verbraucherzentrale
Bundesverband

EVALUATION DER DSGVO AUS SICHT DER VERBRAUCHER

Positionen des vzbv

27. November 2019

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. DIE KERNFORDERUNGEN IM ÜBERBLICK

- Es muss klargestellt werden, dass die **Rechtsgrundlage der Einwilligung** nur alternativ zu den weiteren gesetzlichen Erlaubnistatbeständen genutzt werden darf.
- Die **Rechtsgrundlage „Vertragserfüllung“** muss dahingehend präzisiert werden, dass eine Datenverarbeitung für die Erfüllung eines Vertrags objektiv erforderlich sein muss, damit sie auf diesen Erlaubnistatbestand gestützt werden kann.
- Das besondere **Schutzbedürfnis von Kindern** muss stärker berücksichtigt werden, besonders im Hinblick auf Zweckänderungen, Datenverarbeitungen zu Werbezwecken und für die Profilbildung, Anforderungen an die Einwilligung in die Verarbeitung besonderer Kategorien von personenbezogenen Daten und in automatisierte Entscheidungen sowie den Datenschutz durch Systemgestaltung und Voreinstellung.
- **Informationen**, die Betroffenen zur Verfügung gestellt werden, sollten sich auf aktuell tatsächlich vorgesehene Datenverarbeitungen beziehen müssen. Im Rahmen eines Auskunftsersuchens sollten alle konkreten Empfänger benannt werden müssen, denen personenbezogene Daten des Betroffenen übermittelt wurden/werden.
- Es muss klargestellt werden, dass das **Recht auf Datenübertragung** alle Daten erfasst, die durch den Betroffenen verursacht wurden. Die Daten sollten dem Betroffenen in einem interoperablen Format zur Verfügung gestellt werden müssen.
- Die Regelungen zu **automatisierten Entscheidungen im Einzelfall** müssen ausgeweitet werden auf Entscheidungen, die automatisiert vorbereitet werden sowie auf alle Fälle, in denen Betroffene erheblich beeinträchtigt werden. Betroffenen sollten die zugrundeliegenden Daten sowie ihre Gewichtung im konkreten Fall offengelegt werden müssen. Außerdem sollten Verantwortliche den Betroffenen die Entscheidungsgründe für den Einzelfall erläutern müssen.
- Für die **Profilbildung** sollten u.a. absolute Grenzen definiert, Zulässigkeitsvoraussetzungen normiert und der Verhältnismäßigkeitsgrundsatz konkretisiert werden.
- Die Hersteller von Datenverarbeitungssystemen sollten als Adressaten der Regelungen zum **Datenschutz durch Systemgestaltung** mit aufgenommen werden
- Um die Zukunftsfähigkeit des Datenschutzrechts zu gewährleisten, ohne die DSGVO zu überfrachten, sind **weitere europäische Rechtsakte** erforderlich, wie beispielsweise ein Schutzkonzept und Standards für anonymisierte Daten, eine Verordnung für algorithmische Systeme sowie die Regulierung von „Personal Information Management Services“ (PIMS).

II. EINLEITUNG

Am 24. Mai 2016 trat nach mehr als vierjähriger Verhandlung die europäische Datenschutz-Grundverordnung[1] (DSGVO) in Kraft. Seit dem 25. Mai 2018 ist sie in allen EU-Mitgliedsstaaten – und teilweise auch darüber hinaus – unmittelbar anwendbar.

Zwar schreibt die DSGVO in weiten Teilen lediglich das vorherige Datenschutzrecht fort, dennoch gibt es zahlreiche Neuerungen, die für Verbraucherinnen und Verbraucher[2] – sowie für Unternehmen – einen echten Mehrwert darstellen, wie beispielsweise die Einführung des Marktortprinzips oder die Stärkung der Rechtsdurchsetzung.

Dennoch enthält die Verordnung auch schwache und höchst vage Bestimmungen, die dem Ziel der DSGVO nicht gerecht werden, das Recht auf Schutz personenbezogener Daten sicherzustellen. An vielen Stellen ist außerdem erkennbar, dass es sich bei dem finalen Text um einen politischen Kompromiss handelt, der nicht immer stringent ist.

