch Systemgestaltung konkret bedeutet und welche Gestaltungsmaßnahmen vom Verantwortliche gefordert werden können, nach und nach auf Unionsebene durch den Europäischen Datenschutzausschuss und auf mitgliedstaatlicher Ebene durch die Aufsichtsbehörden erfolgen. Hierzu sollte die Aufgabenliste des Europäischen Datenschutzausschusses in Art. 70 Abs. 1 DSGVO um diese Aufgabe ergänzt werden. Ein Formulierungsvorschlag hierzu findet sich im nächsten Unterkapitel.[248] Um diesen Stellen auch Konkretisierungen des Datenschutzes durch Systemgestaltung und Voreinstellungen gegenüber Herstellern zu ermöglichen sollte der Text des Art. 25 Abs. 1 und 2 DSGVO um die Hersteller als Adressaten erweitert werden.

In Art. 25 Abs. 1 und 2 DSGVO sollte eine Verpflichtung zum besonderen Schutz der Grundrechte und Interessen von Kindern aufgenommen werden.[249] Eine entsprechende Ergänzung im Verordnungstext wird im nächsten Unterkapitel vorgeschlagen.[250]

Die Plicht der Verantwortlichen zu datenschutzfreundlichen Voreinstellungen in Art. 25 Abs. 2 DSGVO ist zwar bestimmter als die Pflicht zum Datenschutz durch Systemgestaltung in Art. 25

---

242 S. Kap. 2.1.6; s. auch Erwägungsgrund 71 Satz 5 DSGVO.
243 S. Kap. 2.1.11.2
244 S. Kap. 2.1.11.4.
245 S. Kap. 2.3.20.
246 S. hierzu Kap. 2.1.13.
247 S. Kap. 3.3.1.
248 S, Kap. 2.3.27.
249 S. hierzu Kap. 2.1.6.
250 S. Kap. 2.3.22.

Abs. 1 DSGVO. Die Voreinstellungen für den Nutzer an der Erforderlichkeit der Verarbeitung für den jeweiligen Verarbeitungszweck auszurichten, lässt dem Verantwortlichen jedoch sehr große Freiheiten, durch die Bestimmung des Zwecks die Voreinstellungen so zu wählen, dass er durch diese die gewünschten Daten erhalten kann. Auch hier sind daher Präzisierungen erforderlich, welche Voreinstellungen von dem Verantwortlichen gefordert werden können.[251]

Hier sind zwei Ansatzpunkte möglich. Zum einen sollte die Vorschrift so angepasst werden, dass der Zweck auf die Funktionalität des jeweiligen Dienstes beschränkt wird. Diese Anpassung kann sich an die Bestimmung des Vertragszwecks ihm Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO orientieren.[252] Zudem ist das Prinzip der Datenvermeidung in die Norm aufzunehmen. Ein entsprechender Vorschlag zur Ergänzung im Verordnungstext erfolgt im nächsten Unterkapitel.[253]

Zum anderen sind für wichtige Anwendungsfelder und Technikfunktionen Präzisierungen zu treffen, welche Voreinstellungen vom Verantwortlichen gefordert werden können. Diese Konkretisierungen des Datenschutzes durch Voreinstellungen sollten ebenfalls in eine Neukonzeption eines risikoorientierten Datenschutzes eingehen. Erste Überlegungen zu diesen notwendigen Diskussionen werden im nächsten Kapitel vorgestellt.[254] Bis zu einer entsprechenden grundlegenden Überarbeitung der Datenschutz-Grundverordnung kann die Aufgabe, die Pflicht zu Voreinstellungen bereichs- und technikbezogen zu präzisieren, von den Aufsichtsbehörden, den mitgliedstaatlichen Gesetzgebern (für einzelne Technikbereiche), dem Europäischen Datenschutzausschuss oder von Verbänden übernommen werden. Für den Europäischen Datenschutzausschuss sollte die Liste seiner Aufgaben in Art. 70 Abs. 1 DSGVO ergänzt werden. Diese Ergänzung kann mit der Aufgabe zur Präzisierung des Datenschutzes durch Systemgestaltung zusammengezogen werden. Ein Formulierungsvorschlag wird im nächsten Unterkapitel präsentiert.[255]

Eine Arbeitsteilung in der Datenverarbeitung – insbesondere im Kontext automatisierter Entscheidungen im Einzelfall – darf nicht dazu führen, dass Informationen über die Datenverarbeitung unterbleiben oder verkürzt werden.[256] Daher sollten bei arbeitsteiligen Datenverarbeitungsverfahren die Verantwortlichen nach Art. 26 Abs. 1 DSGVO verpflichtet sein, ihre Informationen so abzustimmen, dass jeder Kooperationspartner über seinen Anteil am Verfahren samt den Schnittstellen zu allen anderen Anteilen informiert.[257] Im nächsten Unterkapitel findet sich ein Vorschlag, wie eine solche Präzisierung des Art. 15 Abs. 3 DSGVO formuliert werden kann.[258]

In Art. 34 Abs. 2 DSGVO sollte eine Verpflichtung zur Berücksichtigung des Verständnisvermögens und der Hilflosigkeit von Kindern bezogen auf Form und Inhalt der Benachrichtigung

---

251 S. hierzu Kap. 2.1.14.
252 S. hierzu Kap. 2.2.2 und Kap. 2.3.4.
253 S. Kap. 2.3.23.
254 S. Kap. 3.3.1.
255 S. Kap. 2.3.27.
256 S. z.B. Specht-Riemenschneider/Schneider, ZD 2019, 503 (505 f.).
257 S. hierzu Kap. 2.1.8.3.
258 S. Kap. 2.3.24.

aufgenommen werden.[259] Eine entsprechende Ergänzung der Vorschrift wird im nächsten Unterkapitel vorgeschlagen.[260]

In Art. 35 DSGVO sollte eine Verpflichtung zu besonderer Berücksichtigung der Grundrechte und Interessen von Kindern bei der Bestimmung der Notwendigkeit einer Datenschutz-Folgenabschätzung sowie bei der Risikoanalyse und bei der Festlegung von Schutzmaßnahmen aufgenommen werden.[261] Das nächste Unterkapitel enthält einen Vorschlag, wie die Vorschrift ergänzt werden könnte.[262]

2.2.5 Handlungsbedarf zum sechsten Kapitel der Datenschutz-Grundverordnung

Anpassungen des Normtextes in Kapitel 5, 6 und 7 DSGVO sind im Kontext der Stärkung der Stellung von Verbrauchern nicht unmittelbar erforderlich. Allerdings ist indirekt wegen zusätzlicher Zuweisungen von neuen Aufgaben für den Europäischen Datenschutzausschuss die Auflistung seiner Aufgaben in Art. 70 Abs. 1 DSGVO um zwei Aufgaben zu ergänzen.[263] Vorschläge zur Formulierung dieser ergänzenden Aufgaben enthält das nächste Unterkapitel.[264]

Diese zusätzlichen Aufgaben und die Überlastung durch die bereits bestehenden, durch die Datenschutz-Grundverordnung aber neu entstandenen Aufgaben machen eine weitere starke personelle Aufstockung der Aufsichtsbehörden dringend erforderlich.[265] Insbesondere muss die Union dafür sorgen, dass der Europäische Datenschutzausschuss seine Aufgaben zügiger als bisher bearbeiten kann. Diese setzt auch voraus, dass die Datenschutzaufsichtsbehörden in Deutschland in die Lage versetzt werden, in den Arbeitskreisen des Europäischen Datenschutzausschusses intensiv mitzuwirken. Für diese Ressourcenfrage sind der Bund und die Bundesländer verantwortlich.

2.2.6 Handlungsbedarf zum achten Kapitel der Datenschutz-Grundverordnung

Auch die Sanktionsvorschriften in Kapitel 8 DSGVO benötigen Anpassungen. Zu fordern ist eine Präzisierung der Bußgeldtatbestände durch eine Leitlinie des Ausschusses nach Art. 70 Abs. 1 Satz 2 lit. k DSGVO sowie eine Präzisierung durch unverbindliche Bußgeldkataloge der mitgliedstaatlichen Aufsichtsbehörden. Dies ist eine Aufgabe der Datenschutzaufsichtsbehörden und ihrer Konferenz.

Die Aufsichtsbehörden sollten zur Veröffentlichung einer jährlichen Statistik zu ihrer Bußgeldpraxis verpflichtet werden. Dies sollte der Unionsgesetzgeber unionsweit einheitlich in einem neuen Absatz des Art. 83 DSGVO festlegen. Ein Formulierungsvorschlag für diese Ergänzung findet sich im nächsten Unterkapitel.[266]

---

259 S. hierzu Kap. 2.1.6.
260 S. Kap. 2.3.25.
261 S. hierzu Kap. 2.1.6.
262 S. Kap. 2.3.26.
263 S. hierzu Kap. 2.1.10 und 2.1.13.
264 S. Kap. 2.3.27.
265 S. Kap. 2.1.15.
266 S. Kap. 2.3.28.

Die deutschen Gesetzgeber sollten prüfen, ob Bußgelder direkt in den Haushalt der jeweiligen Aufsichtsbehörde einfließen können. Zudem sollte eine Kostenübernahme anfallender Prozesskosten durch den Bund und die Länder erfolgen.

2.3 Regelungsvorschläge

Soweit dieses Gutachten Änderungen einzelner Vorschriften der Datenschutz-Grundverordnung vorschlägt, werden in diesem Unterkapitel Formulierungsvorschläge zur Diskussion gestellt, um erkennen zu können, wie Verbesserungen dieser Vorschriften aussehen könnten.

2.3.1 Aufenthaltsprinzip

Um den räumlichen Anwendungsbereich der Datenschutz-Grundverordnung entsprechend einer konsequenten Anwendung des Aufenthaltsprinzips auf jede Form der Verarbeitung personenbezogener Daten von betroffenen Personen auszuweiten, die sich in der Europäischen Union aufhalten, wird folgende Änderung des Art. 3 Abs. 2 lit. a DSGVO empfohlen:

> „(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht,
>
> a) betroffenen ~~en~~ Personen in der Union ~~Waren oder Dienstleistungen anzubieten~~*anzusprechen*, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;“

Indem das Angebot von Waren und Dienstleistungen nicht mehr gefordert wird, ist eine Abgrenzung dieses Angebots von anderen Tätigkeiten nicht mehr erforderlich. Der Kreis der erfassten Verantwortlichen oder Auftragsverarbeiter wird dadurch erweitert, dass jede Ansprache einer Person in der Union für die Anwendung der Verordnung ausreicht. Zugleich erfolgt keine Anwendung der Verordnung, wenn die Initiative für die letztliche Verarbeitung personenbezogener Daten nicht von dem Verantwortlichen oder Auftragsverarbeiter ausgeht, sondern von der betroffenen Person selbst.

2.3.2 Datenschutzrechtliche Grundsätze

Um in der deutschen Fassung des Art. 5 Abs. 1 lit. a DSGVO den zweiten Grundsatz mit einer ihm gemäßen Bezeichnung auszuweisen und eine Verwirrung bezogenen auf den zivilrechtlichen Begriff von „Treu und Glauben“ zu vermeiden, wird folgende Änderung des Art. 5 Abs. 1 lit. a DSGVO empfohlen:

> „(1) Personenbezogene Daten müssen
>
> a) auf rechtmäßige Weise, *fair* ~~nach Treu und Glauben~~ und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, *Fairness* ~~Verarbeitung nach Treu und Glauben~~, Transparenz“);“

Um den Grundsatz der Datenminimierung um den Grundsatz der Datenvermeidung zu ergänzen, wird folgende Änderung des Art. 5 Abs. 1 lit. c DSGVO empfohlen:

> „(1) Personenbezogene Daten müssen …

> c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“) *und in Datenverarbeitungssystemen verarbeitet werden, deren Auswahl und Gestaltung an dem Ziel ausgerichtet sind, so wenig personenbezogene Daten wie möglich zu verarbeiten (Datenvermeidung)*;“

Durch die Formulierung „so wenig personenbezogene Daten wie möglich zu verarbeiten“ wird das Verhältnismäßigkeitsprinzip zur Geltung gebracht. Entscheidend ist, dass nicht nur Datenminimierung nach einem Zweck, den der Verantwortliche ausgewählt hat, stattfindet, sondern Vermeidung der Verarbeitung personenbezogener Daten durch Systemgestaltung unter Einbeziehung des Zwecks.

2.3.3 Vorrang der Einwilligung

Um klarzustellen, dass ein Verantwortlicher sich neben einer Einwilligung nicht zusätzlich auf einen anderen gesetzlichen Erlaubnistatbestand berufen kann, wird folgende Änderung des Art. 6 Abs. 1 UAbs. 1 DSGVO vorgeschlagen:

> „(1) Die Verarbeitung ist nur rechtmäßig, wenn ~~mindesten eine der nachstehenden Bedingungen erfüllt ist a) Die~~ *entweder die* betroffene Person ~~hat~~ ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben *hat oder* ~~,~~ eine der nachstehenden Bedingungen erfüllt ist:
>
> ~~b~~ *a*) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen; …“

Durch die Anpassungen wird klargestellt, dass die Einwilligung und die anderen gesetzlichen Erlaubnistatbestände nur alternativ genutzt werden können. Indem ein „entweder – oder“ eingefügt und dadurch die Einwilligung von den gesetzlichen Erlaubnistatbeständen abgehoben und das „mindestens“ gestrichen wird, ist es ausgeschlossen, die Einwilligung mit den gesetzlichen Erlaubnistatbeständen gleichzusetzen und sie mit ihnen zu kombinieren. Es gibt nach der Änderung nur noch zwei – sich gegenseitig ausschließende – Wege, die Datenverarbeitung zu rechtfertigen. Dadurch wird verhindert, dass ein Verantwortlicher, nachdem er eine Einwilligung eingeholt hat, die Datenverarbeitung auf einen anderen Erlaubnistatbestand stützen kann. Wer eine Einwilligung einholt, muss auch die Regelungen zur Einwilligung gegen sich gelten lassen.

2.3.4 Bestimmung des Vertragszwecks

Um den Erlaubnistatbestand des bisherigen Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO zu objektivieren und zu präzisieren, wird folgende Änderung des Normtextes vorgeschlagen:

> „b) die Verarbeitung ist *objektiv* für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;“

Durch die Bezugnahme auf die objektive Erforderlichkeit der Verarbeitung personenbezogener Daten für die Erfüllung eines Vertrages, wird die Erlaubnis nur an die funktionale Notwendigkeit für die vereinbarte Leistung geknüpft. Es ist nicht mehr möglich, durch Vertragsformulierungen darüberhinausgehende Datenverarbeitungen zu rechtfertigen, die – wie die Information befreundeter Unternehmen oder die Information des Kunden über weitere Produkte – nicht für die Erfüllung der vertraglichen Hauptpflichten erforderlich sind. Diese Datenverarbeitungen sind nur möglich, wenn sie durch überwiegende berechtigte Interessen gerechtfertigt sind oder die betroffene Person eingewilligt hat.

2.3.5 Prüfung der Vereinbarkeit von Verarbeitungszwecken

Um bei der Prüfung der Vereinbarkeit eines alten mit einem neuen Zweck auch den Umstand gebührend zu berücksichtigen, dass es sich um personenbezogene Daten eines Kindes handelt, sollte Art. 6 Abs. 4 UAbs. 1 lit. d DSGVO um die Beachtung dieses Umstands ergänzt werden.

> „d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen, *insbesondere wenn es sich um die personenbezogenen Daten eines Kindes handelt*;“

Durch die Ergänzung wird der Verantwortliche bei einer Zweckänderung verpflichtet, den Folgen der Weiterverarbeitung für Kinder besondere Beachtung zu schenken. Diese Pflicht ist bisher dem aktuellen Normtext allenfalls implizit zu entnehmen (über Erwägungsgrund 38 Satz 1 DSGVO) und sollte zur Stärkung der Stellung von Kindern im Datenschutz explizit in den Normtext aufgenommen werden.

2.3.6 Ausschluss der Einwilligung eines Kindes in Werbung und Profiling

Um die Wertung des Erwägungsgrundes 38 Satz 2 DSVO in den Normtext des Art. 8 Abs. 1 DSGVO zu übernehmen,[267] wird die Ergänzung um einen neuen Satz 2 vorgeschlagen:

> „Dies gilt nicht für die Verarbeitung personenbezogener Daten eines Kindes für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen.“

Satz 2 wird zu Satz 3. Mit der Ergänzung wird Erwägungsgrund 38 Satz 2 DSGVO von einer Auslegungshilfe zu direkt anwendbarem Recht und stärkt damit die Rechtssicherheit.

2.3.7 Ausschluss der Einwilligung eines Kindes in die Verarbeitung besonderer Kategorien personenbezogener Daten

Für Kinder soll eine Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 2 lit. a DSGVO ausgeschlossen sein, um sie in ausreichender Weise gegen das Eingehen besonderer Risiken zu schützen.[268] Hierzu wird die Ergänzung um ein Wort vorgeschlagen:

> „a) Die *erwachsene* betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann

[267] S. Kap. 2.1.6.
[268] S. Kap. 2.1.6.

> das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,“

Diese Ergänzung bewirkt, dass sich niemand auf die persönliche Einwilligung eines Kindes in die besonders riskante Verarbeitung von besonderen Kategorien personenbezogener Daten berufen kann. Die Einwilligung der Erziehungsberechtigten bleibt möglich.

2.3.8 Beschränkung der Information auf die nächstfolgende Datenverarbeitung

Um die Pflicht zur Information der betroffenen Person über die sie betreffende Datenverarbeitung erfüllen zu können, sollen immer nur die Informationen über die Datenverarbeitungen zulässig sein, die vollständig und präzise mit allen notwendigen Angaben beschrieben werden können.[269] Hierzu wird folgende Änderung des Normtextes in Art. 12 Abs. 1 DSGVO vorgeschlagen:

> „(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die *aktuelle* Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.“

Die Einfügung des Wortes „aktuelle“ stellt klar, dass die Information sich auf die gegenwärtig vorgesehene Datenverarbeitung beziehen soll, für die Umfang, Zweck und Verfahren feststehen und vollständig bekannt sind. Dadurch wird verhindert, die Informationspflicht zu erfüllen, indem auf eine Datenschutzerklärung verwiesen wird, in der alle denkbaren künftigen Datenverarbeitungen mit vagen Hinweisen auf künftige Möglichkeiten zusammengefasst sind. Künftige Änderungen in der Datenverarbeitung, die nicht bereits festgelegt sind und daher nicht präzise beschrieben werden können, müssen zu neuen, dann wiederum aktuellen, Informationen führen.

Begleitet werden sollte die Änderung durch eine Klarstellung in Erwägungsgrund 60 DSGVO, dass eine hohe Komplexität der Datenverarbeitung eine mangelhafte Information nicht entschuldigt.

