Europäische Akademie für Informationsfreiheit und Datenschutz
Académie européenne pour la liberté d'information et la protection des données
European Academy for Freedom of Information and Data Protection
EAID

Berlin, den 27. Januar 2020

Evaluation der Datenschutz – Grundverordnung - Vorschläge zur Weiterentwicklung des Datenschutzrechts

Inhaltsverzeichnis

Europäische Akademie für Informationsfreiheit und Datenschutz e.V.
Vorstand: Peter Schaar * Dr. Alexander Dix * Karsten Neumann * Prof. Dr. Alfred Büllesbach * Dr. Dennis-Kenji Kipker
Geschäftsstelle: Bismarckallee 46/48 * D-14193 Berlin * Telefon: +49 151-62914576
E-Mail: gf@eaid-berlin.de * www.eaid-berlin.de
Vereinsregister-Nr. VR 21680 B Amtsgericht Charlottenburg * Steuer-Nr. 27/664/52926
IBAN DE84 1005 0000 0190 3076 92 * BIC BELADEBEXXX * Berliner Sparkasse

A. Generelle Bemerkungen

Art. 8 EU-Grundrechtecharta (EUGrCh) garantiert den Schutz personenbezogener Daten und schreibt eine unabhängige Datenschutzaufsicht vor. Mit der Datenschutz-Grundverordnung (DSGVO)[1] gibt es seit dem 25. Mai 2018 ein in allen Mitgliedstaaten direkt anwendbares EU-Datenschutzgesetz. Inwieweit die Ziele der DSGVO erreicht worden sind, lässt sich nach nur 18 Monaten noch nicht seriös bewerten. Die Europäische Kommission ist nach Art. 97 DSGVO gehalten, die Anwendung und Wirkungsweise der Verordnung laufend zu überprüfen und darüber erstmals am 25. Mai 2020 zu berichten und erforderlichenfalls Vorschläge zur Änderung und Weiterentwicklung der Verordnung vorzulegen.

Es ist nicht zu bestreiten, dass die DSGVO die Harmonisierung des europäischen Datenschutzrechts und seiner Anwendung gegenüber der weitgehend zersplitterten vorherigen Rechtslage vorangebracht hat. Auch wurden die Datenschutzrechte der von der Verarbeitung ihrer Daten betroffenen Personen gestärkt und die Datenschutzaufsichtsbehörden wurden mit wirksamen Mitteln zur Rechtsdurchsetzung ausgestattet. Indes hat sich gezeigt, dass es in den beschriebenen Bereichen weiterhin Defizite gibt, die der Abhilfe bedürfen.

Die DSGVO hat erhebliche Auswirkungen auf die weltweite Diskussion zu Fragen des Datenschutzes ausgelöst. Mehrere außereuropäische Länder und Bundesstaaten haben inzwischen Gesetze beschlossen, die sich am Vorbild der Grundverordnung orientieren. Zu nennen ist beispielsweise der am 1.Januar 2020 in Kraft getretene kalifornische Consumer Privacy Act (CCPA) und das neue thailändische Datenschutzgesetz. Dem US-Kongress liegen mehrere Entwürfe für Datenschutzgesetze und Gesetze zu damit zusammenhängenden Fragen vor oder werden gegenwärtig parteiübergreifend diskutiert. Zudem ist mit dem Anfang 2019 zwischen der Europäischen Union und Japan geschlossenen Datenschutzabkommen die weltweit größte Zone mit einem einheitlich hohen Datenschutzniveau entstanden. Damit haben sich die Chancen der europäischen Wirtschaft verbessert, auch angesichts der fortschreitenden Digitalisierung wettbewerbsfähig zu bleiben.

Die vorliegende Stellungnahme beruht auf den bisherigen Erfahrungen und hat insofern vorläufigen Charakter. Sie konzentriert sich auf zentrale Handlungsfelder, in denen bereits heute eine Weiterentwicklung des Rechtsrahmens angezeigt erscheint.

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rats 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) - EU Amtsblatt v. 4.5.2016, L119/1.

B. Vorschläge

1. Verbesserte Harmonisierung

Die Vielzahl der **Öffnungs- und Konkretisierungsklauseln in der DSGVO** bedarf dringend der Überprüfung mit dem Ziel ihrer Reduzierung. Dadurch, dass die Mitgliedsstaaten in sehr unterschiedlicher Weise von den nationalen Gestaltungsmöglichkeiten Gebrauch gemacht haben, besteht in vielen Bereichen weiterhin ein Regulierungspatchwork unterschiedlichster Bestimmungen. Damit wird das Ziel einer möglichst weitgehenden Harmonisierung des Datenschutzrechts in der EU und die damit verbundene Datenfreizügigkeit stark beeinträchtigt. Zudem verursacht Fragmentierung erhebliche praktische und juristische Probleme bei den Rechtsanwendern.