Gemäß Art. 97 DSGVO ist die EU-Kommission angehalten, bis zum 25. Mai 2020 und danach alle vier Jahre dem Europäischen Parlament und dem Rat einen Evaluationsbericht vorzulegen, in dem sie die Anwendung und Wirkung der Verordnung überprüfen und bewerten soll. Außerdem soll die Kommission erforderlichenfalls geeignete Vorschläge zur Änderung der Verordnung machen.

Aus Sicht des Verbraucherzentrale Bundesverbands e.V. (vzbv) ist der frühe Zeitpunkt der Evaluation unglücklich gewählt. Auf der einen Seite ist die öffentliche Diskussion vor allem von Kritik und Klagen über Schwierigkeiten bei der Anwendung der DSGVO geprägt. Viele der Klagen sind berechtigt, andere jedoch nicht – in jedem Fall ist unvermeidbar, dass die praktische Umsetzung eines solch umfassenden Gesetzes erst einmal vor allem als Last wahrgenommen wird. Auf der anderen Seite benötigen beispielsweise Rechtsdurchsetzungsverfahren oft mehrere Jahre, sodass viele (positive) Auswirkungen der DSGVO für Verbraucher und Markt erst später zu Tage treten werden. Dementsprechend behutsam sollte bei der Evaluation vorgegangen werden.

Ungeachtet dessen führte der Marktwächter Digitale Welt des vzbv und der Verbraucherzentralen im Jahr 2018 zwei Untersuchungen durch, in der er die Konformität mit der DSGVO von acht sozialen Netzwerken prüfte. Im Fokus der Untersuchungen standen insbesondere die Fragen, wie die Anbieter ihren Informationspflichten nachkamen[3] und die Datenportabilität umsetzten.[4]

Um seinen Beitrag zum Evaluationsprozess zu leisten, hat der vzbv außerdem ein Rechtsgutachten in Auftrag gegeben, das eine Evaluation der DSGVO aus Verbrauchersicht vornehmen sollte. Das Gutachten wurde im Dezember 2019 veröffentlicht.[5]

---

[1] 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).

[2] Die gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

[3] Marktwächter Digitale Welt: Soziale Medien und die EU-Datenschutz-Grundverordnung (2018), URL: https://www.marktwaechter.de/sites/default/files/downloads/bericht_soziale_medien_dsgvo_i.pdf [Zugriff: 30.10.2019].

[4] Dass.: Soziale Medien und die EU-Datenschutzgrundverordnung - Teil 2 (2018), URL: https://www.marktwaechter.de/sites/default/files/downloads/bericht_soziale_medien_dsgvo_ii.pdf [Zugriff: 30.10.2019].

[5] Roßnagel, Alexander; Geminn, Christian: Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht. Gutachten im Auftrag des vzbv (2019).

Darüber hinaus wurde im Oktober 2019 der Endbericht der Datenethikkommission der Bundesregierung (DEK) vorgelegt, der auch Vorschläge zur Überarbeitung der DSGVO enthält.[6] Neben dem vzbv waren Vertreter der Industrie, Wissenschaft und Zivilgesellschaft als Mitglieder berufen. Durch diese paritätische Besetzung repräsentieren die von der DEK erarbeiteten und einstimmig verabschiedeten Handlungsempfehlungen einen breiten gesellschaftlichen Konsens.

Folgend werden die aus Verbrauchersicht wichtigsten Vorschläge zur Evaluation der DSGVO skizziert, die sich aus den vorgelegten Gutachten und teilweise aus dem Endbericht der DEK ergeben. Eine ausführliche Argumentation zu den einzelnen Punkten sowie weitere Vorschläge können den entsprechenden Gutachten entnommen werden.

III. DIE POSITIONEN IM EINZELNEN[7]

1. VERHÄLTNIS ZWISCHEN DER EINWILLIGUNG UND ANDEREN ERLAUBNISTATBESTÄNDEN

Um eine Datenverarbeitung zu rechtfertigen, müssen sich Verantwortliche auf einen Erlaubnistatbestand der DSGVO berufen. Es besteht jedoch Uneinigkeit darüber, ob eine Datenverarbeitung zu einem bestimmten Zweck parallel auf mehrere Erlaubnistatbestände gestützt werden kann.[8] Basiert jedoch die Verarbeitung auf der Rechtsgrundlage der Einwilligung, folgen daraus andere Pflichten für die Verantwortlichen und andere Rechte für die Betroffenen als bei den anderen Erlaubnistatbeständen. Stützt beispielsweise ein Verantwortlicher seine Datenverarbeitung auf eine Einwilligung und informiert den Betroffenen entsprechend, beruft sich jedoch später auf eine andere Rechtsgrundlage, hat er den Betroffenen über seine Rechte (hinsichtlich der Einwilligung) fehlinformiert und andere wichtige Informationen (hinsichtlich der anderen Rechtsgrundlage) vorenthalten. Daher „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“[9].

