Das ist die deutsche Übersetzung der englischen Stellungnahme, die die Digitale Gesellschaft am 29.04.2020 zusammen mit der Verbraucherzentrale Bundesverband zur Konsultation anlässlich des Berichts über die Bewertung und Überprüfung der Datenschutz-Grundverordnung (DSGVO) gemäß Artikel 97 DSGVO bei der Europäischen Kommission eingereicht hat.

Europäische Kommission
Didier Reynders
Justizkommissar

Berlin, 29. April 2020

Verbesserung der DSGVO zum Schutz unserer Grundrechte: Empfehlungen der Digitalen Gesellschaft und des Verbraucherzentrale Bundesverbands (vzbv)

Sehr geehrter Justizkommissar Didier Reynders,

die Datenschutz-Grundverordnung (DSGVO) hat das Bewusstsein für den Datenschutz enorm gestärkt. Sie hat dafür gesorgt, dass Organisationen ihre Datenverarbeitung besser organisieren. Nicht zuletzt hat die DSGVO dazu beigetragen, eine wirksamere Datenschutzaufsicht mit weitreichenderen Befugnissen aufzubauen. Dennoch ist die DSGVO bei weitem nicht perfekt. Ihre Schwachpunkte können und sollten durch die bessere Anwendung und ergänzende Gesetzgebung behoben werden. Mit der folgenden Stellungnahme wollen wir einige Aspekte hervorheben, die wir dahingehend für besonders relevant halten.

Die Umsetzung der DSGVO ist immer noch mangelhaft. Unternehmen und Technologiehersteller, die unsere digitalen Infrastrukturen betreiben, verletzen weiterhin unsere Grundrechte und -freiheiten.

Journalistische Angebote, Gesundheitsseiten und sogar einige Seiten, die auf Kinder zielen, gefährden unsere Grundrechte, indem sie personenbezogene Daten mit einer Vielzahl von Tracking-Unternehmen teilen, um dann individuelle Profile über jeden Einzelnen von uns zu erstellen.

Die zunehmenden Auswirkungen automatisierter Entscheidungssysteme, insbesondere auf Grundlage so genannter „künstlichen Intelligenz“, entziehen sich trotz der Regelungen der DSGVO individueller und gesellschaftlicher Kontrolle.

Anknüpfend an die Hinweise aus Datenschutzbehörden und Forschung schlagen wir die folgenden acht Empfehlungen zur Verbesserung der DSGVO aus der Perspektive der Zivilgesellschaft vor:

1. Bereitstellung von Symbolen für Datenschutzinformationen (Privacy Icons)
2. Schließung der Lücken bei automatisierten Entscheidungen im Einzelfall
3. Spezifizierung der Regeln für das Profiling
4. Regulierung von Web Tracking
5. Regulierung von Datenhändlern
6. Datenschutzverantwortung für Digitalunternehmen und Technologiehersteller
7. Automatisierung des Datenschutzes
8. Über die DSGVO hinausgehen

1. Bereitstellung von Symbolen für Datenschutzinformationen (Privacy Icons)

Die DSGVO sieht mehr Transparenz bei der Datenverarbeitung durch standardisierte Bildsymbole vor (Artikel 12 Absatz 8 und Erwägungsgrund 166). Die Europäische Kommission muss ihre Befugnis zum delegierten Rechtsakt an dieser Stelle nutzen, um die Stellung der Bürgerinnen und Bürger in der Datenwirtschaft durch EU-weit harmonisierte Datenschutz-Piktogramme zu stärken. Dabei sollte sie dem risikobasierten Ansatz der DSGVO Rechnung tragen, indem sie nicht nur Bildsymbole für verschiedene Arten von Daten und Verarbeitungszwecke einführt, sondern auch für die spezifischen Risiken für die Grundrechte und Grundfreiheiten der Betroffenen.

2. Schließung der Lücken bei automatisierten Entscheidungen im Einzelfall

Artikel 22 der DSGVO legt ein generelles Verbot von Entscheidungen fest, die ausschließlich auf einer automatisierten Verarbeitung beruhen, wenn diese Entscheidung der betroffenen Person gegenüber „rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“. Die Bestimmungen von Artikel 22 sind jedoch anfällig für Auslegungen, die ihren Anwendungsbereich unrechtmäßig einschränken. Gleichzeitig wird die Anwendung der automatisierten Entscheidungsfindung immer relevanter. Wir empfehlen, dass der Europäische Datenschutzausschuss die drängendsten Probleme von Artikel 22 angeht, indem er weitere Leitlinien zur automatisierten Entscheidungsfindung gemäß Artikel 70 Absatz 1 Buchstabe d herausgibt.