1.1. Die Öffnungsklauseln der DSGVO zur Verarbeitung durch öffentliche Stellen ermöglichen neben präzisierenden Regelungen im Recht der Mitgliedstaaten auch **Präzisierungen durch das Unionsrecht**. Die rechtlichen Anforderungen an derartige Regelungen, etwa in Art. 6 Abs. 3 DSGVO und Art. 9 Abs. 2 DSGVO sollten im Hinblick auf die **besondere Grundrechtsrelevanz staatlicher Datenverarbeitung** dahingehend konkretisiert werden, dass von den in der DSGVO vorgegebenen Garantien nur zugunsten der Betroffenen abgewichen werden darf. Zudem sollte beim Bestehen von europaweiten Bezügen der EU-Gesetzgeber stärker von seiner Präzisierungsbefugnis Gebrauch machen, um die Prinzipien der DSGVO in harmonisierter Weise bei öffentlichen Stellen weiterzuentwickeln.

1.2. Besonders gravierend ist die Regelungsvielfalt im **Forschungsbereich**. Die Anwendung der Bestimmungen über die wissenschaftliche Forschung hat gezeigt, dass eine stärker integrierte Regelung über die Verarbeitung zu wissenschaftlichen Zwecken, insbesondere für die grenzüberschreitende europäische Forschung, notwendig ist. Art. 89 DSGVO sollte entsprechend überarbeitet werden, um einen EU-weit gleichmäßiges hohes Datenschutzniveau zu gewährleisten.

1.3. Auch bei der Verarbeitung personenbezogener Daten im Beschäftigungskontext ist ein höherer Harmonisierungsgrad erforderlich. Die in Art. 88 DSGVO formulierten Anforderungen an den **Beschäftigtendatenschutz** sollten als verbindliche Vorgaben für die

Verarbeitung von Beschäftigtendaten und nicht bloß als Option für die nationalen Gesetzgeber gestaltet werden. Die weitere Konkretisierung der Vorgaben durch nationales Recht und durch Kollektivvereinbarungen sollte gleichwohl weiterhin möglich sein.

1.4. Angesichts der zunehmenden Bedeutung interaktiver, grenzüberschreitender Medien sind konkretere, für alle Mitgliedstaaten verbindliche Abwägungsmaßstäbe für das **Verhältnis von Datenschutz, Meinungs- und Informationsfreiheit** erforderlich. Art. 85 DSGVO ist entsprechend weiterzuentwickeln.

1.5. Die **Zusammenarbeit der Aufsichtsbehörden** ist für die einheitliche Anwendung des Datenschutzrechts von entscheidender Bedeutung. Die in Kap. VII. (Art. 60-78) DSGVO vorgegebenen Mechanismen zur Zusammenarbeit und Kohärenz müssen effektiver gestaltet werden. Rechtlicher Nachbesserungsbedarf besteht, soweit eine Aufsichtsbehörde in Fällen von grenzüberschreitender Bedeutung einen Beschluss gem. Art. 58 nicht trifft, hinauszögert oder von einer formellen Maßnahme gem. Art. 58 Abs. 2 DSGVO im Hinblick auf eine gütliche Streitbeilegung mit dem Unternehmen abzusehen beabsichtigt. Durch entsprechende Änderungen in Art. 64-66 DSGVO muss sichergestellt werden, dass auch für solche Fälle die Regelungen zum Kohärenzverfahren zur Anwendung kommen.

2. Profiling / Automatisierte Entscheidungen

Stärker ins Blickfeld genommen werden müssen Systeme, welche für den einzelnen Menschen oder für die Gesellschaft wichtige Entscheidungen selbst treffen oder solche vorbereiten. Von besonderer datenschutzrechtlicher Bedeutung ist dabei die Zusammenführung und Auswertung von Daten zum Zwecke der Bewertung von Personen (Profilbildung) und der Einsatz algorithmischer Entscheidungssysteme, etwa im Zusammenhang unter Verwendung „Künstlicher Intelligenz“ (KI).

2.1. Art. 22 DSGVO ist so anzupassen, dass **alle Fälle erfasst werden, in denen Betroffene erheblich beeinträchtigt** werden. Die Profilbildung muss als solche geregelt werden (und nicht lediglich darauf basierende Entscheidungen). Es sollte klargestellt werden, dass die Regeln für automatisierte Entscheidungen auch für solche Entscheidungen gelten, die wesentlich auf algorithmischen Systemen beruhen (**algorithmengestützte**

Entscheidungen). Diesbezüglich müssen absolute Grenzen definiert, Zulässigkeitsvoraussetzungen normiert und der Verhältnismäßigkeitsgrundsatz konkretisiert werden. Dabei ist den besonderen Anforderungen für die Verwendung von sensitiven Daten und für die Verwendung von Daten über Kinder Rechnung zu tragen.