> Es muss klargestellt werden, dass die Einwilligung sowie die weiteren gesetzlichen Erlaubnistatbestände nur alternativ genutzt werden können und sich ein Verantwortlicher nicht auf mehrere Erlaubnistatbestände berufen kann.[10]

[6] Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission (2019), Berlin, URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf [Zugriff: 24.10.2019].

[7] Die Reihenfolge der Empfehlungen entspricht weitgehend der Abfolge der Artikel innerhalb der DSGVO und stellt keine Priorisierung der Vorschläge dar

[8] Vgl. Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 26ff.

[9] Ebd., S. 27.

[10] Vgl. Regelungsvorschlag zu Art. 6 Abs. 1 UAbs. 1 DSGVO ebd., S. 67.

2. BESTIMMUNG DES VERTRAGSZWECKS

Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn sie für die Erfüllung eines Vertrags erforderlich ist. Die vage Formulierung des Erlaubnistatbestands ermöglicht es jedoch Verantwortlichen, mit einer weiten Definition des Vertragszwecks eine umfassende Verarbeitung personenbezogener Daten zu legitimieren.[11] So formulieren Unternehmen beispielsweise auch Datenverarbeitungen zu Werbezwecken und entsprechende Profilbildungen als Vertragszweck. Dabei kann „die notwendige datenschutzrechtliche Eingrenzung des Erlaubnistatbestands des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO […] nicht allein durch die Kontrolle der Allgemeinen Geschäftsbedingungen (AGB) erreicht werden."[12] Daher muss die „funktional objektive Erforderlichkeit der Datenverarbeitung für den zentralen Vertragszweck entscheidend"[13] sein.

> Der Erlaubnistatbestand „Vertragserfüllung" muss dahingehend präzisiert werden, dass die Verarbeitung personenbezogener Daten für die Erfüllung eines Vertrags objektiv erforderlich sein muss, damit Verantwortliche deren Verarbeitung auf diesen Erlaubnistatbestand stützen können.[14]

3. SCHUTZ VON KINDERN

Auf Grund ihrer besonderen Schutzbedürftigkeit muss die Verarbeitung von Daten von Kindern besonderen Restriktionen unterliegen. Solche Restriktionen sind auch bereits in der DSGVO angelegt, greifen jedoch oftmals zu kurz. So sollte beispielsweise bei der Prüfung, ob die Verarbeitung zu einem anderen Zweck als demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, das besondere Schutzbedürfnis von Kindern besonders berücksichtigt werden.

> Um dem besonderen Schutzbedürfnis von Kindern gerecht zu werden, sollten im Falle einer Zweckänderung die möglichen Folgen der beabsichtigten Weiterverarbeitung auf Kinder besonders berücksichtigt werden müssen.[15]

Ein besonderes Augenmerk ist auf den Schutz von Kindern vor Profilbildung zu legen aufgrund der erhöhten Schutzwürdigkeit im Verhältnis zur Eingriffstiefe der Verarbeitung in die Persönlichkeitsrechte.[16] So sollte eine Verarbeitung von Daten von Kindern zu Werbezwecken oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen grundsätzlich ausgeschlossen sein und auch nicht durch Einwilligungen legitimiert werden können. Entsprechende Auslegungshilfen in den Erwägungsgründen sollten daher in den Normtext überführt werden.

---

[11] Vgl. ebd., S. 29ff.

[12] Ebd., S. 29.

[13] Ebd., S. 30.

[14] Vgl. Regelungsvorschlag zu Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO ebd., S. 67f.

[15] Vgl. Regelungsvorschlag zu Art. 6 Abs. 4 UAbs. 1 lit. d DSGVO ebd., S. 68.

[16] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 114.