2.3.9 Ausgleich zwischen Informationspflicht und Geheimnisschutz

Um beim Schutz von rechtlich anerkannten Geheimnissen und Rechten des geistigen Eigentums dennoch das höchstmögliche Maß an Informationen über die Datenverarbeitung zu geben, sollte der Verantwortliche verpflichtet werden, nach Wegen zu suchen, wie möglichst umfangreiche und genaue Informationen gegeben werden können, ohne das Geheimnis zu verletzen.[270] Hierzu sollte Art. 12 DSGVO um eine solche Grundregel zur praktischen Konkordanz zwischen Information und Geheimnis in einem neuen Abs. 7 ergänzt werden:

---

269 S. Kap. 2.1.7.1.
270 S. Kap. 2.1.8.2.

„*(7) Gefährden die der betroffenen Person bereitzustellenden Informationen die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums, so stellt der Verantwortliche unter Wahrung dieser Rechte und Freiheiten ein möglichst hohes Maß an Information sicher.*"

Die bisherigen Absätze 7 und 8 werden zu Absätzen 8 und 9. Durch die Ergänzung um eine neue Grundregel zur Auflösung des Konflikts zwischen Informationsanspruch und Geheimnisschutz gilt für alle Informationen des Verantwortlichen über die Datenverarbeitung gegenüber der betroffenen Person. Sie wird insbesondere das Informationsniveau bei automatisierter Entscheidungsfindung verbessern.

Entsprechend der Neufassung des Abs. 7 des Art. 12 DSGVO müssen die Erwägungen in Erwägungsgrund 63 Satz 5 und 6 DSGVO[271] der neuen Grundregel angepasst werden. Hier könnten Verweise auf angemessene Verfahren zum Schutz von Geschäftsgeheimnissen oder Rechten des geistigen Eigentums (z.B. „Verrauschen") angeführt werden. Auch ein Verschieben in Erwägungsgrund 58 oder 60 DSGVO bietet sich an.

2.3.10 Zeitnahe relevante Information über die Datenerhebung

Um sicherzustellen, dass der Verantwortliche der betroffenen Person jeweils „zum Zeitpunkt der Erhebung" die damit verbundenen relevanten Informationen gibt,[272] sollte der Wortlaut der Eingangsworte des Art. 13 Abs. 1 und Abs. 2 DSGVO wie folgt ergänzt werden:

„(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person *jeweils* zum Zeitpunkt der Erhebung dieser Daten Folgendes *zu dieser Erhebung* mit: …"

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person *jeweils* zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen *zu dieser Erhebung* zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

Durch die Ergänzungen wird sichergestellt, dass die Information zum richtigen Zeitpunkt und damit situationsadäquat erfolgt, nämlich zum Zeitpunkt der Datenerhebung und vor einer notwendigen oder möglichen Entscheidung der betroffenen Person. Dies stärkt die Selbstbestimmung der betroffenen Person und erhöht insbesondere die Transparenz komplexer Verarbeitungsvorgänge.

2.3.11 Information über Empfänger

Um eine ausreichende Information über die Empfänger personenbezogener Daten zu bieten, die der betroffenen Person die Rechtsverfolgung erst ermöglicht, zumindest aber erheblich erleichtert,[273] sollte der Wortlaut des Art. 13 Abs. 1 lit. e DSGVO leicht angepasst werden:

„e) gegebenenfalls die Empfänger*, soweit sie bestimmbar sind,* oder Kategorien von Empfängern der personenbezogenen Daten;"

---

271 S. zu diesen Kap. 2.1.8.2.
272 S. Kap. 2.1.7.3.
273 S. Kap. 2.1.8.

Die gleiche Änderung sollte in der wortgleichen Regelung des Art. 14 Abs. 1 lit. e DSGVO erfolgen.

Durch die Ergänzung wird der Verantwortliche verpflichtet, alle ihm bekannten Empfänger personenbezogener Daten zu benennen. Er kann sich, sofern es ihm möglich ist, einen Empfänger konkret zu benennen, nicht darauf zurückziehen, lediglich Kategorien von Empfängern zu nennen. Die Angabe von Kategorien von Empfängern ist mithin nur zulässig, wenn ein konkreter Empfänger zum Zeitpunkt der Information (noch) nicht benannt werden kann.

2.3.12 Information bei automatisierten Entscheidungsverfahren

Um den Streit über den Umfang der Informationen zu beseitigen, die ein Verantwortlicher über das Bestehen einer automatisierten Entscheidungsfindung zu geben hat, sollte der Gesetzestext in Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO präzisiert werden.

> „f/g) das Bestehen einer automatisierten Entscheidungsfindung ~~einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4~~ und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik *einschließlich der Kriterien für die Entscheidung und ihre Gewichtung* sowie die Tragweite und die angestrebten *und möglichen rechtlichen und tatsächlichen* Auswirkungen einer derartigen Verarbeitung für die betroffene Person.“

Die Ergänzung stärkt die Interessen des Verbrauchers, der künftig über die bereitzustellenden Informationen einen deutlich besseren Einblick in automatisierte Entscheidungsverfahren erhält. Insbesondere soll er erkennen können, welche Kriterien wie die Entscheidung beeinflussen. Zudem erfährt er, welche Auswirkungen die Datenverarbeitung auf ihn hat. Zu Profiling wird im Folgenden eine eigene Regelung vorgeschlagen. Die Streichung von „gemäß Artikel 22 Absätze 1 und 4“ erfolgt, weil diese Formulierung zu der Verwirrung führen kann, dass die Informationspflicht nur gilt, wenn die Datenverarbeitung auf den Absätzen 1 und 4 beruht, nicht jedoch, wenn die Datenverarbeitung von den Absätzen 2 und 3 geregelt wird.

Ferner darf eine Arbeitsteilung im Kontext automatisierter Entscheidungen im Einzelfall nicht dazu führen, dass Informationen über dieses Verfahren unterbleiben oder verkürzt werden. Daher sollten bei arbeitsteiligen automatisierten Entscheidungsverfahren die Verantwortlichen verpflichtet sein, ihre Informationen so abzustimmen, dass jeder Kooperationspartner über seinen Anteil am Verfahren samt den Schnittstellen zu allen anderen Anteilen informiert.[274]

2.3.13 Information über Profiling

Um bei jeder Erhebung von Daten, die auch für Profiling genutzt werden sollen, die betroffene Person ausreichend über dieses zusätzliche Risiko der Datenverarbeitung zu informieren, sollten Art. 13 Abs. 2 DSGVO um einen neuen lit. g und Art. 14 Abs. 2 DSGVO um einen gleichlautenden lit. h ergänzt werden.

> „*g/h) die Verwendung der Daten für Profiling sowie dessen Umfang, Inhalt, Zielsetzung und Verwendungszweck.*“

[274] S. zu diesem Vorschlag Kap. 2.3.24.

Durch die Ergänzungen wird die Transparenz der Verarbeitung erhöht. Insbesondere soll die betroffene Person klar erkennen können, welche möglichen Spätfolgen sich aus der Verarbeitung durch Profiling ergeben können. Ein Verbraucher soll so leichter entscheiden können, ob er Profiling anstrebt oder duldet und einen Dienst auswählt, der dieser Entscheidung entspricht.

2.3.14 Auskunft über Empfänger

Um eine ausreichende Auskunft über die Empfänger personenbezogener Daten zu gewährleisten, die der betroffenen Person die Rechtsverfolgung erst ermöglicht, zumindest aber erheblich erleichtert,[275] sollte in Art. 24 Abs. 1 DSGVO ein neuer Satz 2 eine Verpflichtung zur Protokollierung der Übertragung und der Empfänger begründen und sollte der Wortlaut des Art. 15 Abs. 1 lit. c DSGVO – entsprechend der Neufassung des 13 Abs. 1 lit. e DSGVO und Art. 14 Abs. 1 lit. f DSGVO – leicht angepasst werden:

> „c) die Empfänger*, soweit sie bestimmbar sind,* oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;“

Durch die Ergänzung wird sichergestellt, dass der Verantwortliche alle ihm bekannten Empfänger mit Namen und Kontaktmöglichkeit der betroffenen Person mitteilen muss. Damit ihm die Übertragungen und die Empfänger im Regelfall bekannt sind, begründet der neue Satz 2 von Art. 24 Abs. 1 DSGVO eine Pflicht, die Übertragungen und die Empfänger zu protokollieren.[276]

2.3.15 Auskunft über automatisierte Entscheidungsverfahren

Um den Streit über den Umfang der Auskunft zu beseitigen, die ein Verantwortlicher über das Bestehen einer automatisierten Entscheidungsfindung zu geben hat, sollte der Gesetzestext in Art. 15 Abs. 1 lit. h DSGVO – entsprechend der vorgeschlagenen Ergänzungen der Informationspflichten in Art. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO – präzisiert werden:

> „h) das Bestehen einer automatisierten Entscheidungsfindung ~~einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4~~ und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik *einschließlich der Kriterien für die Entscheidung und ihre Gewichtung* sowie die Tragweite und die angestrebten *und möglichen rechtlichen und tatsächlichen* Auswirkungen einer derartigen Verarbeitung für die betroffene Person.“

Durch die Ergänzung werden die vorgeschlagenen Änderungen der Informationspflichten[277] des Verantwortlichen auch auf das Auskunftsrecht erstreckt. Dies stellt Konsistenz im Gefüge der Betroffenenrechte her und schließt Schutzlücken, die entstünden, wenn die Erstreckung unterbliebe. Zu Profiling wird im Folgenden eine eigene Regelung vorgeschlagen. Die Streichung von „gemäß Artikel 22 Absätze 1 und 4“ erfolgt auch hier, weil diese Formulierung zu der Verwirrung führen kann, dass die Informationspflicht nur gilt, wenn die Datenverarbeitung auf

---

275 S. Kap. 2.1.9.
276 S. Kap. 2.3.21.
277 S. Kap. 2.3.12.

den Abs. 1 und 4 beruht, nicht jedoch, wenn die Datenverarbeitung von den Abs. 2 und 3 geregelt wird.

2.3.16 Auskunft über Profiling

Um bei jeder Verarbeitung von Daten, die für Profiling genutzt werden, der betroffenen Person ein diesem zusätzlichen Risiko ausreichendes Auskunftsrecht zu geben, sollte Art. 15 Abs. 1 DSGVO – vergleichbar zur Informationspflicht nach Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO um einen lit. i ergänzt werden.

> „i*) die Verwendung der Daten für Profiling sowie* ***dessen Umfang, Inhalt, Zielsetzung und Verwendungszweck****.*“

Durch die Ergänzung wird zu den vorgeschlagenen Regelungen in Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO[278] ein Komplementär im Auskunftsrecht geschaffen. Auch hier geht es darum, Konsistenz herzustellen und das Entstehen von Schutzlücken zu vermeiden.

2.3.17 Recht auf eine Kopie

Um die meisten Streitfragen um das Recht auf eine Kopie nach Art. 15 Abs. 3 DSGVO zu beseitigen, sollte die Regelung neu gefasst werden:

> „Der Verantwortliche stellt a*uf Antrag der betroffenen Person* eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind *und in einem Datensatz zusammengefasst sind oder zusammengefasst werden können*, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.“

Durch die Ergänzung wird bezogen auf das Recht auf Kopie Rechtsklarheit geschaffen. Das Recht auf Kopie wird dadurch für die Praxis handhabbar gemacht. Der Zusatz „auf Antrag der betroffenen Person“ erlaubt es einerseits der betroffenen Person bei Wahrnehmung des Rechts auf Auskunft besser zu skalieren, andererseits erleichtert es dem Verantwortlichen seinen Pflichten nachzukommen, indem ihm klar signalisiert wird, was die betroffene Person von ihm erwartet. Der Zusatz „und in einem Datensatz zusammengefasst sind oder zusammengefasst werden können“ konzentriert den Anspruch auf die Gegenstände der Datenverarbeitung, die sich gezielt mit der betroffenen Person befassen oder einer Befassung zugrunde liegen können.

2.3.18 Recht auf Datenübertragung

Die Vorschrift des Art. 20 Abs. 1 DSGVO sollte an mehreren Stellen präzisiert oder um wichtige Festlegungen ergänzt werden, um ihre Umsetzung in der Praxis zu ermöglichen. Ihr Anwendungsbereich sollte auf alle von der betroffenen Person verursachten Daten ausgeweitet werden. Zum Format, in dem die Daten zu übergeben sind, sollte klargestellt werden, dass es interoperabel sein muss. Die Anforderungen an die Interoperabilität sollte der Europäische Datenschutzausschuss festlegen. Außerdem sollte der Verantwortliche verpflichtet werden, die

[278] S. Kap. 2.3.13.

Daten in der jeweiligen Landessprache des Mitgliedstaates oder in englischer Sprache bereitzustellen. Das Recht auf Datenübertragung sollte auch dann gelten, wenn die Einwilligung oder der Vertrag nicht mehr bestehen, die Daten aber während des Bestehens der Einwilligung oder des Vertrags vom Verantwortlichen erhoben worden sind.[279] Um diese Änderungen umzusetzen, sollte Art. 20 Abs. 1 DSGVO angepasst und um einen neuen Satz 2 ergänzt werden.

Artikel 20

Recht auf Datenübertrag~~barkeit~~*ung*

„(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, ~~die~~ deren Erhebung ~~sie~~ bei einem Verantwortlichen *sie verursacht* ~~bereitgestellt~~ hat, in einem ~~strukturierten, gängigen und maschinenlesbaren~~ *interoperablen* Format *und in der jeweiligen Landessprache des Mitgliedstaates der betroffenen Person oder in englischer Sprache* zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

a) die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht *oder beruhte* und

b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Die Bedingungen für die Interoperabilität der Formate bestimmt der Europäische Datenschutzausschuss."

Die Bezeichnung des Rechts auf „Übertragbarkeit" suggeriert ein Recht auf eine doppelte Potentialität: Sowohl die Endung „bar" als auch die Endung „keit" bezeichnen nur die Möglichkeit. Das Recht auf eine Möglichkeit der Übertragung hilft der betroffenen Person jedoch nicht weiter, wenn sie über die Möglichkeit hinaus auch eine tatsächliche Übertragung durchsetzen will. Daher sollte die Überschrift korrigiert werden. Das Ziel der Ausweitung des Anwendungsbereichs des Rechts auf Datenübertragung wird durch eine Ersetzung des Begriffs „bereitgestellt" durch „verursacht" erreicht. Der Streit um die unbestimmten Rechtsbegriffe „strukturiertes gängiges und maschinenlesbares Format" und „technisch machbar" wird durch eine Streichung dieser Begriffe aus der Norm beigelegt. Sie gehen in der Forderung eines interoperablen Formats auf. Die Präzisierung der Bedingungen für die Interoperabilität wird dem Europäischen Datenschutzausschuss auferlegt. Damit wird einerseits sichergestellt, dass eine (notwendige) Präzisierung tatsächlich erfolgt, andererseits kann so bei der Präzisierung ein Detailgrad erreicht werden, der im Normtext oder in den Erwägungsgründen nicht möglich ist.

2.3.19 Schutz von Kindern im Rahmen eines Widerspruchs

Um bei der Prüfung eines Wiederspruchs nach Art. 21 Abs. 1 DSGVO den Umstand gebührend zu berücksichtigen, dass es sich um personenbezogene Daten eines Kindes handelt, sollte diese Vorschrift entsprechend ergänzt werden.

[279] S. Kap. 2.1.10.

„(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, *insbesondere wenn es sich um die personenbezogenen Daten eines Kindes handelt,* jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen."

Durch die Ergänzung erfolgt eine Erwägungsgrund 38 Satz 1 DSGVO entsprechende Stärkung von Kindern bei der Verarbeitung personenbezogener Daten, indem eine Klarstellung zum Begriff „ihrer besonderen Situation" direkt im Normtext stattfindet.

2.3.20 Automatisierte Entscheidungen im Einzelfall

Das in Art. 22 DSGVO normierte Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, erfordert mehrere Anpassungen des Normtextes.[280] Zum einen ist das Verbot automatisierter Entscheidungen im Einzelfall weiter zu fassen.[281] Zum anderen sollte nicht der Verantwortliche oder ein Dritter rechtfertigend festlegen können, dass die automatisierte Entscheidung im Einzelfall erforderlich ist. Es genügt, wenn der Verantwortliche die betroffene Person um ihre Einwilligung nach Abs. 2 lit. c bitten kann. Drittens sollte neben der Auskunftspflicht festgelegt werden, dass die Entscheidungsgründe der betroffenen Person erläutert werden. Schließlich sollte in Abs. 2 lit. c zum Schutz der Kinder die Einwilligung eines Kindes ausgeschlossen werden. Schließlich sollten qualitative Anforderungen an eine auf einer automatisierten Verarbeitung beruhenden Entscheidung aufgenommen werden. Diese Anpassungen des Art. 22 DSGVO könnten in folgender Weise erfolgen:

„(1) Die betroffene Person hat 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~~ *erheblicher* Weise ~~erheblich~~ beeinträchtigt.

(2) Absatz 1 gilt nicht, wenn die Entscheidung

~~a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,~~

a~~b~~) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

[280] S. hierzu Kap. 2.1.11 und 2.2.3.
[281] Zu dem die automatisierte Entscheidung vorbereitenden Profiling s. Kap. 2.1.12 und 2.2.3.

b~~e~~) mit ausdrücklicher Einwilligung der *erwachsenen* betroffenen Person erfolgt.

(3) In den in Absatz 2 ~~Buchstaben a und c~~ genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts*,* ~~und~~ auf Anfechtung der Entscheidung *und die Erläuterung der Entscheidungsgründe* gehört.

(4) Die Erstellung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck einer auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung ist nur zulässig, wenn die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind."

Abs. 4 wird zu Abs. 5. Durch die Anpassungen in Abs. 1 wird die doppelte Einschränkung des Rechts aus Art. 22 Abs. 1 DSGVO zurückgenommen. Die Ausweitung (Streichung von „ausschließlich") und die Absenkung der Schwelle (erhebliche Beeinträchtigung anstelle von rechtlicher Wirkung oder Ähnlichem) haben zur Folge, dass zahlreiche bislang nicht erfasste Grundrechtsbeeinträchtigungen von Verbrauchern eingeschlossen werden. Dadurch wird deren Stellung im Datenschutzrecht verbessert und der Unionsgesetzgeber kann seinen grundrechtlichen Schutzpflichten gerecht werden. Erfasst ist nun auch die durch eine automatisierte Verarbeitung vorbereitete Entscheidung. Dies bedeutet, dass die betroffene Person nicht mehr einer automatisiert vorbereiteten Entscheidung ausgeliefert ist, die der menschliche Entscheider im Regelfall unbesehen übernimmt, ohne dass die betroffene Person eine Möglichkeit hat, ihren Standpunkt vor der Entscheidung vorzutragen.