Es gibt reichlich Klärungsbedarf: Erstens darf das Wort „ausschließlich“ in Absatz 1 nicht so ausgelegt werden, dass ein rein formaler menschlicher Eingriff die Anwendung von Artikel 22 behindert.
Zweitens stellt das Wort „in ähnlicher Weise“ in Absatz 1 eine weitere potenzielle Hintertür dar. Welche automatisierten Entscheidungen „rechtliche Wirkung“ entfalten oder die Betroffenen „in ähnlicher Weise erheblich beeinträchtigen“ muss klargestellt werden. Einschlägige Beispiele hierfür sind die automatische Regulierung von Inhalten („Uploadfilter“) sowie gezielte Werbung. Drittens erlaubt die pauschale Ausnahme von Fällen, in denen die automatisierte Entscheidungsfindung „für den Abschluss oder die Erfüllung eines Vertrages zwischen der betreffenden Person und dem Verantwortlichen erforderlich ist“ in Absatz 2 diskriminierende Praktiken. Diese können die Menschen z.B. von Diensten der Informationsgesellschaft oder anderen wesentlichen Produkten und Dienstleistungen ausschließen. Der Europäische Datenschutzausschuss muss legitime Standardfälle für automatisierte Entscheidungsfindungen im Zusammenhang mit Verträgen empfehlen. Für alle anderen Anwendungsfälle sollten die Verantwortlichen eine Datenschutzfolgenabschätzung gemäß Artikel 35

Absatz 4 und eine vorherige Konsultation gemäß Artikel 36 der DSGVO durchführen müssen.

3. Spezifizierung der Regeln für das Profiling

Profiling umfasst eine große Zahl unterschiedlicher Fälle – von einfachen Kundendatenbanken mit Namen und Adressen bis hin zu Systemen, die detailliert und sekundengenau das Nutzerverhalten verarbeiten. Zur Regulierung von Profiling bedarf es zum einen eines nuancierteren Ansatzes. Zum anderen brauchen wir eine gesellschaftliche Diskussion über die Grenzen des Profilings.

Zunächst einmal aber müssen die gemäß der DSGVO Verantwortlichen für die Erstellung von Profilen zur Rechenschaft verpflichtet werden, auch wenn diese Profile nicht zu einer automatisierten Entscheidung führen. Das gilt insbesondere dann, wenn diese personenbezogene Daten in großem Umfang enthalten. Der Europäische Datenschutzausschuss muss verschiedene Fälle von Profiling nach ihren Risiken für die Rechte und Freiheiten der Betroffenen klassifizieren und für diese geeignete technische und organisatorische Maßnahmen empfehlen.

4. Regulierung von Web Tracking

Jede Nutzung des Internets erinnert daran, dass die DSGVO nicht wie beabsichtigt funktioniert. Die meisten Menschen können die Daten, die über ihr Online-Verhalten gesammelt werden, nicht kontrollieren. Jeder weiß, dass Google und Facebook in der verhaltensbasierten Werbung eine große Rolle spielen. Jedoch werden Daten über das Online-Verhalten der Menschen auch von einer Vielzahl anderer Unternehmen gesammelt und ausgetauscht, von denen die meisten Menschen noch nie etwas gehört haben. Das hat abschreckende Auswirkungen („Chilling Effects“) auf die Meinungs- und Informationsfreiheit, da sich die Menschen nie sicher sein können, wo die Informationen über ihr Online-Verhalten und ihre Lesegewohnheiten landen werden.

Um dieses Problem zu lösen, muss die zur Regulierung von Tracking einschlägige Novelle der ePrivacy-Verordnung verabschiedet werden. Schließlich war die ePrivacy-Verordnung immer als Ergänzung der DSGVO für den Bereich der elektronischen Kommunikation gedacht. Zudem ist der technische Standard „Do Not Track“ nach wie vor ein interessanter Ansatz. Allerdings muss „Do Not Track“ rechtsverbindlich werden, um Wirkung zu entfalten.

Insbesondere muss das sogenannte Real-time Bidding, also die Echtzeit-Versteigerung von Werbeplätzen auf Basis von Nutzerprofilen, in der Online-Werbung reguliert werden. Die Nutzenden müssen die Möglichkeit haben, die unbegrenzte Datenweitergabe über ihr Online-Verhalten, die jedes Mal ausgelöst wird, wenn eine Online-Werbung in ihrem Browser angezeigt wird, zu verstehen und zu deaktivieren. Die Anbieter von Webseiten müssen als gemeinsam Verantwortliche zur Rechenschaft verpflichtet werden, wenn sie es

Dritten ermöglichen, auf ihren Angeboten Daten zu sammeln. Wenn beides sich in der Praxis als unmöglich erweist, muss Real-time Bidding untersagt werden.