> Es muss klargestellt werden, dass die Verarbeitung von personenbezogenen Daten von Kindern zu Werbezwecken oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen grundsätzlich ausgeschlossen ist.[17]

Darüber hinaus ist nicht nachvollziehbar, warum die DSGVO besondere Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft vorsieht, aber Einwilligungen von Kindern in die Verarbeitung besonderer Kategorien von personenbezogenen Daten oder in die Verarbeitung personenbezogener Daten zur automatisierten Entscheidung ohne Einschränkung möglich sind, obgleich solche Verarbeitungen ein großes Risiko für die Rechte und Freiheiten der betroffenen Kinder beinhalten. Daher sollte ausgeschlossen werden, dass Kinder selbst in solche Datenverarbeitungen einwilligen können.

> Es muss grundsätzlich ausgeschlossen werden, dass Kinder selbst in die Verarbeitung besonderer Kategorien von personenbezogenen Daten einwilligen können sowie dass Kinder selbst darin einwilligen können einer auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden.[18]

Einen wichtigen Baustein zum Schutz von Kindern stellt eine datenschutzgerechte Technikgestaltung sowie datenschutzfreundliche Voreinstellungen dar.[19] „Sie übernehmen – mehr noch als Erwachsene – die voreingestellten Werte und konzentrieren sich allein auf die Nutzung des Geräts oder des Dienstes.“[20]

> Es muss sichergestellt werden, dass die besondere Schutzbedürftigkeit von Kindern bei der datenschutzgerechten Systemgestaltung sowie bei datenschutzfreundlichen Voreinstellungen gebührend berücksichtigt wird.[21]

4. INFORMATION DER BETROFFENEN UND AUSKUNFTSRECHTE

Die Informationspflichten von Unternehmen sowie die Auskunftsrechte der Betroffenen sind an einigen Stellen der DSGVO unpräzise formuliert, was die Machtasymmetrie zwischen Unternehmen und Betroffenen verstärken kann. Problemtisch ist beispielsweise die Praxis, in Datenschutzerklärungen eine Vielzahl von künftig denkbaren oder nur vage beschriebenen Datenverarbeitungen aufzuführen.[22] Häufig werden lediglich Beispiele personenbezogener oder personenbeziehbarer Daten genannt, wobei nicht deutlich wird, ob diese Daten tatsächlich verarbeitet werden. Dabei werden Wendun-

[17] Vgl. Regelungsvorschlag zu Art. 8 Abs. 1 DSGVO in Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 68.

[18] Vgl. Regelungsvorschlag zu Art. 9 Abs. 2 lit. a DSGVO sowie Art. 22 Abs. 2 lit. c DSGVO ebd., S. 68f, S. 75f.

[19] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 115.

[20] Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 32.

[21] Vgl. Regelungsvorschlag zu Art. 25 Abs. 1 DSGVO sowie Art. 25 Abs. 2 DSGVO ebd., S. 77f.

[22] Vgl. ebd., S. 34f.

gen wie „zum Beispiel“, „möglicherweise“ oder „unter anderem“ genutzt. Dies führt insbesondere dazu, dass Verbraucher die Reichweite der Datenverarbeitung und ggfs. ihrer Einwilligung nur schwer abschätzen können.

> Es muss präzisiert werden, dass sich die Informationen, die dem Betroffenen zur Verfügung gestellt werden, auf aktuell tatsächlich vorgesehene Datenverarbeitungen beziehen müssen.[23]

Darüber hinaus werden Betroffenen im Rahmen ihrer Auskunftsrechte oft lediglich Kategorien von Empfängern genannt, gegenüber denen personenbezogene Daten offengelegt worden sind oder noch offengelegt werden.[24] Ohne die Benennung konkreter Empfänger ist es Verbrauchern jedoch nicht möglich, auch gegenüber diesen Empfängern ihre Rechte einzufordern.

> Es muss sichergestellt werden, dass der Verantwortliche dem Betroffenen alle ihm bekannten Empfänger benennen muss, denen personenbezogene Daten des Betroffenen übermittelt werden. Zu diesem Zweck sollten Verantwortliche außerdem die Übertragungen der Daten sowie die Empfänger protokollieren müssen.[25]

5. DATENPORTABILITÄT

Die Datenportabilität verfolgt zwei Ziele: Zum einen soll dieses Instrument den Wettbewerb stärken, indem Lock-in-Effekte verringert werden. Zum anderen soll Verbrauchern eine bessere Kontrolle sowie eine Art positives Verfügungsrecht über ihre Daten ermöglicht werden. Denn dadurch, dass Nutzer eines Dienstes die von ihnen bereitgestellten Daten in einem weiterverarbeitbaren Format erhalten können, erhalten sie auch gleichzeitig neue Möglichkeiten, die Daten für ihre eigenen Zwecke zu verarbeiten bzw. verarbeiten zu lassen.[26] „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.“[27] Dennoch ist umstritten, ob Art. 20 DSGVO lediglich Daten umfasst, die von den Betroffenen aktiv in einen Dienst eingestellt wurden oder auch solche, die von ihnen durch die Nutzung eines Dienstes oder eines Produktes generiert wurden.