Die Streichung in Abs. 2 bewirkt letztlich einen Abbau von Machtasymmetrien zwischen Anbieter und Verbraucher und schließt Schutzlücken der Verordnung. Wird Abs. 2 lit. a gestrichen, so ist es nicht länger möglich, dass der Verantwortliche oder ein Dritter einseitig die Erforderlichkeit einer automatisierten Entscheidung im Kontext eines Vertrages erklärt.

Diese Ergänzung von Abs. 2 lit. b („erwachsene") bewirkt, dass sich niemand auf die persönliche Einwilligung eines Kindes in die besonders riskante automatisierte Entscheidung berufen kann. Die Einwilligung der Erziehungsberechtigten bleibt möglich. Die Ergänzung ist im Zusammenhang mit der vorgeschlagenen Ergänzung von Art. 9 Abs. 2 lit. a DSGVO zu sehen und greift die Wertung von Erwägungsgrund 71 Satz 5 DSGVO auf.

Die Ergänzung des Ab. 3 bewirkt, dass im Fall einer Reklamation der Verantwortliche zusätzliche Transparenzpflichten hat. Er muss der betroffenen Person die wesentlichen Gründe der automatisiert getroffenen Entscheidung und deren Auswirkungen erläutern.

Die Einfügung des neuen Abs. 4 hat zur Folge, dass qualitative Anforderungen an automatisierte Entscheidungsfindungen festgesetzt werden. Der neue Abs. 4 greift die Erwägungen aus Erwägungsgrund 71 DSGVO auf und orientiert sich in seinem Wortlaut und Normzweck an §

31 Abs. 1 BDSG, ist jedoch nicht wie diese Vorschrift auf Scoring und Bonitätsauskünfte beschränkt.

2.3.21 Protokollierung der Datenübertragungen und der Empfänger

Um bei einer Auskunft der betroffenen Person die Empfänger ihrer personenbezogenen Daten mitteilen zu können, wird der Verantwortliche verpflichtet, die Empfänger und die ihnen übertragenen Daten zu protokollieren. Für die Begründung dieser Verpflichtung ist eine Ergänzung des Art. 24 Abs. 1 DSGVO um einen neuen Satz 2 erforderlich:

> „(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. *Er protokolliert die Übertragungen personenbezogener Daten an Dritte und deren Empfänger.* Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert."

Der bisherige Satz 2 wird zum neuen Satz 3. Durch die Ergänzung um den neuen Satz 2 werden die Dokumentationspflichten des Verantwortlichen um einen zur Herstellung von Transparenz äußerst relevanten Faktor erweitert. Eine effektive Rechtedurchsetzung der betroffenen Person gegenüber den Empfängern wird auf Grundlage eine Protokollierung von Übertragungen personenbezogener Daten überhaupt erst ermöglicht.

2.3.22 Datenschutz durch Systemgestaltung

In den Text des Art. 25 Abs. 1 DSGVO sollten die Hersteller als Adressaten mit aufgenommen werden.[282] Um bei der datenschutzgerechten Systemgestaltung die besonderen Risiken für Kinder gebührend zu berücksichtigen,[283] sollte Art. 25 Abs. 1 DSGVO um die Beachtung dieses Umstands ergänzt werden:

> „(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen, *insbesondere für Kinder,* trifft der Verantwortliche *und der Hersteller von Datenverarbeitungssystemen* sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung —, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen."

[282] S. Kap. 2.1.13.2 und 2.2.4.
[283] S. Kap. 2.1.6.

Die Ergänzung führt dazu, dass den Rechten und Freiheiten von Kindern im Kontext der Systemgestaltung besondere Beachtung garantiert wird. Dabei hat die Ergänzung im Wesentlichen eine klarstellende Funktion, die jedoch vor dem Hintergrund einer unzureichenden Berücksichtigung von Kindern bei der Systemgestaltung in der Vergangenheit notwendig wird.

Weitere risiko- und anwendungsspezifische Konkretisierungen der Vorschrift sind notwendig und werden im Zusammenhang einer risikoorientierten Überarbeitung der Verordnung diskutiert.[284]

2.3.23 Datenschutz durch Voreinstellungen

Um die Effektivität der Pflicht zu datenschutzfreundlichen Voreinstellungen nach Art. 25 Abs. 2 DSGVO zu erhöhen und die datenschutzunfreundlichen Gestaltungsmöglichkeiten von Verantwortlichen einzuschränken, soll, statt die Voreinstellung auf einen frei bestimmbaren Zweck hin auszurichten, gefordert werden, dass die Voreinstellung sich daran ausrichtet, welche Ausprägung der technischen Funktion notwendig ist, um die Hauptleistung für die betroffene Person zu erbringen.[285] Hierfür ist ein neuer Satz 2 in den Normtext einzufügen. Die bisherigen Sätze 2 und 3 werden Sätze 3 und 4. Um bei der datenschutzfreundlichen Voreinstellung die besonderen Risiken für Kinder gebührend zu berücksichtigen,[286] sollte Art. 25 Abs. 2 DSGVO außerdem in einem neuen Satz 5 um die Beachtung dieses Umstands ergänzt werden:

> „(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. *Zu berücksichtigen ist die Ausprägung des Verarbeitungszwecks, nach der so wenig personenbezogene Daten wie möglich verarbeitet werden.* Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. *Die Voreinstellungen berücksichtigen insbesondere die Schutzbedürftigkeit von Kindern.*“

Der neue Satz 2 hat zur Folge, dass neben dem Grundsatz der Datenminimierung (Satz 1) auch der Grundsatz der Datenvermeidung zu einem wesentlichen Faktor bei der Gestaltung und Auswahl von Voreinstellungen erhoben wird. Anknüpfungspunkt wird die funktionale Notwendigkeit einer bestimmten Voreinstellung beispielsweise zur Erfüllung einer vertraglich vereinbarten Leistung. Relevant wird damit neben der subjektiven Erforderlichkeit für den letztlich vom Verantwortlichen diktierten Zweck auch die objektive Erforderlichkeit.

Die Ergänzung um einen neuen Satz 5 bewirkt ebenso wie die Ergänzung von Art. 25 Abs. 1 DSGVO durch die explizite Erwähnung der Schutzbedürftigkeit von Kindern im Normtext eine Stärkung der Rechte und Freiheiten von Kindern und hat gleichfalls klarstellende Wirkung.

---

284 S. Kap. 3.3.1.
285 S. Kap. 2.1.14.
286 S. Kap. 2.1.6.

2.3.24 Informationspflichten bei gemeinsamer Verantwortlichkeit

Um sicherzustellen, dass bei gemeinsamer Verantwortlichkeit für die Datenverarbeitung die lückenlose Information, die die gemeinsam Verantwortlichen der betroffenen Person bieten müssen, auch tatsächlich erbracht wird, sollte im Text des Art. 26 Abs. 1 Satz 2 DSGVO ausdrücklich festgehalten werden, dass die Verantwortlichen verpflichtet sind, ihre Informationen so abzustimmen, dass eine lückenlose Information der betroffenen Person gewährleistet ist:

> „(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, *um eine lückenlose Information der betroffenen Person zu gewährleisten*, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden."

Durch die Ergänzung wird das Maß der Koordination der gemeinsam Verantwortlichen präzisiert: Sie müssen so zusammenarbeiten, dass durch ihre jeweiligen Informationen keine Informationslücken bei der betroffenen Person entstehen können. Außerdem wird sichergestellt, dass alle gemeinsam Verantwortlichen auch im Sinn des Art. 83 Abs. 5 lit. b DSGVO für die Erfüllung dieser Anforderung haften. Sie können bei unvollständiger Information oder bei Ausbleiben der Information effektiv sanktioniert werden.

2.3.25 Berücksichtigung der Risiken eines Kindes in der Datenschutz-Folgenabschätzung

Um bei jeder Datenschutz-Folgenabschätzung den Umstand gebührend zu berücksichtigen, dass personenbezogene Daten von Kindern verarbeitet werden, sollte Art. 35 Abs. 1 und 7 DSGVO um die Beachtung dieses Umstands ergänzt werden:

> „(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, *insbesondere durch die Verarbeitung personenbezogener Daten eines Kindes,* voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden."
>
> (7) Die Folgenabschätzung enthält zumindest Folgendes:
>
> a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
>
> b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1, *die in besonderer Weise berücksichtigt, wenn es sich um die personenbezogenen Daten eines Kindes handelt,* und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener*, insbesondere von Kindern,* Rechnung getragen wird."

Durch die Ergänzung werden die Vorschläge zur Ergänzung von Art. 21, 25 und 34 DSGVO konsequent fortgeführt und auch auf die Datenschutz-Folgenabschätzung erstreckt. Ziel ist auch hier eine Stärkung der Rechte und Freiheiten von Kindern, indem sichergestellt wird, dass diese durch die explizite Adressierung von Kindern im Normtext tatsächlich Beachtung des Verantwortlichen finden. Die Ergänzungen in Art. 35 DSGVO gehen indes über bloße Klarstellungen hinaus und etablieren konkrete Pflichten bei der Durchführung einer Datenschutz-Folgenabschätzung zur besonderen Berücksichtigung von Kindern, die sich sowohl auf die Risikoanalyse als auch auf die Festlegung von Schutzmaßnahmen erstrecken.

2.3.26 Neue Aufgaben für den Europäische Datenschutzausschuss

Die bisher vorgeschlagenen Änderungen der Datenschutz-Grundverordnung begründen drei zusätzliche Aufgaben des Europäischen Datenschutzausschusses.[287] Diese sollten in die Liste der Aufgaben des Ausschusses in Art. 70 Abs. 1 DSGVO mit aufgenommen werden. Hierbei können die Aufgaben zur Präzisierung der Pflicht zu einer datenschutzgerechten Systemgestaltung nach Art. 25 Abs. 1 DSGVO und der Pflicht zur datenschutzfreundlichen Voreinstellung nach Art. 25 Abs. 2 DSGVO zu einer Aufgabe zusammengezogen werden. Im Text der Norm bieten sich Ergänzungen um einen Buchstaben ea und fa an:

„*(ea) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zur näheren Bestimmung der interoperablen Formate für eine Übertragung von Daten gemäß Artikel 20 Absatz 1und 2;"*

„(fa) Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren gemäß Buchstabe e des vorliegenden Absatzes zur näheren technik- und bereichsspezifischen Bestimmung der Pflicht zu Datenschutz durch Systemgestaltung gemäß Artikel 25 Absatz 1 und durch Voreinstellungen gemäß Artikel 25 Absatz 2;"

Diese Ergänzungen stellen Kohärenz innerhalb der Verordnung sicher und gewährleisten, dass der Ausschuss auch bezogen auf die vorgeschlagenen Änderungen zusätzliche Präzisierungen vornimmt und Empfehlungen zur konkreten Ausgestaltung abgibt.

[287] S. Kap. 2.2.5.

2.3.27 Statistiken zu Sanktionsverfahren

Um den Vollzug der Datenschutz-Grundverordnung zu unterstützen, um Transparenz über das Behördenhandeln herzustellen und um für eine angeglichene Praxis der Verhängung von Geldbußen beizutragen, sollten die Aufsichtsbehörden eine halbjährliche Statistik zu diesen Verfahren veröffentlichen. Hierzu sollte Art. 83 DSGVO um einen zusätzlichen Absatz 10 ergänzt werden:

> *„(10) Jede Aufsichtsbehörde veröffentlicht einen Monat nach Ablauf jedes Halbjahres eine Statistik über die nach dieser Vorschrift durchgeführten Verfahren."*

Dieser zusätzliche Absatz bewirkt eine erhebliche Transparenzsteigerung. Einerseits kann sich der Verbraucher von der effektiven Durchsetzung des Datenschutzrechts überzeugen, andererseits kann ein Verantwortlicher besser antizipieren, wie der äußerst breite Bußgeldrahmen der Datenschutz-Grundverordnung in der Praxis angewendet wird.

3. Fortentwicklung des Datenschutzrechts

Für viele Regelungen der Datenschutz-Grundverordnung musste festgestellt werden, dass sie den gegenwärtigen Herausforderungen des Datenschutzes nicht gerecht werden, dass diese Defizite aber nicht durch kleine Wortlautänderungen behoben werden können. Vielmehr erfordern diese Defizite grundsätzliche Diskussionen der hinter ihnen stehenden Regelungskonzepte. Daher werden in diesem Kapitel wichtige Aspekte dieser Regelungsaspekte aus Sicht des Verbraucherschutzes diskutiert. Im ersten Schritt werden wichtige Herausforderungen des Datenschutzes heute und morgen angesprochen, denen das Datenschutzrecht gerecht werden muss. Im zweiten Schritt werden konzeptionelle Mängel der Datenschutz-Grundverordnung angesprochen, die verhindern, dass sie den Herausforderungen gerecht werden kann, und diskutiert, welche konzeptionellen Ansätze stattdessen verfolgt werden sollten. Im darauffolgenden Kapitel wird dann erörtert, auf welchen Wegen die notwendige Modernisierung des Datenschutzrechts in der Europäischen Union und in der Bundesrepublik Deutschland erreicht werden könnte.[288]

3.1 Datenschutz in der Welt von heute

Die gegenwärtige Datenschutz-Governance zeichnet sich zunächst durch eine Ko-Regulierung durch die Europäische Union und die Mitgliedstaaten aus, die aus den zahlreichen Öffnungsklauseln und Regelungsaufträgen der Datenschutz-Grundverordnung folgt. Darüber hinaus finden sich in der Datenschutz-Grundverordnung weite Erlaubnistatbestände mit hoher Selbstbestimmung der Verantwortlichen. Zahlreiche Defizite gibt es bei der Information der Verbraucher sowie bei der Einwilligung und den anderen Erlaubnistatbeständen.[289] Auch die Reichweite der Betroffenenrechte ist vielfach unklar, zumal diese stark einschränkbar sind. Die technikneutralen Regelungen der Datenschutz-Grundverordnung schlagen in eine Risikoneutralität um, die den Risiken und der Komplexität moderner Datenverarbeitung in allen Wirtschafts-gesellschafts- und Verwaltungsbereichen nicht gerecht wird.[290] Die Aufsichtsbehörden wurden indes zwar mit neuen Aufgaben versehen, gleichzeitig sind sie in ihrer Aufgabenwahrnehmung aber durch unzureichende finanzielle wie personelle Ausstattungen behindert. Die aufwandsreichen Abstimmungsverfahren unter den Aufsichtsbehörden, die die Verordnung vorsieht, dürften zwar mittel- und langfristig zu einer größeren Harmonisierung führen, sind aber zunächst eine zusätzliche Belastung für die Aufsichtsbehörden. Der Erfolg zahlreicher Innovationen der Datenschutz-Grundverordnung ist an hohe Anforderungen an ihre Umsetzung gekoppelt, die weder in der Datenschutz-Grundverordnung geregelt noch in der politischen Umsetzung gesichert sind.[291]

Gerade besonders populäre Dienstleistungen des digitalen Zeitalters werden heute ohne monetäre Gegenleistung angeboten und stattdessen durch die Preisgabe personenbezogener Daten durch die Nutzer entlohnt.[292] Diese Daten stellen das eigentliche Produkt dar; die Finanzierung der Dienstleistung erfolgt durch Leistungen Dritter, die beispielsweise personalisierte Werbung schalten lassen. Die Verarbeitung dieser Daten verspricht mitunter enorme Gewinne und löst

---

288 S. Kap. 4.
289 S. Kap. 2.1.4 bis 2.1.9.
290 S. näher Kap. 3.2.1.
291 S. die Beiträge in DuD 8/2019.
292 Kugelmann, DuD 2016, 566.

so Begehrlichkeiten aus. Diese Verarbeitung kann Grundlage sein, um umfassende Profile zu erstellen, und ermöglicht so eine personalisierte Ansprache des Verbrauchers. Diese ist zwar insofern zu dessen Vorteil, als sie auf dessen (vermeintliche) Bedürfnisse zugeschnitten ist, wirkt aber verhaltensbestimmend und schränkt durch ihre algorithmenbasierte Vorauswahl die autonome Willensbildung des Verbrauchers ein. Sie kann sich sogar unmittelbar ins Negative kehren, wenn der Verantwortliche etwa bestimmte Eigenschaften des Verbrauchers zu dessen Manipulation ausnutzt.

Die Datenschutz-Grundverordnung war mit dem Ziel angetreten, eine umfassende Modernisierung und Harmonisierung des europäischen Datenschutzes zu bewirken, gleichzeitig aber auch positive ökonomische Effekte im europäischen Binnenmarkt mit einem verbesserten Grundrechtsschutz natürlicher Personen zu verbinden.[293] Der Modernisierungsbedarf des Datenschutzrechts ergab sich aus zahlreichen technischen Entwicklungen, die letztlich zur Entstehung neuer Datenquellen sowie neuer Möglichkeiten der Vernetzung dieser Datenquellen und damit zu einer sowohl quantitativen wie auch qualitativen Zunahme der Verarbeitung personenbezogener Daten führte. Die so gewonnenen Daten können bei immer weiter steigender Rechenleistung und ständig verbesserten Analyseverfahren trotz immenser Datenmassen auch immer besser und schneller zusammengeführt und ausgewertet werden.[294] Diese Entwicklung ist dabei keineswegs abgeschlossen, sondern stellt das Datenschutzrecht vor nach wie vor ungelöste Herausforderungen. Als Schlagworte seien hier Smart Car,[295] Smart Health,[296] Smart Home,[297] Smarte Assistenten[298] und Robotik[299] sowie als Oberbegriffe Ubiquitous Computing, Internet of Things, Artificial Intelligence und Big Data genannt. Die Techniken bereiten den Weg für einen immer stärker informatisierten Alltag,[300] in dem Erkenntnisse über die betroffene Person nicht nur aus den von dieser direkt eingegebenen Informationen (etwa in einem Social Network) abgeleitet werden, sondern gerade auch aus einer immer weiter verbreiteten Beobachtung des Verhaltens der Person – auch in privaten Räumen. Diese Erkenntnisse können dann in Form von Profilen und algorithmenbasierten Einordnungsverfahren für die Bewertung von Verbrauchern sowie etwa in Form von Microtargeting für die Verhaltensbeeinflussung zum Zweck der Werbung für Dienstleistungen und Produkten, der Wahlinformation und vieler anderer Zwecke genutzt werden.