2.2. Die **Transparenzanforderungen** in Art. 12ff für das Profiling und automatisierte Entscheidungen sind zu konkretisieren. Betroffene müssen **stets informiert** werden, wenn Profiling durchgeführt wird und welche Folgen dies hat. Im Fall algorithmischer und algorithmengestützter Entscheidungssysteme müssen die **zugrundeliegenden Daten sowie ihre Gewichtung** für den konkreten Fall in einer nachvollziehbaren Form **offengelegt** werden.

2.3. Im Hinblick auf die **Funktionsweise und Wirkungen algorithmischer und algorithmengestützter Entscheidungssysteme**, insb. zur Vermeidung von Diskriminierungseffekten sollten Mechanismen der Algorithmenkontrolle implementiert werden. Die in Art. 35 Abs. 7 DSGVO formulierten Anforderungen an die Datenschutzfolgenabschätzung sind entsprechend zu konkretisieren.

3. Technologischer Datenschutz

Neben dem geschriebenen Recht wird die Gewährleistung eines effektiven Datenschutzes maßgeblich durch die Gestaltung technischer Systeme bestimmt. Die Feststellung „Code is Law“ (Lessig) gilt angesichts immer leistungsfähigerer IT-Systeme und globaler Verarbeitungsprozesse mehr denn je. Umso wichtiger ist es, für eine datenschutzgerechte Gestaltung der technischen Systeme zu sorgen, insb. Im Hinblick auf die Beschränkung des Umfangs der verarbeiteten personenbezogenen Daten (Datenvermeidung, Datenminimierung). Die Anonymisierung und die Verwendung von Pseudonymen sind wirksame Techniken, mit denen sich Risiken für die Grundrechte und -freiheiten natürlicher Personen begrenzen lassen, ohne den durch die Datenverarbeitung bezweckten Erkenntnisgewinn zu unangemessen einzuschränken. Im Hinblick auf die hohe Innovationsgeschwindigkeit ist zu überprüfen, inwieweit die rechtlichen Vorgaben einen angemessenen Schutz gewährleisten.

3.1. Die **Zusammenarbeit der Aufsichtsbehörden** ist für die einheitliche Anwendung des Datenschutzrechts von entscheidender Bedeutung. Die in Kap. VII. (Art. 60-78) DSGVO vorgegebenen Mechanismen zur

Zusammenarbeit und Kohärenz müssen effektiver gestaltet werden. Rechtlicher Nachbesserungsbedarf besteht, soweit eine Aufsichtsbehörde in Fällen von grenzüberschreitender Bedeutung einen Beschluss gem. Art. 58 nicht trifft, hinauszögert oder von einer formellen Maßnahme gem. Art. 58 Abs. 2 DSGVO im Hinblick auf eine gütliche Streitbeilegung mit dem Unternehmen abzusehen beabsichtigt. Durch entsprechende Änderungen in Art. 64-66 DSGVO muss sichergestellt werden, dass auch für solche Fälle die Regelungen zum Kohärenzverfahren zur Anwendung kommen.

3.2. Die Vorgaben zum technologischen Datenschutz (Art. 25 DSGVO) sollten den besonderen Risiken Rechnung tragen, die von der Verwendung neuartiger Techniken und Geschäftsmodelle ausgehen (insb. **Künstliche Intelligenz, Data Mining, Plattformen**). Entsprechende Vorgaben zum Design solcher Systeme sollten durch den Europäischen Datenschutzausschuss konkretisiert werden.

3.3. Angesichts der schnellen technologischen Entwicklung sollten die Vorgaben zur **Anonymisierung und Pseudonymisierung** in Art. 25 DSGVO sowie an die Verwendung anonymisierter Daten konkretisiert werden. Dies sollte um strafbewehrte **Verbote der De-Anonymisierung** und der **unerlaubten Auflösung von Pseudonymen** ergänzt werden.

3.4. Die **Hersteller** von Hard- und Software **sollten stärker in die Verantwortung genommen werden,** etwa durch eine Erweiterung der Begriffsdefinition des Verantwortlichen um die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Dateisysteme oder Dienstleistungen zur Verarbeitung personenbezogener Daten in Verkehr bringt. Zumindest sollten sie als Adressaten der Regelungen zum Datenschutz durch Technikgestaltung und durch datenschutzgerechte Voreinstellungen, Art. 25, und Sicherheit der Verarbeitung, Art. 32 DSGVO, zusätzlich zum Verantwortlichen und Auftragsverarbeiter mit der Folge aufgenommen werden, dass Anbieter von Systemen und Diensten zur Verarbeitung personenbezogener Daten für die Umsetzung der Anforderungen zum Zeitpunkt des In-Verkehr-Bringens verantwortlich und haftbar sind. Sie sind insbesondere gesetzlich zu verpflichten, ungeachtet von Betriebs- und Geschäftsgeheimnissen alle für eine Datenschutzfolgenabschätzung erforderlichen Informationen bereits vor Vertragsschluss und alle zur Umsetzung der Betroffenenrechte erforderlichen Informationen und Mittel zur Verfügung zu stellen. Damit könnten auch die Regelungen zur Zertifizierung nach Art. 42 wirksam