---

[23] Vgl. Regelungsvorschlag zu Art. 12 Abs. 1 DSGVO sowie Art. 13 Abs. 1 und Abs. 2 DSGVO ebd., S. 69, S. 70.

[24] Marktwächter Digitale Welt (DMW) (2018) (wie Anm. 3), S. 16f.

[25] Vgl. Regelungsvorschläge zu Art. 15 Abs. 1 lit. c DSGVO sowie Art. 24. Abs. 1 DSGVO in Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 72, S. 77.

[26] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 135; Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), 41f

[27] Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 42.

> Es muss klargestellt werden, dass das Recht auf Datenübertragung alle Daten erfasst, die durch den Betroffenen verursacht wurden.[28]

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. „Die Anforderungen an ein „strukturiertes, gängiges und maschinenlesbares Format“ werden in der Praxis bislang noch sehr unterschiedlich und uneinheitlich ausgelegt, obwohl sie Grundvoraussetzung für eine wirkungsvolle Ausübung des Portabilitätsrechts sind.“[29] In einer Untersuchung von acht Diensten sozialer Medien hat der Marktwächter Digitale Welt die Ausübung des Rechts auf Datenübertragbarkeit getestet.[30] Zwar wurden Datensätze zur Verfügung gestellt, allerdings lagen diese nur in sehr unterschiedlichen Dateiformaten vor und waren mit Standardsoftware meist nicht zu öffnen. Die Daten waren für Verbraucher damit nicht überprüfbar. Kritisiert wurde, dass Verbraucher keine informierte Entscheidung darüber treffen können, ob die Daten zutreffend sind und welche Daten bei einem Wechsel zum neuen Anbieter übertragen werden sollen.

> Es muss festgelegt werden, dass dem Betroffenen die Daten in einem interoperablen Format zur Verfügung gestellt werden müssen. Der Europäischen Datenschutzausschuss sollte die Aufgabe erhalten, entsprechende Vorgaben für die Formate zu entwickeln.[31]

6. AUTOMATISIERTE EINZELFALLENTSCHEIDUNGEN[32]

Eine 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 Weise erheblich beeinträchtigt. Problematisch ist, dass der Anwendungsbereich auf Entscheidungen begrenzt ist, die „ausschließlich“ auf einer automatisierten Datenverarbeitung beruhen. Eine große Zahl algorithmischer Entscheidungsverfahren dürfte durch die Regelung nicht erfasst sein, was den grundrechtlichen Schutzpflichten des Gesetzgebers nicht gerecht wird.[33] „Das Schädigungspotential algorithmendeterminierter Entscheidungssysteme, die ursprünglich das Leitbild des Art. 22 DSGVO gebildet hatten, unterscheidet sich insbesondere nicht kategorial von demjenigen vieler algorithmengetriebe-

[28] Vgl. Regelungsvorschlag zu Art. 20 Abs. 1 DSGVO ebd., S. 72f.

[29] Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 136.

[30] Marktwächter Digitale Welt (DMW) (2018) (wie Anm. 4).

[31] Vgl. Regelungsvorschlag zu Art. 20 Abs. 1 DSGVO sowie Art. 70 Abs. 1 DSGVO in Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 73f, S. 80.

[32] Eine ausführliche Auseinandersetzung mit der Problematik der bzw. den Anforderungen an eine „Algorithmenkontrolle“ ist dem entsprechenden Positionspapier des vzbv zu entnehmen. Verbraucherzentrale Bundesverband: Algorithmenkontrolle (2019), URL: https://www.vzbv.de/sites/default/files/downloads/2019/05/02/19-05-02_vzbv_positionspapier_algorithmenkontrolle.pdf [Zugriff: 30.10.2019].