Sind bereits mit Blick auf aktuelle Datenverarbeitungen zahlreiche datenschutzrechtliche Probleme ungelöst, so kündigen sich durch die dargestellte technische Entwicklung der Verarbeitung personenbezogener Daten und die diese ausnutzenden Geschäftsmodelle bereits neue Problemfelder an. Besondere Herausforderungen für das Recht stellen „intelligente“ Systeme dar, die auf Basis einer umfänglichen Sensorik algorithmenbasierter Verfahren perspektivisch eine umfassende Unterstützung des Verbrauchers in allen Lebenslagen in Aussicht stellen. Das System kann dann als Erweiterung des menschlichen Gedächtnisses fungieren und einfache

293 So die Erwägungsgründe 1, 2, 4, 5, 6, 7, 10 und 13 DSGVO.
294 S. zu den Herausforderungen von Big Data für das Recht z.B. Hoffmann-Riem, 2018.
295 S. hierzu umfassend Roßnagel/Hornung, 2019.
296 S. z.B. Jandt, DuD 2016, 571; Dochow, 2017.
297 S. z.B. Skistims, 2016; Geminn, DuD 2016, 575.
298 S. z.B. Thies/Knote u.a., in: Roßnagel/Friedewald/Hansen, 2018, 175; Steidle 2005.
299 S. z.B. Keßler, MMR 2017, 589.
300 S. Roßnagel, 2007.

Aufgaben des Alltags ganz übernehmen, gleichzeitig aber auch bei komplexen Tätigkeiten Hilfestellung geben. Gegenüber den immensen Vorteilen solcher Systeme treten die Nachteile durch die zugrundeliegende Verarbeitung personenbezogener Daten in der Wahrnehmung des Verbrauchers in den Hintergrund.

3.2 Datenschutzherausforderungen in der Welt von morgen

Die Entwicklung von Techniken, die für die Verarbeitung und Nutzung von Verbraucherdaten genutzt werden können, und die Entwicklung von Geschäftsideen, diese Techniken für die Erfassung und Beeinflussung von Verbraucherverhalten einzusetzen, werden viele weitere und derzeit noch unbekannte Herausforderungen für den Verbraucherdatenschutz hervorrufen. Diese sind sehr schwer vorherzusehen. Wichtig ist daher, dass das Datenschutzrecht so konzipiert ist, praktiziert wird und angepasst werden kann, dass es mit all diesen Herausforderungen konstruktiv umgehen kann. Dies wird im Folgenden bei der Konzipierung von Entwicklungsideen zum Datenschutzrecht berücksichtigt.

Eine Entwicklung ist aber im Kontext von Big Data und Künstlicher Intelligenz bereits heute schon gut absehbar: Die immer stärkere Auswertung der explodierenden Mengen an personenbezogenen Daten der Verbraucher in Form ihrer Quantifizierung und Verwendung in Maßnahmen der Verhaltensbeeinflussung und menschlichen oder automatisierten algorithmenbasierten Entscheidungsverfahren.

Der Verbraucher der Zukunft wird jederzeit von digitalen Infrastrukturen umgeben sein und durch alle seine Handlungen in diesen Strukturen Datenspuren hinterlassen, die zur Ausbeutung durch Anbieter und Dritte zur Verfügung stehen. Diese legen auf der Basis algorithmenbasierter Datenverarbeitungssysteme von ihren Nutzern Profile an, schließen aus den erfassten Merkmalen auf Eigenschaften dieser Personen und übertragen diese statistisch erwiesenen Eigenschaften auf alle, die diese Merkmale aufweisen. Daher sind alle in der Statistik gefangen – auch wenn sie sich ihr entziehen wollen.[301] Sie sind unentrinnbar Teil einer anonymen Vergemeinschaftung[302] durch algorithmenbasierte Systeme. Beispielsweise verhindert dann in einer digitalisierten Verkehrsinfrastruktur auch die Nutzung eines unvernetzten Fahrzeugs nicht die Erfassung durch diese smarte Infrastruktur und die Erfassung aller anderen, vernetzten Verkehrsteilnehmer. Auch durch bewusste Technikaskese kann der einzelne es nicht vermeiden, etwa von automatisierter Entscheidungsfindung betroffen zu sein. Dies schließt ein, Ziel von Prognosen, Verhaltensbeeinflussungen und algorithmenbasierten Entscheidungen zu sein, die auf diesen Statistiken beruhen.[303] Das Konzept von Einwilligung und individueller Selbstbestimmung wird dadurch infrage gestellt. Der Einzelne verliert die Kontrolle darüber, „wer was wann und bei welcher Gelegenheit“ über ihn weiß.[304] Die Statistik wirkt auch gegenüber dem, der nicht an ihrem Zustandekommen durch Datenpreisgabe mitgewirkt hat.

Statistiken, wie sie zur Mustererkennung bei Big Data-Analysen oder beim Lernen von algorithmenbasierten Systemen eingesetzt werden, wirken normbildend und verhaltensbestimmend.

---

301 S. hierzu Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 365 ff.
302 S. zu dieser z.B. Hubig, in: Roßnagel/Sommerlatte/Winand 2008, 165 ff.
303 S. Roßnagel, ZD 2013, 562 (566); Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 365 ff.
304 BVerfGE 65, 1 (43).

Sie korrelieren Verhaltensmerkmale und beschreiben „normales“ und „abweichendes“ Verhalten. Wenn an diese Muster oder Modelle positive und negative menschliche oder automatisierte Entscheidungen anknüpfen, werden sich die Menschen diesen Mustern und Modellen anpassen, um in den Genuss der positiven Wirkungen zu gelangen und negative zu vermeiden. Durch sie unterliegt jeder der „Normativität der Normalität“.[305] Wer nicht auffallen oder bestimmte algorithmenbasiert getroffene Entscheidungen beeinflussen will, akzeptiert die erwartete Normalität als Verhaltensnorm. Verhaltensmuster und -modelle können durch diese Normbildung indirekt, aber wirkungsvoll die Wahrnehmung von Grundrechten beeinflussen. Die anonymen Muster wirken so genauso negativ auf die Persönlichkeitsentfaltung des Einzelnen und die freie Kommunikation und Willensbildung in der Gesellschaft insgesamt ein, wie dies das Bundesverfassungsgericht bereits im Volkszählungsurteil als Auswirkungen personenbezogener Überwachung festgestellt hat.[306]

3.3 Vorschläge zur Fortentwicklung des Datenschutzes

Im Folgenden werden Ansätze zur Weiterentwicklung des Datenschutzes angesprochen, die sich nicht auf einzelne Regelungen der Datenschutz-Grundverordnung, sondern auf Regelungskonzepte beziehen, die ihr zu Grunde liegen oder die sie verfolgen sollte, um den absehbaren Herausforderungen in der Zukunft gerecht werden zu können. Hierzu werden aus Verbrauchersicht die Möglichkeiten einer risikoadäquaten Weiterentwicklung des geltenden Datenschutzrechts sowohl auf Ebene der Europäischen Union als auch auf Ebene der Mitgliedstaaten beleuchtet und konzeptionelle Beiträge unterbreitet, um die notwendige Diskussion zu einer risikoorientierten Modernisierung des Datenschutzrechts anzuregen (3.3.1). Weiterhin wird geprüft, wie konzeptionell die Stellung der Verbraucher gestärkt (3.3.2) und ihre Überforderung verhindert werden kann (3.3.3). Da durch moderne Datenverarbeitungssysteme auch dritte Verbraucher, die nicht selbst betroffene Personen sind, beeinträchtigt sein können, erstreckt sich die Prüfung auch auf die Frage, wie sich diese Beeinträchtigungen bewerten und steuern lassen (3.3.4). Schließlich folgen konzeptionelle Überlegungen, wie das Recht die Datenschutzprinzipien stärken kann (3.3.5).

3.3.1 Risikoadäquate Weiterentwicklung oder Ergänzung des Datenschutzrechts

Ein wesentlicher Schwachpunkt der Datenschutz-Grundverordnung ist ihre weitgehende Risikoneutralität. Sie beachtet zwar Risiken der Datenverarbeitung, um die Belastungen der Verantwortlichen zu reduzieren.[307] Ihr fehlen jedoch risikoadäquate Differenzierungen der Datenschutzgrundsätze, der Zulässigkeit der Datenverarbeitung und der Betroffenenrechte. Auch wo die Datenverarbeitung sehr unterschiedliche Grundrechtsrisiken verursacht, finden die gleichen abstrakten Regelungen Anwendung – etwa für die wenig riskante Kundenliste eines Handwerkers ebenso wie für die um Potenzen risikoreicheren Datenverarbeitungsformen des Internet der Dinge, von Big Data, Cloud Computing und datengetriebenen Geschäftsmodellen. Die Datenschutzpraxis berichtet: „Gerade kleinere Wirtschaftsakteure und insbesondere Vereine übten

305 Weichert, ZD 2013, 251 (258); Roßnagel, ZD 2013, 562 (566).

306 BVerfGE 65, 1 (43).

307 Vor allem in ihrem Kapitel IV stellt die DSGVO die Pflichten der Verantwortlichen unter Risikovorbehalt – s. z.B. Art. 24, 25, 30, 32, 33, 34, 35, 36 und 37 DSGVO – mit der Folge, dass in der Praxis diese Pflichten nur für einen Bruchteil der Verantwortlichen tatsächlich wirksam werden – s. hierzu auch Albrecht, CR 2016, 88 (94); Roßnagel, DuD 2016, 561 (565); Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 375 f.

dahingehend Kritik, dass sie von den Anforderungen der DSGVO in gleicher Weise berührt sind wie datenhungrige Großkonzerne und Soziale Netzwerke."[308] Gerade diese ungerechtfertigte Risikoneutralität ist es, die erhebliche Akzeptanzprobleme der Datenschutz-Grundverordnung auf Seiten der Bevölkerung in Europa – und damit Skepsis gegenüber Politik und Rechtsetzung der Europäischen Union insgesamt – hervorzurufen droht.

Der Grund für diese Risikoneutralität ist, dass die Datenschutz-Grundverordnung einer übertriebenen Ausprägung des Grundsatzes der Technikneutralität folgt. Dies soll das Risiko einer Umgehung rechtlicher Vorschriften minimieren, indem die Datenschutzregelungen „nicht von den verwendeten Techniken abhängen".[309] Richtig verstanden ist eine technikneutrale Regelung dann sinnvoll, wenn sie verhindern soll, dass rechtliche Vorschriften technische Weiterentwicklungen ausschließen. Sie ist daher so zu fassen, dass die rechtlichen Vorgaben auch auf weiterentwickelte Techniken anwendbar sind.[310] Dies schließt aus, Regelungen für einzelne *Ausprägungen* einer spezifischen Technikanwendung zu treffen. Dies darf aber nicht verhindern, Vorgaben für bestimmte technische *Funktionen* vorzusehen – insbesondere, wenn sie besondere Risiken für Grundrechte verursachen. Denn in einer technikgeprägten Welt kann Grundrechtsschutz nicht erfolgen, wenn nicht auch Risiken durch Technik aufgegriffen und durch die Regulierung technischer Funktionen gesteuert werden. Funktionen – wie z.B. Protokollierung, Profilbildung, Löschung oder Anonymisierung – können datenschutzgerecht reguliert werden, ohne dass im Regelfall die rechtliche Anforderung durch die Weiterentwicklung einer Technik überholt oder nicht anwendbar wird.[311]

Zwar benennt die Datenschutz-Grundverordnung in den Erwägungsgründen 6 und 101 abstrakt die in Kapitel 3.1 geschilderten Herausforderungen, die technischer Fortschritt und Globalisierung für das Datenschutzrecht bedeuten. Sie greift jedoch keine einzige Technikfunktion auf, deren Datenschutzrisiken – wie etwa bei Big Data, Cloud Computing, Internet der Dinge und künstlicher Intelligenz – bereits heute intensiv diskutiert werden und die auch noch bei veränderten technischen Merkmalen in vielen Jahren ein Problem für den Datenschutz darstellen.[312] Damit überspannt sie das Konzept der Technikneutralität und wird als Resultat risikoneutral.

Ziel der Europäischen Kommission war es, einen besonders zukunftsoffenen Datenschutzrahmen zu schaffen.[313] Damit bleibt es aber bei den Bedingungen für die Zulässigkeit der Verarbeitung personenbezogener Daten, der Voraussetzungen und Folgen der Betroffenenrechte und der Konkretisierung der Datenschutzprinzipien bei höchst abstrakten Vorgaben. Die Praxis zeigt, dass „der dem Vollharmonisierungsanspruch und der technikneutralen Ausgestaltung geschuldete hohe Abstraktionsgrad einzelner Regelungen der Verordnung… eine Bandbreite an Deutungsmöglichkeiten bietet und dem Anwender die Umsetzung der Vorgaben erschwert".[314]

---

308 S. Unabhängiges Datenschutzzentrum Saarland 2019, 15.

309 S. Erwägungsgrund 15 Satz 1 DSGVO.

310 S. grundsätzlich Roßnagel, in: Eifert/Hoffmann-Riem, 2009, 323 ff.

311 S. hierzu weiter unten in diesem Unterkapitel.

312 Dies ist und für Social Networks in Art. 20 DSGVO und für algorithmenbasierte Entscheidungsverfahren 22 DSGVO allenfalls in abstrakten Ansätzen der Fall. S. zur Kritik an diesen beiden Vorschriften Kap. 2.1.10 und 2.1.11.

313 „Es sollte … nicht versucht werden, jede Frage, die den Datenschutz in Europa in den nächsten 20 Jahren beschäftigen könnte, bereits heute im Detail regeln zu wollen", Reding, ZD 2012, 195 (198).

314 Unabhängiges Datenschutzzentrum Saarland 2019, 16.

Datenverarbeitungen zu verhindern, die unzumutbare Risiken verursachen, ist nicht das Ziel der Verordnung. Sie knüpft an keiner Stelle die Zulässigkeit besonders riskanter Funktionen der Datenverarbeitung an das Fehlen bestimmter Grundrechtsrisiken oder macht sie von der Bewältigung dieser Risiken abhängig. Doch nur durch die Berücksichtigung typischer Risiken bestimmter Datenverarbeitungsformen im Verordnungstext kann die notwendige Rechtssicherheit und Interessengerechtigkeit erreicht werden.

Die Konkretisierung der hochabstrakten Vorgaben für die unendliche Vielfalt von einzelnen Diensten und Anwendungen in allen Gesellschafts-, Wirtschafts- und Verwaltungsbereichen sollte den Gerichten, den mitgliedstaatlichen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss überlassen bleiben.[315] In der Praxis bleiben im ersten Zugriff diese Konkretisierungen jedoch den Verantwortlichen überlassen. Sie nutzen die Abstraktheit der Vorgaben, um sie nach ihren Interessen zu praktizieren. So berichten Aufsichtsbehörden: „Ab dem ersten Geltungstag der Datenschutz-Grundverordnung taten einige große außereuropäische Anbieter so, als wäre nun der Datenschutz viel laxer zu handhaben. Gerichtliche Untersagungen gegen eine invasive Datenverarbeitung wurden nicht mehr als bindend angesehen, da das neue Datenschutzrecht die entsprechende Verarbeitung angeblich erlauben würde.“[316] Die betroffenen Personen, die damit nicht einverstanden sind, müssen sich bei den Aufsichtsbehörden beschweren. Diese können im Einzelfall prüfen und notfalls – nach Abstimmung mit anderen Aufsichtsbehörden – eingreifen. Sie sind aber durch die vielen anderen Aufgaben, die ihnen Art. 57 und 70 DSGVO stellen, angesichts ihrer zu geringen Ressourcen überfordert.[317]

Endgültig verbindliche Aussagen zur Auslegung der Datenschutz-Grundverordnung kann jedoch nur der Europäische Gerichtshof treffen. Dieser ist wiederum auf die Vorlage bestimmter Fragen und Themen durch die mitgliedstaatlichen Gerichte angewiesen. Problematisch ist auch die Dauer von Verfahren, bis sie zum Europäischen Gerichtshof gelangen und bis sie von diesem entschieden sind. Wegen der dynamischen Entwicklung der Informationstechnik und ihrer Anwendungen sind die dem Streitgegenstand zugrundeliegenden Datenschutzprobleme oft nicht mehr aktuell, bis durch die Entscheidung des Europäischen Gerichtshofs eine gesicherte Rechtsprechung zu entstehen beginnt. Eine praktikable Lösung, um das Ziel zu erreichen, die vielen Vorgaben der Datenschutz-Grundverordnung zu konkretisieren und die zahlreichen offenen Fragen zu beantworten, die sie verursacht, ist dies nicht.[318] Bis zur abschließenden Klärung einzelner Fragen durch den Europäischen Gerichtshof lädt die Datenschutz-Grundverordnung zu interessengeleiteten Interpretationen und Meinungsstreitigkeiten geradezu ein. Die Machtasymmetrie zwischen großen datenverarbeitenden Unternehmen und Verbrauchern führt vor diesem Hintergrund zu einer Schlechterstellung der Verbraucher.[319]

Technikneutralität ist zur Regelung komplexer Sachverhalte ein unverzichtbares Instrument, sofern die Regelung einzelner technischer Ausprägungen vermieden wird.[320] Zum Problem

315 Reding, ZD 2012, 195 (198).
316 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein 2019, 9.
317 S. Kap. 2.1.14.
318 Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 376.
319 Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 376 f.
320 S. Roßnagel, in: Eifert/Hoffmann-Riem, 2009, 323 ff.

wird sie dort, wo auch einzelne technische Funktionen nicht risikospezifisch adressiert werden.[321] Letzterem verweigert sich die Datenschutz-Grundverordnung aber – zu Unrecht. Diese Form der Regulierung wird den eigenen Zielsetzungen der Verordnung nicht gerecht, die betroffenen Personen vor den Bedrohungen, die sich durch den Einsatz moderner Technik für ihre Grundrechte und Freiheiten manifestieren, zu schützen. Dies zeigt sich exemplarisch bei den neuen Anforderungen wie der Pflicht zum Datenschutz durch Systemgestaltung und durch Voreinstellungen. Diese Vorgaben sind in ihrer Abstraktheit nicht in der Lage, die Entwicklung und den Einsatz der Techniksysteme und Geschäftsmodelle datenschutzgerecht zu steuern.

