Aufgewertet

Die DSGVO bringt den Bürgern neue Rechte

Die Verbraucher sind die großen Gewinner des neuen europäischen Datenschutzes. Er stärkt ihre Rechte – auch durch neue Regelungen – und vereinheitlicht die Gesetzgebung im europäischen Binnenmarkt.

Von Joerg Heidrich

Das Juristen-Kauderwelsch soll weg: Artikel 12 der europäischen Datenschutzgrundverordnung (DSGVO) verpflichtet Unternehmen, Nutzer über die Verarbeitung ihrer Daten „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ über ihre Rechte zu informieren. Dabei sollen „gegebenenfalls zusätzlich visuelle Elemente“ zum Einsatz kommen, wenngleich die DSGVO nicht näher darauf eingeht, was in diesem Zusammenhang „gegebenenfalls“ heißt und wie die „visuellen Elemente“ auszusehen haben.

Die Intention des Gesetzgebers ist aber dennoch unmissverständlich: Verbraucher sollen einfacher verstehen können als bisher, was mit ihren Daten geschieht. Kein Unternehmen soll mehr hinter juristischen Formeln verstecken, welchen Schmu es mit den Daten seiner Nutzer betreibt. Dies gilt insbesondere für komplizierte Sachverhalte, „wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik“ es den Kunden schwermache zu erkennen, was mit ihren persönlichen Daten passiert.

Das Gesetz an sich ist in alles anderer als einfacher Sprache geschrieben. Artikel 32 Absatz 1 zum Beispiel ist ein Monstersatz mit mehr als 900 Zeichen. Verständlicher formuliert als die trockenen juristischen Artikel der DSGVO sind die sogenannten Erwägungsgründe, die helfen sollen, die Artikel richtig zu interpretieren. Erwägungsgrund 58 etwa nennt als Beispiel für das Transparenzgebot explizit „Werbung im Internet“. Website-Betreiber sind in Zukunft also noch mehr gefordert

zu erklären, wie Werbung auf ihren Seiten funktioniert.

So lobenswert der Versuch ist, den Anbietern eine verständliche Sprache vorzuschreiben: Das hat man auch in der Vergangenheit erfolglos probiert. Und es stellt sich die Frage, ob den Verbrauchern mit einer klaren, aber in Zukunft zig Seiten langen Datenschutzerklärung wirklich geholfen ist.

Auskunfts- und Löschrechte

Bürger stehen dank der DSGVO mehr Mittel als bisher zur Verfügung, um zu erfahren, welche Daten Unternehmen über sie speichern, und um diese löschen zu lassen. Alle bisherigen Rechte der Verbraucher und Pflichten der Unternehmen bleiben dabei erhalten. Unternehmen müssen also wie bisher über gespeicherte Daten informieren und auf Nachfrage über deren Weitergabe berichten.

Erwägungsgrund 63 geht zum Auskunftsrecht weiter ins Detail. So müssen Unternehmen auf Nachfrage belegen, „zu welchen Zwecken die personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind." Außerdem müssen sie erklären können, nach welcher Logik sie Profiling betreiben und welche Folgen das Profiling haben kann.

Als Profiling wiederum bezeichnet Erwägungsgrund 71 jegliche „Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte" einer Person, „soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt". Das gilt insbesondere, wenn dies der „Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche[n] Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel" dient.

Ihre Bank will Ihnen einen Kredit nur zu sehr schlechten Bedingungen geben? In Zukunft können Sie nachfragen, auf Basis welcher Berechnungen das Angebot zustande kam – zumindest in der Theorie. Allzu tiefgreifende Einblicke sollten Sie sich aber auch zukünftig nicht erhoffen – im Zweifelsfall werden sich Unternehmen auf den Schutz von Geschäftsgeheimnissen berufen, um ihre Karten nicht zu detailliert offenlegen zu müssen.

Ein Unternehmen kann einen Verbraucher schriftlich oder elektronisch über dessen Daten informieren, wobei es eine Kopie des Datensatzes zur Verfügung stellen muss. Besonders verbraucherfreundlich: Erwägungsgrund 63 sieht einen Fernzugriff vor. Sie sollten also zukünftig relativ einfach ein Backup aller ihrer bei Unternehmen lagernden persönlichen Daten ziehen können.