[33] Vgl. Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 45.

ner Entscheidungssysteme. Dafür ist auch die Neigung menschlicher Akteure, Empfehlungen algorithmischer Systeme schlicht zu übernehmen und bestehendes Ermessen nicht auszuüben, mitverantwortlich."[34]

> Der Regelungsgehalt des Art. 22 DSGVO muss daher ausgeweitet werden auf Entscheidungen, die automatisiert vorbereitet und von einem menschlichen Entscheider zumeist ungeprüft übernommen werden.[35]

Darüber hinaus ist der Anwendungsbereich des Art. 22 weiter eingeschränkt auf Fälle, in denen eine auf einer automatisierten Verarbeitung beruhende Entscheidung der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Doch: „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."[36]

> Art. 22 DSGVO muss daher alle Fälle erfassen, in denen Betroffene erheblich beeinträchtigt werden.[37]

Besonders im Kontext von automatisierten Einzelfallentscheidungen sind Auskunftsrechte für Verbraucher zentral, um die Entscheidungen nachvollziehen und individuell überprüfen zu können. Nur so können sie ihre in der DSGVO festgelegten Rechte wahrnehmen und beispielsweise eine Entscheidung anfechten. Wesentlich ist dabei, dass Verbraucher verständlich, relevant und konkret informiert werden. Die betroffene Person muss erfahren, welche Informationen und damit verbundenen Annahmen wesentlich und damit prägend für eine Entscheidung waren. „Nur so kann verhindert werden, dass sie als Persönlichkeit einem für sie unverständlichen algorithmenbasierten System unterworfen wird."[38] Aus diesen Gründen sollten Verbraucher darüber hinaus das Recht erhalten, dass ihnen auf Anfrage die Gründe einer automatisierten Entscheidung für ihren Einzelfall erläutert werden müssen.[39]

> Betroffene sollten das Recht erhalten, dass ihnen im Fall einer automatisierten Entscheidung die zugrundeliegenden Daten sowie ihre Gewichtung bei der Berechnung für den konkreten Fall in einer nachvollziehbaren Form offengelegt werden müssen.

---

[34] Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 192.

[35] Vgl. Regelungsvorschlag zu Art. 22 Abs. 1 DSGVO in Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 75ff.

[36] Ebd., S. 47.

[37] Vgl. Regelungsvorschlag zu Art. 22 Abs. 1 DSGVO ebd., S 75ff.

[38] Ebd., S. 36f.

[39] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 187.

> Außerdem sollten Betroffene das Recht erhalten, dass ihnen der Verantwortliche die Entscheidungsgründe für den Einzelfall erläutern muss.[40]

Ein großes Manko ist ferner, dass Art. 22 DSGVO keine Qualitätsanforderungen an automatisierte Entscheidungen festschreibt. Solche Qualitätsanforderungen sollten sicherstellen, dass Fehler und Risiken von automatisierten Entscheidungen reduziert werden und dass Verbraucher darauf vertrauen können, dass automatisierten Entscheidungen tatsächlich auf Basis valider Annahmen und Modelle getroffen werden.[41]

> Um sicherzustellen, dass die Ergebnisse der Entscheidungen rechtmäßig und korrekt sind, sollten materiell-rechtliche Verfahrensvorgaben festgeschrieben werden. Insbesondere sollten die für die Entscheidung genutzten Daten unter Zugrundelegung eines anerkannten mathematisch-statistischen Verfahrens verarbeitet werden und für die Entscheidungsfindung nachweislich erheblich sein.[42]

7. PROFILBILDUNG

Höchst problematisch ist, dass die Profilbildung zwar in der DSGVO definiert wird, ihre Risiken in der Verordnung jedoch nicht weiter geregelt werden. „Profiling von Verbrauchern ist jedoch immer ein starker Eingriff in deren Grundrechte, der über die normale Verarbeitung von personenbezogenen Daten hinausgeht. […] Daher bedarf die Datenschutz-Grundverordnung einer risikoadäquaten Regelung, die Datenschutz und Entscheidungsfreiheit schützt und Diskriminierung verhindert. 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“.[43]

> Auch die Profilbildung als solche (und nicht lediglich darauf basierende Entscheidungen) muss strenger geregelt werden. So sollten diesbezüglich u.a. absolute Grenzen definiert, Zulässigkeitsvoraussetzungen normiert und der Verhältnismäßigkeitsgrundsatz konkretisiert werden.[44]

Dementsprechend sollten sich „die mit Art. 22 DSGVO – „einschließlich Profiling“ – verbundenen Informationspflichten und Auskunftsrechte […] auch auf die automatisierte Profilbildung als solche beziehen“.[45] Alles andere würde der Intention der DSGVO nicht ausreichend Rechnung tragen.