5. Regulierung von Datenhändlern

Ohne öffentliche Kontrolle ist in den letzten Jahren ein milliardenschwerer Datenhandel entstanden. Spezialisierte Unternehmen sammeln Daten über Personen aus allen möglichen Quellen – von Browserdaten bis zum Einkaufsverhalten – und kombinieren diese Daten in individuellen Profilen, um sie an andere Unternehmen zu vermarkten. Weder Einzelpersonen noch Datenschutzbehörden haben einen ausreichenden Einblick in diese Praktiken. Die DSGVO sieht hierfür keine spezifische Regelung vor. Aus Sicht der DSGVO ist der Handel mit Personendaten eine Verarbeitung wie jede andere. Auch die Digitale-Inhalte-Richtlinie (EU 2019/770) geht nicht auf Datenhandel ein.

Wir empfehlen, die DSGVO durch eine spezifische Regelung für den Handel mit personenbezogenen Daten zu ergänzen. Personenbezogene Daten dürfen grundsätzlich nicht gehandelt werden, sondern nur in streng begrenzten, gesellschaftlich akzeptablen Fällen.

6. Datenschutzverantwortung für Digitalunternehmen und Technologiehersteller

Auf dem europäischen Markt fehlen Technologien zum Datenschutz noch weitgehend. Digitalunternehmen und Technologiehersteller müssen verpflichtet werden, den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25) sowie die Sicherheit der Verarbeitung (Artikel 32) in ihre Systeme zu implementieren. Nur so können die Betroffenen geschützt werden und die Verantwortlichen und Auftragsverarbeiter ihren Datenschutzverpflichtungen nachkommen. Darüber hinaus sind es häufig die Digitalunternehmen und Technologiehersteller, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmen. Gemäß der DSGVO sind sie dann auch Verantwortliche.

Wir empfehlen, dass der Europäische Datenschutzausschuss Richtlinien verabschiedet, unter welchen Bedingungen und in welchen Fällen Digitalunternehmen und Technologiehersteller als für die Verarbeitung Verantwortliche gemäß Artikel 4 Nummer 7 DSGVO anzusehen sind.

7. Automatisierung des Datenschutzes

Die Umsetzung des Datenschutzes erfolgt noch immer weitgehend manuell und mittels willkürlicher und inkompatibler Formate und Systeme. Der Europäische Gesetzgeber muss die Entwicklung auffindbarer, zugänglicher, interoperabler und

wiederverwendbarer Standards unterstützen, die helfen, Datenschutzanforderungen in die Praxis umzusetzen. Dazu gehören Standards für Datenschutz-Folgenabschätzungen (Artikel 35), für den Datenschutz durch Technik und Voreinstellungen (Artikel 25), zur Information der Betroffenen (Artikel 12-14) sowie zur Ausübung der Betroffenenrechte (Artikel 15-18, 20-21). Darüber hinaus muss der Gesetzgeber die Entwicklung von Standards und Schnittstellen für die Maschine-zu-Maschine-Kommunikation zwischen den betroffenen Personen, den Verantwortlichen und den Datenschutzbehörden fördern. Zur Förderung der Transparenz muss der Gesetzgeber die Verantwortlichen verpflichten, ihre Verzeichnisse über die Verarbeitungstätigkeiten (Artikel 30) in maschinenlesbarer Form zu veröffentlichen. Um den Datenschutz in der Praxis zu stärken, muss der Gesetzgeber die Entwicklung und Implementierung von freien und quelloffenen Datenschutz-Management-Tools für alle Beteiligten unterstützen.

8. Über die DSGVO hinausgehen

Es gibt gute Gründe, unsere Abhängigkeit von digitalen Infrastrukturen internationaler Unternehmen, die zunehmende Monopolisierung und Zentralisierung von Diensten der Informationsgesellschaft und die Macht der großen Digitalunternehmen zur Beeinflussung des gesellschaftlichen Diskurses in Frage zu stellen. Die DSGVO ist jedoch kein ausreichendes Instrument, um all diese Probleme zu lösen. Erfolgsversprechender hierfür sind spezifische Regulierungsansätze, z.B. im Bereich des öffentlichen Beschaffungswesens, des Wettbewerbsrechts oder der Medienregulierung.

Mit freundlichen Grüßen

DIGITALE GESELLSCHAFT

verbraucherzentrale
Bundesverband