gemacht werden. Es ist zudem zu erwägen, die Regelungen auf Haftung und Schadensersatz (Art. 82 DSGVO) und zu den Sanktionen (Art. 83 f) auf Hersteller zu erstrecken.

4. Betroffenenrechte / Selbstbestimmung

Die Selbstbestimmung und die Rechte der von der Verarbeitung betroffenen Personen stehen im Mittelpunkt des Grundrechts auf Datenschutz und des vom Bundesverfassungsgericht festgestellten Grundrechts auf informationelle Selbstbestimmung. Obwohl die DSGVO die zentralen Einwirkungsmöglichkeiten des Einzelnen auf die Verarbeitung seiner Daten und seine Rechte gegenüber den Verantwortlichen normiert, sind die tatsächlichen Einwirkungsmöglichkeiten der Betroffenen vielfach sehr begrenzt. Dies gilt insbesondere für die Praxis verschiedener marktmächtiger Unternehmen, die Dienste anbieten, in denen Betroffene durch Lock-in-Effekte gefangen sind. Deshalb sollten die Betroffenenrechte weiter gestärkt werden.

4.1. Die Regelungen zur Einwilligung (Art. 7 DSGVO) und zum Widerspruchsrecht (Art. 21 DSGVO) sind dahingehend zu ergänzen, dass die betroffenen Personen sich zur Wahrnehmung ihrer Entscheidungsbefugnisse technischer Systeme bedienen können, um ihre datenschutzrechtlichen Präferenzen festzulegen. Die Verantwortlichen müssen verpflichtet werden, diese Festlegungen und darauf basierende Entscheidungen zu respektieren.

4.2. In Art. 12 ff DSGVO ist sicherzustellen, dass sich die Informationen, die dem Betroffenen zur Verfügung gestellt werden, auf **tatsächlich vorgesehene Datenverarbeitungen** beziehen. Zudem sollte klargestellt werden, dass der Verantwortliche dem Betroffenen alle ihm bekannten **Empfänger benennen** muss, denen personenbezogene Daten des Betroffenen übermittelt werden bzw. wurden. Zudem muss der Verantwortliche verpflichtet werden, die Übermittlung der Daten sowie die Empfänger zu protokollieren, damit er sich nicht unter Berufung auf „Nichtwissen“ seiner Informationsverpflichtung entziehen kann.

4.3. Die **Transparenzpflichten** gem. Art. 12 ff sind hinsichtlich der Verwendung von Profilingtechniken und algorithmischer Entscheidungsverfahren zu konkretisieren (vgl. oben Ziff. 1, 2. Anstrich).

4.4. Das Recht auf **Einschränkung der Verarbeitung** (Sperrung) in Art. 18 DSGVO sollte auf die Fälle erstreckt werden, in denen die an sich gebotene Löschung unterbleibt, weil die Daten lediglich zur Einhaltung von Aufbewahrungsfristen vorgehalten werden müssen.

4.5. Das **Recht auf Datenübertragbarkeit** (Art. 20 DSGVO) sollte so konkretisiert werden, dass dem Betroffenen die Daten in einem **interoperablen Format** zur Verfügung gestellt werden müssen. Zudem sollte sichergestellt werden, dass das Recht sämtliche automatisiert verarbeitete Daten umfasst, welche der Betroffene verursacht hat (also auch **Metadaten**) und nicht nur auf solche, die er bewusst in ein System eingegeben hat. Ferner sollten Unternehmen und Plattformen mit starker Marktdurchdringung dazu verpflichtet werden, ihre Angebote interoperabel zu gestalten, indem sie **Schnittstellen mit offenen Standards** zur Verfügung stellen.

C. Evaluation des Rechtsrahmens

Bisher sieht Art. 97 Abs- 1 DS-GVO eine Evaluation der Grundverordnung nach dem 25. Mai 2020 jeweils im Abstand von vier Jahren vor. Angesichts der rasanten technischen Entwicklung im Bereich der Datenverarbeitung erscheint es notwendig, diesen Evaluationsrhythmus auf zwei Jahre zu verkürzen. Auch wenn der Rechtsrahmen technikneutral gestaltet ist, muss er möglichst zeitnah auf technische Entwicklungen reagieren, wenn er nicht schnell obsolet werden soll.