---

[40] Vgl. Regelungsvorschläge zu Art. 15 Abs. 1 lit. h DSGVO sowie Art. 22 Abs. 3 DSGVO in Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 72, S, 75ff.

[41] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 190.

[42] Vgl. Regelungsvorschlag zu Art. 22 Abs. 4 in Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 75ff.

[43] Ebd., S. 49.

[44] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 99f.

[45] Ebd., S. 193.

Es sollte klargestellt werden, dass Betroffene stets informiert werden müssen, wenn Profiling durchgeführt wird und welche Folgen dies hat – selbst, wenn das Profiling keine rechtliche Wirkung für den Betroffenen entfaltet.[46]

8. DATENSCHUTZ DURCH SYSTEMGESTALTUNG UND VOREINSTELLUNG

Problematisch ist weiterhin, dass Regelungsadressat der DSGVO lediglich die datenverarbeitenden Stellen sind, nicht jedoch die Hersteller von Produkten und Software. Dabei sind es vor allem die Hersteller, die über Gestaltungsspielräume hinsichtlich der datenschutzkonformen Technikgestaltung der Produkte verfügen.[47] „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.“[48]

Die Hersteller von Datenverarbeitungssystemen sollten als Adressaten der Regelungen zum Datenschutz durch Systemgestaltung mit aufgenommen werden.[49]

9. KONKRETISIERUNGEN UND ERGÄNZUNGEN AUßERHALB DER DSGVO

Wie ihre Bezeichnung bereits andeutet, ist die DSGVO als Grundverordnung angelegt. Dies bedeutet, dass sie abstrakte Regelungen festlegt, die allerdings für unterschiedliche Bereiche konkretisiert und ergänzt werden sollten.[50] Ein Beispiel ist die ePrivacy-Verordnung für den besonders sensiblen Bereich der elektronischen Kommunikation, die derzeit in Brüssel verhandelt wird.

Um die Zukunftsfähigkeit des Datenschutzrechts weiterhin zu gewährleisten ohne dabei die DSGVO zu überfrachten, sind daher weitere europäische Rechtsakte erforderlich, wie beispielsweise

Schutzkonzepte für anonymisierte Daten: Durch gesetzgeberische Vorgaben und die Entwicklung von Standards sollten konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten definiert werden. Dies sollte um strafbewehrte Verbote der De-Anonymisierung ergänzt werden.[51]

---

[46] Vgl. Regelungsvorschläge zu Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO sowie Art. 15 Abs. 1 DSGVO in Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 70, S. 73.

[47] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 119f.

[48] Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 5), S. 51.

[49] Vgl. Regelungsvorschläge zu Art. 25 Abs. 1 DSGVO ebd., S. 77f.

[50] Vgl. ebd., S. 100ff.

[51] Vgl. ebd., S. 97f.; Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 129ff

Europäische Verordnung für algorithmische Systeme (EUVAS): Eine EUVAS sollte einem risikoadaptierten Regulierungsansatz folgen mit horizontalen Regeln zur Gestaltung und Zulässigkeit von algorithmenbasierten Entscheidungssystemen und Künstlicher Intelligenz, zu Betroffenenrechten, Transparenz, Aufsichtsinstitutionen und -strukturen, sowie technischen Vorgaben zur Absicherung der Rechtmäßigkeit der Systeme. Dies sollte durch sektorale Regeln weiter konkretisiert werden.[52]

Regulierung von „Personal Information Management Services" (PIMS): Wenngleich solche Systeme primär die Selbstbestimmung des Einzelnen stärken sollen, gehen von ihnen erhebliche Gefahren aus. Daher sollte ein gesetzlicher Rahmen vorgegeben werden, der Zulässigkeit und Grenzen regelt, Treuepflichten normiert, konfligierende Interessen ausschließt sowie entsprechende Kontroll- und Sanktionsmöglichkeiten schafft.[53]

[52] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 6), S. 180ff.

[53] Vgl. ebd., S. 133f.