Dabei sind technik- und bereichsspezifische Regelungen zum Datenschutz in der Union möglich, die gerade nicht der in der Datenschutz-Grundverordnung verfolgten spezifischen Ausprägung von Technikneutralität folgen. Ein bereits existierendes Beispiel hierfür ist Art. 6 eCall-Verordnung (EU) 2015/758[322] zur Regelung der Datenschutzanforderungen beim automatisierten Notruf in Kraftfahrzeugen. Auch die geplante ePrivacy-Verordnung fällt in die Kategorie bereichsspezifischer risikoadäquater Regulierung.[323]

Risikospezifische Regelungen, bei denen sich der Gesetzgeber mit den besonderen Risiken bestimmter Technikanwendungen und Geschäftsmodelle auseinandersetzt, sind im Datenschutzrecht zum Schutz der Grundrechte und Freiheiten der betroffenen Personen unabdingbar. Beispiele für solche risikoadäquaten, aber dennoch technikneutralen Regelungen, die überwiegend den Ansatz eines Datenschutzes durch Systemgestaltung verfolgen und als Konkretisierung von Art. 25 DSGVO angesehen werden können, könnten sein:[324]

- Riskante Datenverarbeitung darf nur zulässig sein, wenn geeignete Schutzvorkehrungen getroffen sind. Deren Eignung ist permanent nachzuweisen.
- Profile sind nur zulässig, wenn sie für den objektiven Zweck einer zulässigen datenvermeidenden Anwendung erforderlich sind.
- Vorsorgemaßnahmen müssen Risiken reduzieren und potenzielle Schäden begrenzen – auch bei anonymen Daten, die noch einen Personenbezug erhalten können.
- Neben den Datenverarbeitern sind auch die Hersteller von Informationstechnik dafür in die Pflicht zu nehmen, dass sie diese datenschutzgerecht gestalten und voreinstellen.
- Anforderungen an die transparente, datenvermeidende und missbrauchsresistente Gestaltung des Systems (Vermeidung von Profilen) und deren datenärmste Konfigurierung müssen bereichsspezifisch konkretisiert werden.
- Anforderungen an die Architektur der Datenverarbeitung müssen so gestaltet werden, dass die personenbezogenen Daten prinzipiell im Bereich der betroffenen Person selbst

321 S. hierzu umfassend Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 374 ff.
322 EU ABl. L 123 vom 19.5.2015, 77.
323 S. im Kommissionsentwurf die Art. 8, 10, 12 und 16; KOM(2017) 10 endg.
324 Beispiele überwiegend entnommen aus Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 361 (377 f.). Zu weiteren Beispielen für den Datenschutz in der öffentlichen Verwaltung und im Beschäftigtenkontext s. Roßnagel, DuD 2017, 290 (293 f.).

verbleiben und nur anonymisierte oder pseudonymisierte Daten in den zentralen Systemen verarbeitet werden.

- Die Datensicherheit ist an den Schutzzielen Datenvermeidung, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit auszurichten.[325]

- Um Maßnahmen, die technischen Selbstdatenschutz durch die betroffenen Personen ermöglichen, zur Durchsetzung zu verhelfen, sind Hersteller und Verantwortliche zu verpflichten, geeignete Schnittstellen zu Verfügung zu stellen.

- An Pseudonymisierung oder Anonymisierung sind konkrete Anforderungen an den Grad der Sicherheit gegen De-Anonymisierung zu stellen und die Wiederherstellung eines Personenbezugs ist ausdrücklich zu verbieten.[326]

- Für bestimmte riskante Datenverarbeitungsvorgänge sind Anforderungen an die Zweckbestimmung und die Absicherung von Zweckbindungen festzulegen und insbesondere Zweckänderungen für Daten zu verbieten, an deren Zweckbindung ein hohes Vertrauen besteht, wie z.B. Protokolldaten zu Sicherungszwecken.

- An die Zulässigkeit der Auftragsdatenverarbeitung und speziell des Cloud Computing sind risikospezifische Anforderungen festzulegen.

- Algorithmenbasierte Entscheidungsverfahren dürfen nur für ihren Einsatzbereich nachgewiesen relevante Merkmale verwenden und müssen für Aufsichtsbehörden in ihrer Entscheidungsfindung nachvollziehbar und für die betroffene Person erklärbar sein.

Die Regelungen zu den Voraussetzungen der Zulässigkeit der Datenverarbeitung, zur Zulässigkeit von Zweckänderungen, zu konkreten Rechten der betroffenen Personen und zu den Pflichten der Verantwortlichen müssen spezifisch für bestimmte Technikfunktionen oder bereichsspezifisch für bestimmte Anwendungsprobleme konkretisiert werden. Grundsätzlich sind zwei unterschiedliche Ansatzpunkte für im richtigen Sinn technikneutrale, aber risikospezifische Datenschutzregelungen möglich:

- Entweder regelt das Datenschutzrecht Funktionen von Techniken, die in vielen Wirtschafts-, Gesellschafts- und Verwaltungsbereichen zum Einsatz kommen – wie etwa Videoüberwachung, Cloud Computing oder algorithmenbasierte Entscheidungsverfahren – und fordert für diese bereichsübergreifend die Ausgestaltung einzelner wichtiger Funktionen – wie z.B. die Nachvollziehbarkeit und Begründbarkeit von algorithmenbasierten Entscheidungen.

- Oder es regelt Ausprägungen von Datenschutzvorgaben in spezifischen Anwendungsbereichen – wie z.B. für Smart Cars, Smart Buildings oder Social Networks. In diesen Regelungen fordert es bereichsspezifische Ausgestaltungen von Technikfunktionen – wie etwa im Smart Car bestimmte Anzeigen vor der Verarbeitung von bestimmten personenbezogenen

---

325 Konferenz der unabhängigen Datenschutzaufsichtsbehörden, Entschließung „Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen“ vom 6./7.4.2016.

326 S. zu dem Beispiel im japanischen Datenschutzrecht Geminn/Laubach/Fujiwara, ZD 2018, 413.

Daten, Möglichkeiten der Intervention von Fahrern oder die Zulässigkeit von Speicherungen oder Weitergaben von Daten an Dritte – und berücksichtigt dabei die spezifischen Bedingungen und Ausprägungen ihrer Anwendung.

Notwendig ist immer, die geeigneten Anforderungen an die Verantwortlichen, aber auch an die Hersteller und Anbieter von Techniksystemen zu stellen, mit deren Hilfe die Verantwortlichen die Anforderungen erfüllen sollen. Darauf zu vertrauen, dass der Markt dafür sorgt, dass rechtzeitig genau die vom Datenschutzrecht geforderten Datenschutzfunktionen von den Herstellern und Anbietern angeboten werden, wäre naiv. In der Praxis der Aufsichtsbehörden ist festzustellen: „Diejenigen, die es richtig machen wollten, waren auch nicht glücklich, weil sie feststellten, dass Hersteller von Produkten und Anbieter von Dienstleistungen ihnen oft keine Hilfe waren und es damit schwierig war, die eigene Rechenschaftspflicht zu erfüllen.“[327] Die Hersteller nicht zu verpflichten, ihre Produkte und Dienstleistungen mit bestimmten Technikfunktionen auszustatten, stürzt Verantwortliche in ein Erfüllungsdilemma und begründet von Anfang an Vollzugsdefizite.

Auch hier wäre eine abstrakte Verpflichtung über alle Gesellschafts-, Wirtschafts- und Verwaltungsbereiche hinweg verfehlt, vielmehr sollte sie technik- und bereichsspezifisch die jeweils spezifischen Risiken der Produkte und Dienste sowie die Bedingungen ihrer Entwicklung und ihres Angebots berücksichtigen.

Dabei ist es nicht notwendig, die Datenschutz-Grundverordnung durch einen umfassenden Katalog risikospezifischer Regelungen zu überfrachten. Vielmehr könnte die Datenschutz-Grundverordnung als die Regelung gelten, die Datenschutz dem Grundsatz nach regelt und konkretisierende Regelungen anderen Vorschriftenwerken überlässt.[328]

Die Risikoneutralität der Datenschutz-Grundverordnung wird auch deutlich, wenn sie in Art. 2 Abs. 2 lit. c die Datenverarbeitung für persönliche oder familiäre Tätigkeiten unabhängig von ihrem Risiko für betroffene Personen vollständig aus dem Anwendungsbereich des Datenschutzrechts ausnimmt.[329] Da diese Ausnahme keinen Ausgleich zwischen den Grundrechten der Datenverarbeiter und der betroffenen Personen kennt, sondern ohne jede Rücksicht auf die Risiken oder Schäden bei den betroffenen Personen gilt, bedarf sie einer Korrektur. Diese könnte darin bestehen, dass die Datenschutz-Grundverordnung zwischen der Datenverarbeitung für persönliche oder familiäre Tätigkeiten, für die keine Vorschrift der Verordnung gilt und der Datenverarbeitung für nicht persönliche und familiäre Tätigkeiten, für die alle Vorschriften der Verordnung gelten, eine dritte Gruppe bildet. Diese könnte die Datenverarbeitungen für persönliche und familiäre Tätigkeiten umfassen, die nicht zu vernachlässigende Risiken für betroffenen Personen begründet. Für diese Gruppe müssten nicht alle Vorschriften der Verordnung gelten. Für sie könnte es ausreichen, wenn für sie etwa die Vorschriften der Art. 5, 6 Abs. 4, 9, 15, 21, 32 DSGVO gelten.

Zu diskutieren wäre, wie man im Bereich der Datenverarbeitung für persönliche oder familiäre Tätigkeiten mit breiter sozialer Übung umgeht wie die Veröffentlichung von personenbezogenen Daten Dritter aus dem persönlichen und familiären Bereich in Social Media-Plattformen

327 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2019, 10.
328 S. hierzu Kap. 4.
329 S. hierzu Kap. 2.1.1.

oder auf selbstbetriebenen Webseiten (Urlaubsfotos), die nur für einen sehr eingeschränkten Kreis freigegeben werden. Da diesen unvermeidlich eine Übermittlung personenbezogener Daten an den Betreiber der Plattform zugrunde liegt, ist damit der Ausnahmebereich der „ausschließlich persönlichen und familiären Tätigkeit“ verlassen. Sollte diese Datenverarbeitung aber nicht auch in den neuen mittleren Regelungsbereich aufgenommen werden – schlicht um zu verhindern, dass es zu regelmäßigen Rechtsbrüchen bei der Verwendung von sozialen Medien kommt, für die kein Verständnis bei den Nutzern besteht?[330]

3.3.2 Stärkung der Stellung der Verbraucher

Aufgrund der Machtasymmetrie zwischen Anbieter und Verbraucher sind verschiedene Maßnahmen zur Stärkung der Stellung des Verbrauchers zu prüfen. Zum einen könnte die Nutzung der Einwilligung zur vollständigen Befreiung des Verantwortlichen von seinen datenschutzrechtlichen Verpflichtungen dadurch verhindert werden, dass bestimmte Verpflichtungen und Rechte für nicht abdingbar erklärt werden. Dies schränkt zwar die Selbstbestimmung der betroffenen Person ein, schützt sie aber davor, dass sie in sozialen oder psychischen Zwangssituationen verleitet wird, auf eigene zentrale Rechte zu verzichten. Hierfür könnte der bis zum 24. Mai 2018 geltende § 6 BDSG ein Vorbild sein.

Zum anderen könnte der Schutz des Verbrauchers nicht seiner individuellen Entscheidung überantwortet werden, sondern vor allem in „Take it or Leave it“-Situationen objektiviert werden, indem z.B. die Einwilligungserklärungen oder AGBs von einer dafür zuständigen kompetenten Stelle objektiv und vor Inkrafttreten geprüft und zugelassen werden müssen.[331] Das Vorhandensein geforderter Datenschutzfunktionen könnte auch in Zulassungen überprüft werden, die in bestimmten Bereichen die Qualität des Systems – auch bezogen auf die Risiken seiner Nutzung – überprüfen. Beispiele hierfür sind die Zulassungen von Kraftfahrzeugen und von Medizinprodukten. Auch wird vorgeschlagen, vor dem Einsatz bestimmter risikoreicher algorithmenbasierter Entscheidungssysteme die Qualität der Daten, die Qualität der statistischen Modelle sowie die Diskriminierungsfreiheit und Nachvollziehbarkeit der Ergebnisse durch eine hierfür vorgesehene Stelle überprüfen zu lassen.[332]

Ein dritter Ansatz ist mit Art. 80 DSGVO angedeutet, nämlich die Kollektivierung der Rechtewahrnehmung: Die Feststellung und Verfolgung eines Rechts wird nicht mehr allein der Privatinitiative einer betroffenen Person überlassen, sondern professionell von einem Verband übernommen. Die Datenschutz-Grundverordnung hat den Rechtsschutz im Datenschutz deutlich gestärkt. Beschwerde- und Klagerecht[333] sind dabei grundsätzlich bei der betroffenen Person verortet. Art. 80 Abs. 1 DSGVO ermöglicht die Beauftragung bestimmter Einrichtungen,

330 S. Kap. 2.1.1.2.
331 Roßnagel u.a., 2016, 130.
332 S. z.B. vzbv 2017, 3; Krafft/Zweig 2019, 42; Martini 2019, 73 f.
333 Art. 77 ff. DSGVO.

Organisationen oder Vereinigungen.[334] Vertretungsberechtigt sind unter anderem die Verbraucherzentralen in Deutschland.[335] Ob diese jedoch auch unabhängig von einer Beauftragung durch die betroffene Person tätig werden können, obliegt nach Art. 80 Abs. 2 DSGVO den Mitgliedstaaten.[336] Hier hält das deutsche Recht mit § 2 UKlaG eine entsprechende Regelung bereit, die jedoch kein eigenständiges Beschwerderecht qualifizierter Einrichtungen etabliert. Zudem soll § 2 Abs. 2 Satz 1 Nr. 11 UklaG nach Maßgabe von § 2 Abs. 2 Satz 2 UKlaG nicht greifen, „wenn personenbezogene Daten eines Verbrauchers von einem Unternehmer ausschließlich für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Verbraucher erhoben, verarbeitet oder genutzt werden“. Hier sollte eine Ausweitung erfolgen. Die nationale Umsetzung von Art. 80 Abs. 2 DSGVO bleibt hinten den Möglichkeiten zurück, die die Öffnungsklausel bietet. Auch der Kreis der Vertretungsberechtigten könnte mit Blick auf Art. 80 Abs. 1 DSGVO weiter gefasst werden – jenseits von Verbraucherschutzverbänden im Sinne von § 3 und 4 UKlaG. Der nationale Gesetzgeber sollte ein echtes Verbandsklagerecht zulassen, das es ermöglicht, auch unabhängig von Einzelfällen offene Fragen des Datenschutzrechts grundsätzlich zu klären.

Zu beachten ist auch die Problematik hinter Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Auch wenn kein Erlaubnistatbestand nach lit. a bis e greift, so kann dennoch eine Verarbeitung personenbezogener Daten stattfinden, wenn der Verantwortliche eigene Interessen oder Interessen Dritter geltend machen kann. Dazu müssen diese Interessen im Vergleich mit den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person überwiegen.[337] Zusätzlich ist die Erforderlichkeit der Verarbeitung festzustellen. Die Abwägung und die Feststellung nimmt jedoch der Verantwortliche vor. Daher besteht die Gefahr, dass dieser in der Praxis zu einer Überschätzung der Erforderlichkeit der Verarbeitung und der eigenen Interessen sowie zu einer Unterschätzung der Interessen der betroffenen Person tendiert. Eine Korrektur dieser Fehleinschätzung findet aber allenfalls erst im Nachgang statt, wenn sich Risiken der fraglichen Verarbeitung für die betroffenen Personen bereits realisiert haben. Der zeitliche Abstand von der Verarbeitung bis zur Korrektur kann im Falle eines Rechtsstreits um die getroffene Abwägung stark anwachsen. Die betroffene Person muss hierzu aber zunächst feststellen können, dass eine rechtswidrige Verarbeitung stattfindet, und sie muss im zweiten Schritt Willens und fähig sein, gegen die Verarbeitung vorzugehen. Zur Stärkung der betroffenen Person sollte der Unionsgesetzgeber die Abwägung nicht den Verantwortlichen überlassen, sondern selbst Regelungen treffen, die in typischen Verarbeitungssituationen (z.B. Werbung oder Profiling) oder bei typischen Geschäftsmodellen (z.B. Suchmaschinen, Social Media) greifen. Klare Regelungen würden auch hier dazu beitragen, die Stellung des Verbrauchers zu stärken und Machtasymmetrien abzubauen.

---

334 Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet sind, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig sind. S. umfassend zur Vertretung betroffener Personen, Verbandsbeschwerde und Verbandsklage Geminn, in: Jandt/Steidle, 2019, B. VI. Rn. 103 ff.

335 S. § 3 und 4 UKlaG.

336 S. Weichert, 2017, 13.

337 S. zur Berücksichtigung der Interessen Dritter Kap. 3.3.4.

3.3.3 Verhinderung einer Überforderung der Verbraucher

Den Verbraucher können vor allem ungeeignete (zu viel oder zu wenig) Informationen und Entscheidungszwänge mit unzureichender Übersicht über die Folgen überfordern. Genau dies aber ist die Folge der gegenwärtigen Praxis, über alle vagen langfristig möglichen Datenverarbeitung bereits beim ersten Kontakt mit dem Verbraucher durch Verweis auf eine umfassende Datenschutzerklärung zu informieren. Auf Grundlage dieser viel zu umfassenden Informationen zu einem Zeitpunkt, zu dem sich der Verbraucher nicht für alle Details interessieren kann, von ihm eine Einwilligung zu verlangen oder die Daten auch ohne seine Zustimmung zu verarbeiten, muss den Verbraucher überfordern. Notwendig ist daher über die Regelungen der Art. 12 bis 14 DSGVO und die vorgeschlagenen Detailverbesserungen[338] hinaus ein neues, auch an den Interessen der betroffenen Person und nicht nur an der Aufwandsreduktion für den Verantwortlichen orientiertes Informationskonzept zu etablieren. Dieses muss folgende Eigenschaften der notwendigen Datenschutzinformationen sicherstellen: Die Informationen müssen

- entscheidungsrelevant (die Informationen, die für ein unmittelbar folgendes Handeln der betroffenen Person entscheidend sein können, so dass sie auf ihrer Grundlage entscheiden kann, einen Dienst zu nutzen, eine Funktion einzuschalten oder eine Einwilligung zu erteilen),
- interessenabhängig (die Information, die dem Interesse und der Aufmerksamkeit der betroffenen Person in der jeweiligen Situation entspricht. Sie muss z.B. zwischen mehreren Sichten wählen können: Symbol – Kurzinformation – ausführlichere Information – gesamte Datenschutzerklärung) und
- rechtzeitig (die Information erfolgt immer unmittelbar vor der Handlung der betroffenen Person, die die Datenverarbeitung verursacht, in einer Weise, dass sie diese Handlung auch noch unterlassen kann)

angeboten werden.

Beispielsweise wäre im Smart Car eine situationsangepasste Information notwendig, die mindestens drei Ebenen umfasst:[339] Allgemeine Strukturinformationen sollten ständig – auf einer Website – bereitgehalten werden, auf die mit dem Kaufvertrag und in Allgemeinen Geschäftsbedingungen aufmerksam gemacht wird. Mit der Inbetriebnahme der jeweiligen Funktion muss im Auto eine technische Anzeige erfolgen, dass diese Funktion eingeschaltet ist, und schließlich muss bei der aktuellen Nutzung des Automobils z.B. auf dem Armaturenbrett auf die derzeit genutzten Dienste hingewiesen werden. Bei einer Aktivierung der Anzeige können weitere Informationen zum Datenschutz abgerufen werden. Untersuchungen zur Umsetzung von Transparenzanforderungen im vernetzten Auto zeigen, dass es hier prinzipiell umsetzbare Ansätze gibt;[340] diese bedürfen jedoch der Erprobung und Fortentwicklung mit Blick auf die immer weiter fortschreitende Vernetzung mit der Infrastruktur.[341]

---

338 S. Kap. 2.3.9 bis 2.3.13.
339 S. hierzu auch Husemann, in: Roßnagel/Hornung, 2019, 367 ff.
340 S. z.B. Bönninger/Eichelmann/Methner, in: Roßnagel/Hornung, 2019, 355 ff.
341 S. Roßnagel/Hornung, in: Roßnagel/Hornung, 2019, 475.

Hilfreich ist auch eine Prüfung durch Dritte, denen der Verbraucher vertraut. Hierfür sieht die Datenschutz-Grundverordnung in Art. 42 und 43 als Innovation des Datenschutzrechts eine freiwillige Zertifizierung der Datenschutzkonformität einer Anwendung vor.[342] Fraglich ist, welche rechtlichen und technischen Möglichkeiten der Unterstützung der Verbraucher gegeben sind. Die Zertifizierung sollte für bestimmte Bereiche verpflichtend sein. Orientierungskriterium könnte sein, dass dann, wenn Produkte oder Dienste, denen die Verarbeitung personenbezogener Daten dient, zulassungsbedürftig sind, auch die Feststellung der Datenschutzrechtskonformität der Datenverarbeitung in Form eines Zertifikats obligatorisch ist. Dies würde zum Beispiel für viele Dienste und Produkte, die Gesundheitsdaten verarbeiten, oder für vernetzte und automatisiert fahrende Kraftfahrzeuge zutreffen.[343]

Die Durchsetzung der Datenschutzprinzipien kann durch eine konsequent datenschutzfreundliche Technikgestaltung bewirkt werden. Die Gestaltung insbesondere von komplexer Informationssystemen muss dabei so erfolgen, dass Datenschutz nicht zur Belästigung des Verbrauchers wird, sondern situationsadäquat und wo möglich auch automatisiert erfolgt. Einwilligungen könnten etwa nach vordefinierten Kriterien automatisiert durch ein digitales „Alter Ego“ des Verbrauchers in dessen Auftrag erteilt werden und Geräteeinstellungen ebenfalls automatisiert an dessen Vorstellungen zum Datenschutz angepasst werden.[344] Das „Alter Ego“ kontrolliert die Einhaltung der gemachten Vorgaben durch den Datenverarbeiter. So könnte Kontrolle über Datenverarbeitungsvorgänge auch bei immer komplexerer Datenverarbeitung erreicht werden, ohne zu einer Überforderung der betroffenen Person zu führen. Erreicht werden kann dies nur, wenn die Technik entsprechende Schnittstellen bereitstellt, über die das „Alter Ego“ mit ihr in Kontakt treten und die Vorgaben des Verbrauchers kommunizieren kann.

3.3.4 Verhinderung negativer Auswirkungen auf Dritte

Die Verarbeitung personenbezogener Daten, aber auch anonymer Daten kann Risiken für die Entscheidungs- und Entfaltungsfreiheit Dritter sowie für deren diskriminierende Behandlung in Form gruppenbezogener Schlechterstellung bewirken. Werden diese Daten für die Erstellung von Statistiken im Rahmen von Big-Data-Analysen und von selbstlernenden algorithmenbasierten Entscheidungssystemen genutzt, entstehen Bewertungen von Eigenschaften sowie Verhaltensprognosen und -beeinflussungen auch dritter Personen, die gar keine Daten für diese Analysen geliefert haben. Durch die anonyme Vergemeinschaftung aller Merkmalsträger im Rahmen der Statistiken werden ihnen die gleichen Eigenschaften zugeordnet und durch die Normativität der durch die Statistiken beschriebenen Normalität haben diese Statistiken verhaltensbestimmende Wirkung. Viele Verbraucher werden Vorteile daraus ziehen wollen, sich „normal“ zu verhalten, sofern diese Normalität als Entscheidungsgrundlage bei Anbietern dient. Hinzu kommt, dass aus diesem Wissen über statistisch wahrscheinliches Verhalten und über statistisch wahrscheinliche Wirkungen bestimmter Anreize gezielte Verhaltenssteuerungen erfolgen.[345]

342 S. z.B. Maier/Bile, DuD 2019, 478 ff.
343 S. auch Kap. 3.3.1.
344 Roßnagel u.a., 2016, 134 f.
345 S. hierzu näher Kap. 3.2.

Datenschutzrecht ist bezogen auf die beeinträchtigten Dritten nicht anwendbar. Soweit anonyme Daten verarbeitet werden, scheidet Datenschutzrecht mangels Personenbezugs der Daten aus. Soweit personenbezogene Daten verarbeitet werden, sind diese Daten anderen betroffenen Personen zuzuordnen und gerade nicht den Dritten. Diese können keine Betroffenenrechte geltend machen. Da der sachliche Anwendungsbereich des Datenschutzrechts mangels Verwendung personenbezogener Daten nicht eröffnet ist, fehlt ein effektiver rechtlicher Schutz des Verbrauchers vor den aufgezeigten Risiken durch statistische Verhaltensmuster.

Dennoch können sie die Grundrechtsausübung und das demokratische Engagement gefährden.[346] Durch das Einordnen des Verhaltens in statistische Handlungsmuster als konform oder nicht konform und durch das so indirekt erzwungene Anpassungsverhalten werden die Entscheidungs- und die Verhaltensfreiheit faktisch eingeschränkt, was das Recht auf informationelle Selbstbestimmung gerade vermeiden soll. Solche statistischen Muster verstärken die Normativität der Normalität und reduzieren „Soziodiversität". Diese ist aber Voraussetzungen für Innovationen und Demokratie.[347] Für die Verwirklichungsbedingungen von Grundrechten und Demokratie hat der Staat aber eine Schutzpflicht. Diese fordert ein angemessenes Handeln und rechtfertigt sogar verhältnismäßige Beschränkungen von Grundrechten, wenn dies zum Schutz von Selbstbestimmung, freier Entfaltung und Funktionsfähigkeit der Demokratie erforderlich ist.

Rechtliche Schutzmaßnahmen könnten bei der Einwilligung ansetzen. Da der Einwilligende nur für sich, nicht aber zu Lasten Dritter rechtfertigen kann, könnte die Möglichkeit der Einwilligung beschränkt werden, wenn sie nicht nur Folgen für den Einwilligenden, sondern auch für einen Dritten hat. Sie könnte etwa in bestimmten Verarbeitungskontexten als Rechtfertigungsgrundlage für eine Verarbeitung personenbezogener Daten ausgeschlossen oder zumindest befristet werden.[348] Auch könnten die Voraussetzungen für die Wirksamkeit einer Einwilligung je nach Risiko der Verarbeitung skalieren. Sie könnte etwa von der Erfüllung gesteigerter Transparenzpflichten des Verantwortlichen abhängig gemacht werden, der auch über die Folgen der Datenverarbeitung für Dritte informieren muss. Der Einwilligende müsste dann konsequenter Weise auch für die Folgen seiner Einwilligung verantwortlich sein.

Ein solcher Ansatz könnte vor allem dann gerechtfertigt sein, wenn betroffene Personen als Gegenleistung für Rabatte, Boni oder gar die kostenlose Nutzung eines Dienstes mit der Preisgabe ihrer Daten und der Einwilligung zu einer (fast) unbegrenzten Nutzung dieser Daten bezahlen und sich dabei nicht um die negativen Folgen für andere kümmern oder diese zu ihrem Vorteil bewusst in Kauf nehmen.

Gegen diesen Ansatz spricht jedoch, dass die Einwilligung meist nicht der einzige Weg ist, die Daten für statistische Muster oder Modelle zu erlangen. Die statistische Verarbeitung personenbezogener Daten kann auch aufgrund anderer gesetzlicher Erlaubnistatbestände erfolgen. Über eine Zweckänderung für eine statistische Verarbeitung der personenbezogenen Daten muss der Verantwortliche nach Art. 13 Abs. 3 und 14 Abs. 4 DSGVO die betroffene Person

346 S. z.B. Weichert, ZD 2013, 251 ff.; Roßnagel, ZD 2013, 562 ff.
347 S. Roßnagel/Nebel, DuD 2015, 455.
348 S. Roßnagel u.a., 2016, 130 f.

zwar informieren. Diese Information kommt aber für eine Verhinderung der statistischen Datenverarbeitung zu spät. Sind die Daten inzwischen anonymisiert, fällt die Verarbeitung ohnehin aus dem Anwendungsbereich des Datenschutzrechts heraus. Von den betroffenen Personen den Verzicht auf (vermeintlich) kostenlose Dienste zu verlangen, auf die sie dringend angewiesen sind, weil die mit ihren Daten erzeugten statistischen Muster oder Modelle zum Nachteil von Dritten genutzt werden können, dürfte meist unverhältnismäßig sein. Auch dürfte es schwer sein, vor der Einwilligung oder vor der Nutzung eines Dienstes zu prognostizieren, was mit den Daten geschieht und für wen die nachfolgende Datenverarbeitung welche Nachteile oder Vorteile verursacht. Außerdem liegt der Schwerpunkt der nachträglichen benachteiligenden Nutzung der Daten nicht bei der betroffenen Person, sondern beim Verantwortlichen.

Der Schutz Dritter muss daher beim Verantwortlichen ansetzen. Dieser erhebt die Daten bei der betroffenen Person und verantwortet die statistische Muster- oder Modellerstellung aus diesen Daten als Grundlage für die Anwendung bei anderen Nutzern. Auch wenn der Verantwortliche, der die Daten erhebt, sich von demjenigen unterscheidet, der die statistischen Muster oder Modelle erstellt, und von demjenigen, der die Muster oder Modelle auf Dritte anwendet, so sind sie doch alle Verantwortliche, solange die Daten noch personenbezogen sind. Für den ersten, der die Daten erhebt, und für den zweiten, der personenbezogene Daten in statistischen Mustern oder für solche anonymisiert, handelt es sich um Zweckänderungen, die dem Datenschutzrecht unterfallen. Soweit der Anwender die aus der Statistik gewonnenen Entscheidungsmodelle – im Rahmen algorithmenbasierter Datenverarbeitungen – auf individualisierbare Dritte anwendet, ist er für diese Datenverarbeitung datenschutzrechtlich verantwortlich. Datenschutzrechtlich führt diese Form der Datenverarbeitung zumindest zu drei Fragen:

Auf welcher Rechtsgrundlage dürfen personenbezogene Daten erhoben und für solche statistischen Zwecke verarbeitet werden? Ist die Erhebung nicht durch Einwilligungen gerechtfertigt, kommt eine Rechtfertigung durch überwiegende berechtigte Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO in Betracht.[349] Diese Vorschrift erlaubt, auch berechtigte Interessen Dritter zu berücksichtigen. Warum aber ist sie nur mit den „Interessen oder Grundrechte(n) und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern," abzuwägen und nicht auch mit denen aller anderen betroffenen Dritten? Eine Schutzmöglichkeit könnte sein, in den Gesetzestext auch die Interessen oder Grundrechte und Grundfreiheiten Dritter aufzunehmen. Der statistischen Verarbeitung geht im Regelfall eine Zweckänderung voraus. Da diese statistische Verarbeitung nicht unter die Ausnahme für die öffentliche Statistik des Art. 5 Abs. 1 lit. b DSGVO fällt,[350] ist sie als Zweckänderung nach Art. 6 Abs. 4 DSGVO nur zulässig, wenn sie mit dem bisherigen Zweck vereinbar ist. Hier könnte eine Klarstellung in Art. 6 Abs. 4 DSGVO erfolgen, dass dies nicht der Fall ist, wenn die Daten als Material für selbstlernende algorithmenbasierte Systeme oder für Big Data-Muster einer bestimmten Risikoklasse[351] verwendet werden sollen.

Soweit statistische Muster erstellt und selbstlernende algorithmenbasierte Systeme trainiert werden sollen, sind qualitative Anforderungen an die Daten und ihre Verarbeitung aufzustellen,

349 S. hierzu auch Kap. 3.3.2.
350 S. Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 5 Rn. 107.
351 S. zur Einteilung in Risikoklassen Krafft/Zweig, 2019, 31 ff.

die je nach Risikoklasse unterschiedlich stark kontrolliert werden sollten. Ein Vorschlag für solche qualitativen Anforderungen finden sich in dem vorgeschlagenen neuen Abs. 4 von Art. 22 DSGVO.[352]

Die Anwendung der statistischen Muster im Einzelfall, ist vom Datenschutzrecht nur dann erfasst, wenn es dabei wiederum zur Verarbeitung personenbezogener Daten kommt. Werden die personenbezogenen Daten von algorithmenbasierten Entscheidungssystemen verarbeitet, fällt dies in den Anwendungsbereich des bestehenden oder – wie hier vorgeschlagen[353] – modifizierten Art. 22 DSGVO. Die Kontrolle der Wirkungen kann jedoch – insbesondere für Diskriminierungen – aus dem Anwendungsbereich dieser Vorschrift herausfallen.

Letztlich weist das Thema der negativen Auswirkungen der Datenverarbeitung auf Dritte über das Datenschutzrecht hinaus, das dem Schutz der informationellen Selbstbestimmung dient.[354] Es betrifft neben der Selbstbestimmung und Selbstentfaltung auch Fragen der Gleichbehandlung, der Gerechtigkeit und der Rechtsstaatlichkeit. Für dieses Thema sollte daher ein den Datenschutz einbeziehendes, aber über diesen hinausgehendes Schutzkonzept gesucht werden.

Dies gilt vor allem für die Verwendung von anonymen Daten. Diese wirft zum einen Fragen auf nach der Zulässigkeit der Anwendung von Ergebnissen aus Big-Data-Analysen, zum anderen Fragen nach der Notwendigkeit eines Schutzkonzeptes auch für anonymisierte Daten.

Beispiele für solche Schutzkonzepte lassen sich im außereuropäischen Ausland bereits finden. Japan hat etwa im Zuge einer umfassenden Reform seines Datenschutzrechts auch Regelungen für sogenannte „anonymously processed information“ eingeführt.[355] Dabei handelt es sich um personenbezogene Daten, die einer Anonymisierung unterzogen wurden und nun ohne Personenbezug sind. Das japanische Datenschutzrecht sieht für solche Daten Maßnahmen zur Datensicherheit vor, die der Datenverarbeiter ergreifen muss. Diese Maßnahmen betreffen sowohl das Verfahren zur Entfernung des Personenbezuges als auch den Umgang mit den anonymisierten Daten. Darüber hinaus treffen den Datenverarbeiter Informationspflichten bezogen auf die Kategorien von Informationen, die in den anonymisierten Daten enthalten sind. Ergänzt wird dies durch ein Verbot, anonymisierte Daten mit anderen Daten zusammenzuführen, um den Personenbezug wiederherzustellen. Ein Verantwortlicher darf auch im Anonymisierungsverfahren entfernte, aber noch andernorts vorhandene Merkmale nicht erwerben. Werden diese Vorgaben nicht beachtet, sieht das japanische Datenschutzrecht allerdings keine Bußgelder vor. Bezogen auf Datenübermittlungen aus der Europäischen Union gelten Daten nur dann als anonymisiert, wenn Informationen zur Anonymisierungsmethode unwiderruflich gelöscht werden und eine Re-Identifizierung der betroffenen Person unmöglich gemacht wird. Letztere, im Zuge des Angemessenheitsbeschlusses für Japan[356] eingeführte Ergänzung zeigt, dass konzeptionelle

352 S. Kap. 2.3.20.
353 S. Kap. 2.3.20.
354 S. auch vzbv 2017, 3; Schulz/Dreyer, 2018, 9; Krafft/Zweig, 2019, 16.
355 S. hierzu umfassend Geminn/Laubach/Fujiwara, ZD 2018, 413. Man beachte auch den gescheiterten Versuch der Kriminalisierung einer Re-Identifizierung durch die australische Privacy Amendment (Re-identification Offence) Bill 2016.
356 S. hierzu Fujiwara/Geminn/Roßnagel, ZD 2019, 204 ff.; Tatsumi, CR 2019, 424 ff.; Geminn/Laubach, ZD 2019, 403 ff.

Unterschiede bestehen, die eine direkte Übernahme drittstaatlicher Instrumente in der Europäischen Union verhindert. Dennoch können diese Vorbilder dazu anregen, konzeptionell weiter zu denken als die Datenschutz-Grundverordnung.

3.3.5 Stärkung der Datenschutzprinzipien

Die Datenschutzprinzipien stammen weitgehend aus einer Zeit, in der weder PCs noch das Internet bekannt waren. Allgegenwärtige Datenverarbeitung, die Auswertung unendlich vieler personenbezogener Daten aus verschiedensten Quellen, die Datenverarbeitung durch lernfähige Algorithmen und die Erfassung der Welt durch Systeme der Künstlichen Intelligenz machen neue, ergänzende oder präzisierende Grundsätze erforderlich, um die Grundrechte der Verbraucher auf Persönlichkeitsschutz und Selbstbestimmung auch in der künftigen Welt zu schützen.

Auch wenn die Datenschutz-Grundverordnung keine spezifischen Antworten auf diese gravierenden Herausforderungen bietet,[357] könnte erwartet werden, dass zumindest die allgemeinen Regelungen der Verordnung – vor allem die Grundsätze der Datenverarbeitung in Art. 5 DSGVO – ausreichend Schutz gewähren. Doch diese Grundsätze geraten durch die neuen technischen Herausforderungen unter einen massiven Druck, der ihre künftige Anwendbarkeit in Frage stellt.[358]

So verliert etwa die Zweckbindung bei allen Systemen ihren schützenden und steuernden Charakter, deren Verarbeitungszweck – wie etwa bei Assistenzsystemen im Auto, in der Wohnung, bei der Arbeit oder beim Hobby – in der umfassenden Unterstützung des Verbrauchers liegen. Dafür ist eine möglichst breite Datenbasis über Verhalten, Interessen und Vorlieben unerlässlich. Das eigentliche Ziel der Zweckbindung, Datenverarbeitung auf das erforderliche Maß zu begrenzen, wird dabei konterkariert, denn jede Information kann potenziell der Zweckerfüllung des Assistenten dienen. Der Grundsatz der Transparenz stößt an subjektive und objektive Grenzen. Subjektiv übersteigt die zu erwartende Vervielfachung der Datenverarbeitungsvorgänge in allen Lebensbereichen die mögliche Aufmerksamkeit, die zur Effektivität der Transparenz erforderlich ist, um ein Vielfaches. Objektiv setzen hohe Komplexität, vielfältige Zwecke und lernfähige Systeme der möglichen Transparenz hohe Grenzen. Um ein letztes Beispiel zu geben: Die Grundsätze der Datenminimierung und der Speicherbegrenzung sind an den jeweils begrenzten Zweck gebunden. Ebenso wie dieser werden auch diese Grundsätze ihre Steuerungskraft verlieren. Wenn der Zweck der Datenverarbeitung ohne wirkliche Grenzen ist, führt auch die Frage, welche Datenverarbeitung für diesen Zweck erforderlich ist, nicht mehr zu einer überschaubaren Eingrenzung erlaubter Datenverarbeitung. Wenn etwa das Gedächtnis der Dinge der betroffenen Person helfen soll, sich an vergessene Ereignisse zu erinnern, ist eine nach Umfang und Zeitraum grenzenlose Datenspeicherung erforderlich. Sensorbestückte Gegenstände und Umgebungen sind fast immer aktiv und erheben eine enorme Menge Daten, um den Verbrauchern nach ihrem – sich ständig ändernden – Bedarf jederzeit ihre Dienste anbieten zu können. Alle Systeme, die kontextsensitiv die betroffene Person entlasten oder unterstützen sollen, die Präferenzen des Nutzenden erkennen und ihnen gerecht werden sollen, können ihre Funktionen nur richtig erfüllen, wenn sie den Grundsatz der Datenminimierung und der Speicherbegrenzung ignorieren. In dem Konflikt zwischen modernen Technikanwendungen und

357 S. Kap. 3.3.1.
358 S. z.B. Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 367 ff.

Datenschutzgrundsätzen dürfte entscheidend sein, dass die neuen Technikanwendungen den betroffenen Personen in den meisten Fällen nicht aufgedrängt werden – in diesem Fall dürften die Grundsätze greifen –, sondern von diesen gewollt werden. Sie wollen sich mit ihrer Hilfe die Träume erfüllen, die sie sich von diesen Technikanwendungen erhoffen.[359] Die Grundsätze zum Schutz der Verbraucher gegen den aktuellen Willen der Verbraucher zur Geltung zu bringen, dürfte nahezu aussichtslos sein.

Obwohl diese Grundsätze durch moderne Datenverarbeitung in Frage gestellt werden, darf dies kein Grund sein, sie als rechtliche Gebote aufzuweichen. Vielmehr sollte durch gesteigerte Anforderungen an technisch-organisatorische Maßnahmen versucht werden, das Regelungsziel der Grundsätze zu erreichen. Viele Vorschläge zur Überarbeitung der Datenschutz-Grundverordnung dienen diesem Ziel.[360]

Neben diesen von der Datenschutz-Grundverordnung in Art. 5 anerkannten Grundsätze der Datenverarbeitung und den vorgeschlagenen Verbesserungen und Ergänzungen, fordert die technische Entwicklung neue zusätzliche Grundsätze zu diskutieren, anzuerkennen und umzusetzen. Insbesondere die Anwendungen Künstlicher Intelligenz erfordern neue Grundsätze. Als solche sind etwa zu diskutieren die nachgewiesene Relevanz (Aussagekraft) der Kriterien von Expertensystemen oder der Daten und der Algorithmen für lernende Systeme, die Nachvollziehbarkeit algorithmenbasierter Entscheidungen[361] und die Erklärbarkeit der Ergebnisse gegenüber der betroffenen Person[362] sowie die dauerhafte Überwachung besonders riskanter algorithmenbasierter Entscheidungssysteme.[363]

Um eine Stärkung der Datenschutzprinzipien in der Praxis zu erreichen, sollten greifbare Anreize für Datenverarbeiter zur Gewährleistung eines möglichst hohen Datenschutzniveaus gesetzt werden, um Eigennutz und Gemeinwohl in Einklang zu bringen.[364] Solche Anreize könnten beispielsweise durch die Einbeziehung von Datenschutzfragen als Vergabekriterien in öffentliche Ausschreibungen gesetzt werden.[365]

Zudem sollte ein umfassendes, institutionalisiertes Kontrollsystem zur Einhaltung von datenschutzrechtlichen Vorgaben eingerichtet werden, das neben Behörden auch Verbände und sonstige Einrichtungen einbezieht. Die Datenschutz-Grundverordnung hat hier bereits eine wesentliche Verbesserung des Status Quo bewirkt. Jedoch sollten die Funktionen und Strukturen von Systemen hier stärker in den Vordergrund gerückt werden, anstelle den Fokus auf das einzelne personenbezogene Datum zu richten.[366]

---

359 S. hierzu Roßnagel, in: Simitis/Hornung/Spiecker, 2019, Art. 5 DSGVO, Rn. 193.
360 S. zu diesen Kap. 2.3.
361 S. hierzu auch vzbv, 2017, 3 ff., 12; Schulz/Dreyer, 2018, 45 ff.
362 S. hierzu auch die Qualitätskriterien, die in Kap. 2.3.20 für automatisierte Entscheidungen im Einzelfall gefordert werden.
363 S. z.B. Krafft/Zweig 2019, 5; Martini, 2019, 22.
364 Roßnagel u.a., 2016, 138.
365 S. hierzu umfassend Bile u.a., in: Friedewald, 2018, 83 ff.
366 S. hierzu auch Roßnagel u.a., 2016, 138 f.

4. Gewährleistung der Zukunftsfähigkeit des Datenschutzrechts

Es zeigt sich, dass die Datenschutz-Grundverordnung das Ziel einer umfassenden Modernisierung und Harmonisierung des Datenschutzrechts verfehlt hat. Sie gibt aber als *Grund*verordnung eine gemeinsame Basis für den Datenschutz in der Europäischen Union und im Europäischen Wirtschaftsraum. Lediglich fünfzig materielle Datenschutzvorschriften geben den Rahmen vor für eine Verarbeitung personenbezogener Daten, die bereits heute und weiter zunehmend nahezu sämtliche Lebensbereiche durchdringt. Sie reicht dabei von der Kundendatei eines kleinen Unternehmens über die Verarbeitung im Sportverein bis hin zur massenhaften Verarbeitung im Kontext datengetriebener Geschäftsmodelle. Dieser risikoneutrale „One Size Fits All"-Ansatz macht bereichsspezifische Konkretisierungen und Ergänzungen des Datenschutzrechts unumgänglich, um auf spezifische Anforderungen einzelner Bereiche und Technologien sowie deren Risiken adäquat reagieren zu können. Diese Konkretisierungen und Ergänzungen können je nach Art und Abstraktionsgrad auf vielfältige Weise erfolgen. Denkbar sind:

(1) eine Überarbeitung der Datenschutz-Grundverordnung selbst infolge einer Evaluation ihrer Schwächen,

(2) die Erstellung bereichs- oder technologiespezifischer europäischer Verordnungen oder Richtlinien durch den europäischen Gesetzgeber,

(3) die Ergänzung und Konkretisierung der Datenschutz-Grundverordnung durch mitgliedstaatliches Recht im Rahmen des von der Verordnung belassenen nationalen Gestaltungsspielraums,

(4) Leitlinien und Empfehlungen des Europäischen Datenschutzausschusses,

(5) die Erarbeitung von Standards auf Ebene der datenverarbeitenden Unternehmen selbst und branchenspezifische Verhaltensregelungen nach Art. 40 und 41[367] sowie

(6) Regeln der technischen Normung in Normungsorganisationen wie ISO, CEN und DIN.

Dabei soll nicht in Zweifel gezogen werden, dass die Datenschutz-Grundverordnung bereits zahlreiche notwendige Innovationen und Verbesserungen im Vergleich zur Datenschutzrichtlinie enthält. Der Erfolg dieser Innovationen und Verbesserungen ist jedoch davon abhängig, dass diese in der Praxis auch gelebt werden. Dies kann nur gelingen, wenn ihre Durchsetzung durch die Aufsichtsbehörden und die Gerichte, soweit es ihnen möglich ist, konsequent erfolgt. Zudem müssen aber auch handhabbare Erläuterungen gegeben werden, die klarstellen, wie die oft nur unscharf umrissenen Vorgaben der Grundverordnung umzusetzen sind. Die Leitlinien der Datenschutzgruppe und des Ausschusses sind dabei nur ein Anfang.

Die Regelung des Art. 97 DSGVO zur regelmäßigen Evaluation der Verordnung ist Ausdruck der Erkenntnis, dass die Digitalisierung die Gesellschaft sehr schnell und nachhaltig verändert und dass der Schutz der Werte, die in diesem Wandel unverändert bleiben sollen, sich immer wieder anpassen muss. Art. 97 DSGVO ist auch Ausdruck davon, dass die Datenschutz-Grundverordnung nur ein erster Entwurf einer unionsweiten Datenschutzregelung ist, der bei gegebenen Interessengegensätzen und Machtverhältnissen durchsetzbar war. Sie ist ein Entwurf, der

[367] S. zu diesen Roßnagel, in: Roßnagel 2018, 202 ff.

angesichts neuer Herausforderungen für Persönlichkeitsrechte und Demokratie immer wieder neu zu konzipieren und zu verhandeln ist.

Hierfür ist jedoch zu beachten, dass die Datenschutz-Grundverordnung zwei grundlegende Ziele verfolgt, die miteinander in Konflikt geraten können. Beide hat sie nicht konsequent umgesetzt. Zum einen will sie das Datenschutzrecht unionsweit vereinheitlichen und einen soliden, „kohärenten und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union" schaffen.[368] Dieses Ziel hat sie insofern erreicht, als ihr Text nach Art. 288 Abs. 2 Satz 1 AEUV in allen Mitgliedstaaten unmittelbar gilt. Sie hat es jedoch dadurch verfehlt, dass sie in 70 Öffnungsklauseln den Mitgliedstaaten die Möglichkeit eröffnet, in wichtigen Regelungsbereichen (z.B. öffentliche Verwaltung, Medien, Arbeit, Forschung) jeweils eigene und damit unterschiedliche Datenschutzregelungen zu erlassen. Statt Vereinheitlichung sieht die verabschiedete Datenschutz-Grundverordnung deshalb – letztlich zurecht – eine Ko-Regulierung zwischen unionaler und mitgliedstaatlicher Ebene vor.[369] Zum anderen will sie den Datenschutz angesichts der Herausforderungen der technischen Entwicklung modernisieren und den Schutz der Grundrechte verbessern.[370] Dieses Ziel hat sie dadurch verfehlt, dass sie wegen übertriebener Technikneutralität keine der modernen Herausforderungen risikospezifisch aufgegriffen hat.[371]

Soll das Ziel der Vereinheitlichung in den folgenden Evaluationen erreicht werden, setzt dies als rechtspolitische Vorgehensweise Zentralisierung und Monopolisierung der weiteren Fortentwicklung des Datenschutzrechts voraus. Soll das Ziel der Modernisierung, die den künftigen Herausforderungen für Grundrechte und Demokratie gerecht werden will, erreicht werden, erfordert dieses als Vorgehensweise eine den Herausforderungen angemessene Evolution des Datenschutzrechts nach dessen Prinzipien der Variation und Selektion.

Die von der Datenschutz-Grundverordnung realisierte Ko-Regulierung ermöglicht, diesen Widerspruch der Vorgehendweisen aufzulösen. Denn eine reine Zentralisierung und Monopolisierung der Fortentwicklung des Datenschutzrechts, wie sie im Entwurf der Europäischen Kommission zur Datenschutz-Grundverordnung aus dem Jahr 2012 noch vorgesehen war,[372] ist letztlich innovationsschädlich. Dagegen ermöglicht die durchgesetzte Ko-Regulierung die Erprobung neuer Konzepte durch die Mitgliedstaaten im Rahmen des Gestaltungsspielraums, den die Datenschutz-Grundverordnung den Mitgliedstaaten belässt. Nur so ist die notwendige Komplexität der Datenschutzregelungen angesichts einer sich ständig wandelnden, gesellschaftsweiten Verarbeitung personenbezogener Daten auch zu erreichen. Die Suche nach einem modernen Datenschutzrecht muss einem in sich stimmigen, demokratischen und pluralistischen Modell der Evolution des Datenschutzrechts folgen. Dieses könnte unter anderem wie folgt aussehen:

Die notwendige Variation von Lösungsansätzen könnte dadurch erreicht werden, dass die Mitgliedstaaten – innerhalb des Spielraumes der Datenschutz-Grundverordnung – vielfältige neue

368 S. hierzu Erwägungsgründe 3 und 9 DSGVO.
369 S. hierzu näher Roßnagel, in: Roßnagel 2018, 31 ff.
370 S. hierzu Erwägungsgründe 1, 2, 4 und 6 DSGVO.
371 S. hierzu näher Roßnagel, in: Roßnagel 2018, 34 f.
372 S. Roßnagel, in: Roßnagel 2018, 28 ff.

Datenschutzkonzepte erproben, die auf immer neue Herausforderungen moderner Informationstechnik reagieren oder diese sogar steuern.[373] Angesichts der Vielfalt und Dynamik der zukünftigen, heute noch unbekannten Herausforderungen der Digitalisierung für die Grundrechte kann auf der Ebene der Mitgliedstaaten mit unterschiedlichen Regelungskonzepten experimentiert werden. Dadurch können vielfältige Quellen dazu beitragen, dass sich in der Union ein lebendiger Datenschutz entwickelt. Statt einer Vereinheitlichung der Datenschutzpraxis ermöglichen unbestimmte Rechtsbegriffe und ihre situationsgerechte Konkretisierung, dass in den einzelnen Mitgliedstaaten Datenschutz den lokalen Bedingungen angepasst werden kann. Schließlich bieten die vielen Regelungsmöglichkeiten der Mitgliedstaaten Chancen für eine Modernisierung des Datenschutzrechts, indem dort versucht wird, durch risikoadäquate Regelungen einen ausreichenden Schutz der Grundrechte gegen künftige Herausforderungen zu gewährleisten. Erfolgreiche Regulierungsmodelle können in andere Mitgliedstaaten und darüber hinaus exportiert werden. So entsteht ein pluralistisches Modell, bei dem zahlreiche Mitspieler die Evolution des Datenschutzrechts vorantreiben.[374] Die notwendige Harmonisierung des Datenschutzrechts im europäischen Binnenmarkt wird dabei durch die Grundverordnung selbst gewährleistet.

Die Kommission sollte diese Variationen nicht als Verstoß gegen die Datenschutz-Grundverordnung ansehen, sondern deren Anwendung in einem oder mehreren Mitgliedstaaten als geeignetes Mittel verstehen, um eine Erprobung der verschiedenen Datenschutzkonzepte in der Praxis durchzuführen. Solange diese nicht gegen grundlegende Festlegungen der Datenschutz-Grundverordnung verstoßen, helfen sie, diese durch Erfahrung mit neuen und angepassten Datenschutzkonzepten zu verbessern.

In den regelmäßigen Evaluationen der Kommission zur Umsetzung der Datenschutz-Grundverordnung findet eine Bewertung und Selektion der verschiedenen Datenschutzkonzepte statt. In den Diskussionen über den Evaluationsbericht haben alle Interessierte die Möglichkeit, ihre individuellen Bewertungen in die Evaluation einzubringen. Hier werden die Erfolge für den Grundrechtsschutz der Betroffenen und für den Ausgleich mit den Grundrechtspositionen und den öffentlichen Interessen der Datenverarbeiter bewertet.

Schließlich finden in regelmäßigen Novellen zur Datenschutz-Grundverordnung Festlegungen durch den Unionsgesetzgeber statt, in denen er das in einzelnen Mitgliedstaaten Bewährte unionsweit übernimmt. So kann die notwendige Modernisierung des Datenschutzrechts mit seiner notwendigen Vereinheitlichung in der Europäischen Union vereinbart werden.

---

373 Ein verbraucherrelevantes Beispiel ist § 31 BDSG.

374 S. hierzu ausführlicher Roßnagel, in: Roßnagel/Friedewald/Hansen, 2018, 383 f.

5. Zusammenfassung der Ergebnisse

Die Innovationen der Datenschutz-Grundverordnung können sich nur entfalten, wenn ausreichend konkrete Regelungen eine effektive Anwendung gewährleisten. Rechtsunsicherheit muss vermieden werden. Dabei schlägt die Datenschutz-Grundverordnung an vielen Stellen zu stark in Richtung Offenheit aus und verhindert mangels Präzisierung, dass Pflichten ernst genommen werden und Datenschutz in allen Facetten auch tatsächlich gelebt wird. Der Erfolg der Innovationen der Datenschutz-Grundverordnung steht und fällt mit diesen Präzisierungen. Hierzu hat dieses Gutachten Vorschläge unterbreitet, die im Rahmen der Evaluation der Datenschutz-Grundverordnung im Jahr 2020 für eine konstruktive Weiterentwicklung der Verordnung genutzt werden können. Bei der Erarbeitung dieser Vorschläge stand die Sicht des Verbrauchers im Mittelpunkt. Dessen Stellung zu stärken und Machtasymmetrien zwischen Verarbeitern und betroffenen Personen abzubauen steht im Einklang mit dem erklärten Ziel der Datenschutz-Grundverordnung, die Verarbeitung personenbezogener Daten in die Dienste der Menschheit zu stellen[375] und die Rechte und Freiheiten der betroffenen Personen – freilich unter Beachtung der Rechte der Datenverarbeiter – zu wahren und zu ihrem Wohlergehen beizutragen.[376]

Die Untersuchung hat gezeigt, dass bereits kleine Veränderungen des Wortlauts im Normtext der Datenschutz-Grundverordnung eine deutlich verbraucherstärkende Wirkung entfalten und Fehlentwicklungen vorbeugen können. An einigen Stellen ist jedoch eine umfassende Präzisierung und Klarstellung durch Leitlinien des Europäischen Datenschutzausschusses unerlässlich.

Auch mit der Evaluation der Datenschutz-Grundverordnung im Jahr 2020 darf der datenschutzrechtliche Diskurs nicht stehen bleiben. Die Grundprinzipien des Datenschutzes in Europa sind in ihren Grundzügen seit den 1970er Jahren im Wesentlichen unverändert geblieben. Die seither realisierten technischen Innovationen sowie die absehbare zukünftige technische Entwicklung machen es notwendig, auch diese Grundprinzipien zu hinterfragen und weiterzuentwickeln.

375 S. Erwägungsgrund 4 Satz 1 DSGVO.
376 S. Erwägungsgründe 2 und 4 DSGVO.

6. Summary

The innovations of the General Data Protection Regulation can only unfold, if sufficiently concrete provisions ensure an effective application. Legal uncertainty must be avoided. However, in many places the GDPR goes too far in the direction of openness and thus prevents – for lack of specification – that legal obligations are taken seriously, and that data protection is appreciated in all its facets. The success of the innovations of the GDPR depends on these specifications. This report has made recommendations to this end which can be taken advantage of in the context of the evaluation of the GDPR in 2020 in order to constructively advance the regulation. While drafting these recommendations, the view of the consumer took centre stage. Strengthening the position of the consumer and to reduce asymmetry between controller and data subject is in line with the pronounced goal of the GDPR to have the processing of personal data serve mankind[377] and to safeguard the fundamental rights and freedoms of data subjects while and contribute to the well-being of natural persons – indeed with respect to the rights of the controllers.[378]

This report has demonstrated that even small changes in the wording of the provisions of the regulation can have a significant effect in strengthening the position of consumers and to prevent aberration. In some places however, extensive specification and clarification through guidelines issued by the European Data Protection Board is irremissible.

The discourse about data protection law must not stop with the evaluation of the GDPR in 2020. The fundamental principles of data protection in Europe have remained essentially unchanged since the 1970s. The technological innovations that have taken place since then as well as the foreseeable technological evaluation necessitate that we question these fundamental principles and that we evolve them.

377 Recital 4(1) GDPR.
378 Recitals 2 and 4 GDPR.

Literatur

Abel, R. B., Automatisierte Entscheidungen im Einzelfall gem. Art. 22 DS-GVO, ZD 2018, 304-307.

Albrecht, J. P., Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, 88-98.

Albrecht, J. P./Jotzo, F., Das neue Datenschutzrecht der EU, Baden-Baden 2017 (zitiert: Bearbeiter, in: Albrecht/Jotzo).

Bayerisches Landesamt für Datenschutz, 8. Tätigkeitsbericht 2017/2018, Arnsberg 2019.

Bergt, M., Sanktionierung von Verstößen gegen die Datenschutz-Grundverordnung, DuD 2017, 555-561.

Bieker, F./Bremert, B./Hansen, M., Die Risikobeurteilung nach der DSGVO, DuD 2018, 492-496.

Bischoff, B., Drohnen im rechtlichen Praxistest, DuD 2017, 142-146.

BITKOM, Kinder und Jugend in der digitalen Welt, Berlin 2017.

Born, T., Bonitätsprüfungen im Online-Handel – Scorewert-basierte automatisierte Entscheidung über das Angebot von Zahlungsmöglichkeiten, ZD 2015, 66-72.

Buchner, B., Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155-161.

Buchner, B., Von der Wiege bis zur Bahre? – Datenschutz im Familienrecht unter der DSGVO, FamRZ 2019, 665-671.

Bundesregierung, Germany, in: Council of the European Union, Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) – Comments from Member States, No. prev. doc.: 11292/19, Brussels 2019, https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf.

Dammann, U., Der EuGH im Internet – Ende des internationalen Datenschutzes?, RDV 2004, 19-21.

Dausend, T., Der Auskunftsanspruch in der Unternehmenspraxis. Beispiel zur Bearbeitung von Betroffenenanfragen und Exkurs zur Reichweite des Auskunftsanspruchs, ZD 2019, 103-107.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Tätigkeitsbericht 2017-2018, 27. Tätigkeitsbericht, Berlin 2019.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Tätigkeitsbericht Datenschutz 2018, 27. Tätigkeitsbericht, Hamburg 2019.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Vierzehnter Tätigkeitsbericht zum Datenschutz, Schwerin 2019.

Dieterich, D., Rechtsdurchsetzungsmöglichkeiten der DS-GVO - Einheitlicher Rechtsrahmen führt nicht zwangsläufig zu einheitlicher Rechtsanwendung, ZD 2016, 260-266.

Dochow, C., Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, Baden-Baden 2017.

Dorfleitner, D./Hornuf, L, Analyse der Datenschutzerklärungen deutscher FinTech-Unternehmen nach Einführung der DSGVO, Münster 2018.

Dünkel, H., Kollektiver Rechtsschutz bei Datenschutzrechtsverstößen – Durchsetzung der DSGVO durch deutsche Verbraucherverbände, DuD 2019, 483-487.

Eckhardt, J./Menz, K., Bußgeldsanktionen der DS-GVO, DuD 2018, 139-144.

Eifert, M./Hoffmann-Riem, W. (Hrsg.), Innovationsfördernde Regulierung, Berlin 2009.

Ehmann, E./Selmayr, M. (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2. Aufl. München 2018 (zitiert: Bearbeiter, in: Ehmann/Selmayr, DSGVO 2018).

Eifert, M./Hoffmann-Riem, W. (Hrsg.), Geistiges Eigentum und Innovation, Band 1, Berlin-Steglitz 2011 (zitiert: Bearbeiter, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation und Recht, 2011).

Engeler, M., Das überschätzte Kopplungsverbot, ZD 2018, 55-62.

Engeler, M./Quiel, P., Recht auf Kopie und Auskunftsanspruch im Datenschutzrecht, NJW 2019, 2201-2205.

Eßer, M./Kramer, P./v. Lewinski, K. (Hrsg.), Auernhammer DSGVO/BDSG, 6. Aufl., Köln 2018 (zitiert: Bearbeiter, in: Auernhammer).

Faust, S./Spittka, J./Wybitul, T., Milliardenbußgelder nach der DS-GVO? - Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, ZD 2016, 120-125.

Friedewald, M. (Hrsg.), Privatheit und selbstbestimmtes Leben in der digitalen Welt, Wiesbaden 2018.

Friedewald, M./Schiering, I./Martin, N., Datenschutz-Folgenabschätzung in der Praxis - Herausforderungen bei der Implementierung eines innovativen Instruments der DSGVO, DuD 2019, 473-477.

Fujiwara, S./Geminn, C./Roßnagel, A.: Angemessenes Datenschutzniveau in Japan. Der Angemessenheitsbeschluss der Kommission und seine Folgen, ZD 2019, 204-208.

Geminn, C., Das Europäische Datenschutzrecht – Zwischen Leuchtturmfunktion und Werteexport?, DVBI 2018, 1539-1599.

Geminn, C., Das Smart Home als Herausforderung für das Datenschutzrecht. Enthält die Datenschutz-Grundverordnung risikoadäquate Regelungen?, DuD 2015, 575-580.

Geminn, C./Laubach, A., Gewährleistung einer unabhängigen Datenschutzaufsicht in Japan, ZD 2019, 403-407.

Geminn, C./Laubach, A./Fujiwara, S., Schutz anonymisierter Daten im japanischen Datenschutzrecht, ZD 2018, 413-420.

Gola, P. (Hrsg.), Datenschutz-Grundverordnung VO (EU) 2016/679, 2. Aufl. München 2018 (zitiert: Bearbeiter, in: Gola).

Gola, P./Lepperhoff, N., Reichweite des Haushalts- und Familienprivilegs bei der Datenverarbeitung - Aufnahme und Umfang der Ausnahmeregelung in der DS-GVO, ZD 2016, 9-12.

Greger, R., Kamera on board – Zur Zulässigkeit des Video-Beweises im Verkehrsunfallprozess, NZV 2015, 114-117.

Härting, N., Was ist eigentlich eine „Kopie“? Zur Auslegung des Art. 15 Abs. 3 Satz 1 DSGVO, CR 2019, 219-225.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit: 47. Tätigkeitsbericht Datenschutz, 1. Tätigkeitsbericht Informationsfreiheit, Wiesbaden 2019.

Hoffmann-Riem, W. (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018.

IHK München und Oberbayern, Datenschutz modernisieren, IHK-Positionen zur Evaluierung der DSGVO, 2019.

Jandt, S., Smart Health – Wird der DSGVO den dynamischen Herausforderungen gerecht?, DuD 2016, 571-574.

Jandt, S./Roßnagel, A., Datenschutz in Social Networks - Kollektive Verantwortlichkeit für die Datenverarbeitung, ZD 2011, 160-166.

Jandt, S./Steidle, R. (Hrsg.), Datenschutz im Internet – Rechtshandbuch zu DSGVO und BDSG, Baden-Baden 2018 (zitiert: Bearbeiter, in: Jandt/Steidle (Hrsg.), Datenschutz im Internet, 2019).

Jülicher, T./Röttgen, C./v. Schönfeld, M., Das Recht auf Datenübertragbarkeit - Ein datenschutzrechtliches Novum, ZD 358-362.

Keßler, O., Intelligente Roboter – neue Technologien im Einsatz. Voraussetzungen und Rechtsfolgen des Handelns informationstechnischer Systeme, MMR 2017, 589-594.

Kinast, K./Kühnl, C., Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten, NJW 2014, 3057-3062.

Krafft, T. D./Zweig, K. A., Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse – Ein Regelungsvorschlag aus sozioinformatischer Perspektive, Berlin 2019.

Kugelmann, D., Datenfinanzierte Internetangebote – Regelungs- und Schutzmechanismen der DSGVO, DuD 2016, 566-570.

Kühling, J./Buchner, B. (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 2. Aufl., München 2018 (zitiert: Bearbeiter, in: Kühling/Buchner, DSGVO/BDSG, 2018).

Kühling, J./Sackmann, F., Rechte an Daten, Berlin 2018.

Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg, Tätigkeitsbericht 2018, Datenschutz, Potsdam 2019.

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Unsere Freiheiten: Daten nützen – Daten schützen, Tätigkeitsbericht Datenschutz 2018, 34. Tätigkeitsbericht, Stuttgart 2019.

Lapp, T., Informations- und Auskunftspflichten von Anwaltskanzleien, NJW 2019, 345-348.

Maier, N./Bile, T., Die Zertifizierung nach der DSGVO, DuD 2019, 468-482.

Martin, N./Friedewald, M., Warum Unternehmen sich (nicht) an Recht und Gesetz halten, DuD 2019, Heft 8, 493-497.

Martini, M., Grundlinien eines Kontrollsystems für algorithmenbasierte Entscheidungsprozesse, Berlin 2019.

MPFS – Medienpädagogischer Forschungsverbund Südwest, KIM-Studie 2016, Kindheit, Internet, Medien 2016, https://www.mpfs.de/studien/kim-studie/2016/.

MPFS – Medienpädagogischer Forschungsverbund Südwest, JIM-Studie 2018, Jugend, Information, Medien 2018, 29. November 2018.

Nebel, M./Richter, P., Datenschutz bei Internetdiensten nach der DS-GVO - Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf, ZD 2014, 407-413.

Paal, B./Pauly, D., Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Beck'sche Kompakt-Kommentar, 2. Aufl., München 2018 (zitiert: Bearbeiter, in: Paal/Pauly).

Raith, N., Das vernetzte Automobil – im Konfliktzwischen Datenschutz und Beweisführung, Wiesbaden 2019.

Reding, V., Sieben Grundbausteine der europäischen Datenschutzreform, ZD 2012, 195-198.

Reibach, B., Private Dashcams & Co. – Household Exemption ade?, DuD 2015, 157-160.

Richter, P., Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, DuD 2015, 735-740.

Rose, E., Datenbrillen, Drohnen, Dashcams …, DuD 2017, 137-141.

Roßnagel, A., Quantifizierung der Persönlichkeit – aus grundrechtlicher und datenschutzrechtlicher Sicht, in: Baule, B./Hohnsträter, D./Krankenhagen, S./Lamla, J. (Hrsg.), Transformationen des Konsums – Vom industriellen Massenkonsum zum individualisierten Digitalkonsum, Baden-Baden, i.E.

Roßnagel, A., Innovationen der Datenschutz-Grundverordnung – Wer greift die Chancen zu besserem Datenschutz auf?, DuD 2019, 467-472.

Roßnagel, A., Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Baden-Baden 2018.

Roßnagel, A., Notwendige Schritte zu einem modernen Datenschutzrecht, in: Roßnagel, A./Friedewald, M./Hansen, M. (Hrsg.), Die Fortentwicklung des Datenschutzrechts, Berlin/Wiesbaden, 2018, 361-384.

Roßnagel, A., Umsetzung der Unionsregelungen zum Datenschutz – Erste Erfahrungen mit der Datenschutz-Grundverordnung aus rechtswissenschaftlicher Sicht, DuD 2018, 741-745.

Roßnagel, A., Europäische Datenschutz-Grundverordnung, Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, Baden-Baden 2017.

Roßnagel, A., Datenschutzgesetzgebung für öffentliche Interessen und das Arbeitsumfeld – Chancen für risikoadäquate Datenschutzregelungen?, DuD 2017, 290-294.

Roßnagel, A., Datenschutzaufsicht nach der Datenschutz-Grundverordnung, Wiesbaden 2017.

Roßnagel, A., Wie zukunftsfähig ist die Datenschutz-Grundverordnung? – Welche Antworten bietet sie für die neuen Herausforderungen des Datenschutzrechts?, DuD 2016, 561-565.

Roßnagel, A., Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD 2013, 562-567.

Roßnagel, A., Datenschutz in einem informatisierten Alltag, Berlin 2007.

Roßnagel, A., Globale Datennetze: Ohnmacht des Staates - Selbstschutz der Bürger. Thesen zur Änderung der Staatsaufgaben in einer „civil information society“, ZRP 1997, 26-30.

Roßnagel, A., Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin, Baden-Baden 1993.

Roßnagel, A./Friedewald, M./Hansen, M. (Hrsg.), Die Fortentwicklung des Datenschutzes, Wiesbaden 2018.

Roßnagel, A./Geminn, C./Jandt, S./Richter, P., Datenschutzrecht 2016 - „Smart genug für die Zukunft?“, Ubiquitous Computing und Big Data als Herausforderung des Datenschutzrechts, Band 4, Kassel 2016.

Roßnagel, A./Hornung, G. (Hrsg.), Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug, Wiesbaden 2019.

Roßnagel, A./Kroschwald, S., Was wird aus der Datenschutzgrundverordnung? - Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument, ZD 2014, 495-500.

Roßnagel, A./Nebel, M., (Verlorene) Selbstbestimmung im Datenmeer, DuD 2015, 455-459.

Roßnagel, A./Nebel, M./Richter, P., Was bleibt vom Europäischen Datenschutzrecht? - Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455-460.

Roßnagel, A./Pfitzmann, A./Garstka, H., Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2011.

Roßnagel, A./Richter, P./Nebel, M., Besserer Internetdatenschutz für Europa - Vorschläge zur Spezifizierung der DS-GVO, ZD 2013, 103-108.

Rost, M. C., Datenschutzsanktionen: scharfes Schwert oder Papiertiger?, Die deutsche Datenschutzaufsicht erstarkt durch ein neues Maßnahmen- und Sanktionsinstrumentarium, DuD 2019, 488-492.

Sachsen-Anhalt, XV. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz, LT-Drs. 7/4095, Magdeburg 2019.

Schantz, P., Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841-1847.

Schantz, P./Wolff, H. A., Datenschutzgrundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017 (zitiert: Bearbeiter, in: Schantz/Wolff).

Scheibel, L./Horn, M./Öksüz, A., Soziale Medien und die EU-Datenschutz-Grundverordnung, Teil II Recht auf Auskunft und Datenübertragbarkeit, hrsg. von Verbraucherzentrale NRW e.V., Düsseldorf 2018.

Schulz, W./Dreyer, S., Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme, Gütersloh 2018.

Schwartmann, R./Jaspers, A./Thüsing, G./Kugelmann, D. (Hrsg.), Datenschutz-Grundverordnung mit Bundesdatenschutzgesetz, München 2018 (zitiert: Bearbeiter, in: Schwartmann u.a.).

Schwenke, T., Schnittstellen zum „Cyborgspace“ – Erkenntnisse zu Datenbrillen nach Ende des „Google Glass“ – Experiments, DuD 2015, 161-166.

Simitis, S./Hornung, G./Spiecker gen. Döhmann, I. (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019 (zitiert: Bearbeiter, in: Simitis/Hornung/Spiecker gen. Döhmann).

Skistims, H., Smart Homes, Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Band 31, Baden-Baden 2016.

Solmecke, C./Kocatepe, S., Google Glass – Der Gläserne Mensch 2.0 - Die neueste technische Errungenschaft – ein Fluch oder eine Herausforderung? ZD 2014, 22-27.

Specht-Riemenschneider, L./Schneider, R., Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, 503-509.

Spindler, G., Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937-945.

Steidle, R., Multimedia-Assistenten im Betrieb – Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsvorschläge für mobile Agentensysteme, Wiesbaden 2005.

Stiftung Datenschutz (Hrsg.), Praktische Umsetzung des Rechts auf Datenübertragbarkeit – Rechtliche, technische und verbraucherbezogene Implikationen, 2017.

Stöber, M., Zulässigkeit und Grenzen der Videoüberwachung durch Private, NJW 2015, 3681-3685.

Strubel, M., Anwendungsbereich des Rechts auf Datenübertragbarkeit, ZD 2017, 355-361.

Sydow, G. (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, Baden-Baden 2017 (zitiert: Bearbeiter, in: Sydow).

Taeger, J./Gabel, D., DSGVO – BDSG, Kommentar, 3. Aufl., München 2019 (zitiert: Bearbeiter, in: Taeger/Gabel).

Tatsumi, T., „Angemessene" Datenschutzaufsicht in Japan? Kurze Diagnose der ersten Angemessenheitsfeststellung unter DSGVO, CR 2019, 424 - 429.

Uecker, P., Die Einwilligung im Datenschutzrecht und ihre Alternativen. Mögliche Lösungen für Unternehmen und Vereine, ZD 2019, 248-251.

Unabhängiges Datenschutzzentrum Saarland, 27. Tätigkeitsbericht 2017/2018, LT-Drs. 16/780, Saarbrücken 2019.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Tätigkeitsbericht 2019, 37. Tätigkeitsbericht, LT-Drs. 19/1430, Kiel 2019.

Veil, W., DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip, ZD 2015, 347-353.

Verbraucherzentrale Bundesverband (vzbv), Modernisierung des europäischen Datenschutzrechts, Berlin 2013.

Verbraucherzentrale Bundesverband (vzbv), Algorithmenbasierte Entscheidungsprozesse, Berlin 2013.

Verbraucherzentrale Bundesverband (vzbv), Die Europäischen Datenschutz-Grundverordnung, Berlin 2016.

Verbraucherzentrale Bundesverband (vzbv), Algorithmenkontrolle, Berlin 2019.

Verbraucherzentrale Bundesverband (vzbv), Für eine effektive Durchsetzung von Verbraucherrechten in der Plattformökonomie, Berlin 2019.

Weichert, T., Big Data und Datenschutz. Chancen und Risiken einer neuen Form der Datenanalyse, ZD 2013, 251-259.

Weichert, T., Verbraucherverbandsklage bei Datenschutzverstößen, Netzwerk Datenschutzexpertise, 20.3.2017.

Wendehorst, C./Graf v. Westphalen, F., Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, 3745-3750.

Westphal, M./Wichtermann, M., Datenportierung nach Art. 20 DS-GVO. Ausgewählte Ausschlussgründe, ZD 2019, 191-194.

Wybitul, T., Datenschutz-Grundverordnung im Unternehmen, Frankfurt 2016.

Wybitul, T., Anmerkung zu LAG Baden-Württemberg: Einsichtsrecht des Arbeitnehmers in die Personalakte, Urteil vom 20.12.2018, ZD 2019, 278-280.

Zikesch, P./Sörup, T., Der Auskunftsanspruch nach Art. 15 DS-GVO. Reichweite und Begrenzung, ZD 2019, 239-245.