Der Fernzugang muss wie alle anderen Kommunikationswege „angemessene Sicherheitsanforderungen" erfüllen und sicherstellen, dass die zu beauskunftenden Daten nicht an unbefugte Dritte gelangen. Sollte ein Unternehmen begründete Zweifel an der Identität eines Auskunftssuchenden haben, kann es zusätzliche Nachweise verlangen, bei einem elektronischen Auskunftsantrag zum Beispiel eine Postadresse oder eine Bestellnummer.

Ein Unternehmen muss persönliche Informationen löschen, sobald der Zweck weggefallen ist, für den es sie ursprünglich erhoben hat. Vorher darf es das allerdings nicht. Ein typisches Beispiel: Kundendaten, die es bei einem Kauf erfasst hat, muss es löschen, wenn die steuerrechtlichen Pflichten zur Aufbewahrung enden, aber nicht vorher.

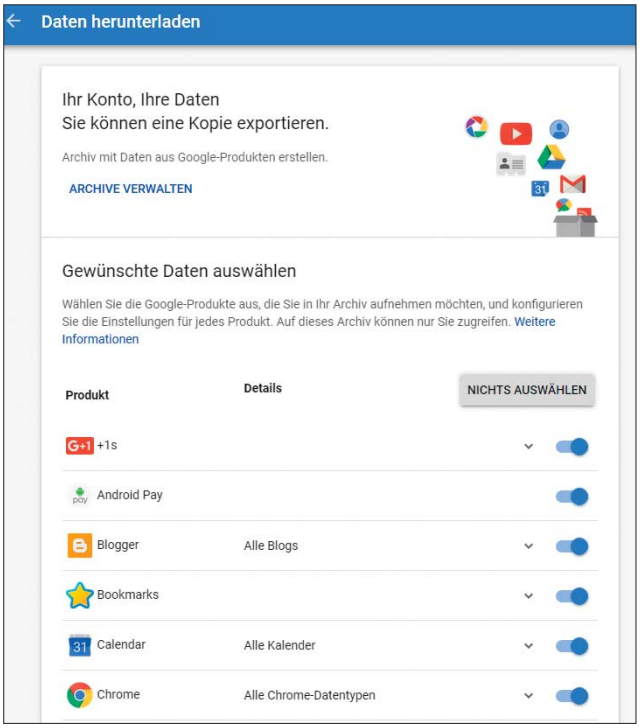
Der freundliche Folterfragebogen

Sie können aktiv darauf hinwirken, dass ein Unternehmen Ihre Daten löscht. Ein Recht auf das Löschen besteht zum Beispiel, wenn Sie eine Einwilligung zur Speicherung widerrufen – etwa bei Daten, die ein Unternehmen für einen Newsletter oder ein Preisausschreiben erhoben hat.

Unternehmen sollen Auskünfte unverzüglich erteilen und Daten ebenso unverzüglich löschen. Laut Artikel 12 bedeutet das innerhalb eines Monats nach Eingang des Antrags. Diese Frist kann das Unternehmen in komplexen Fällen um zwei Monate verlängern. Dann muss es allerdings den Verbraucher darüber informieren sowie über die Gründe der Verlängerung.

Damit Sie Ihre Ansprüche gegen die ungewollte Speicherung Ihrer Daten durchsetzen können, haben wir eine Vorlage entwickelt, mit der Sie Auskunfts- und Löschansprüche geltend machen können. Eine bekannte Vorlage hinsichtlich der Ansprüche aus dem alten Bundesdatenschutzgesetz gab es bislang bereits unter dem Titel „T5F – Thoms Fassung von Framstags freundlichem Folterfragebogen".

Um diese seit 2001 im Netz erhältliche Vorgabe zu ehren, haben wir unser Dokument „ct5F" genannt – „Die c't-Fassung von Framstags freundlichem Folterfragebogen". Unsere Vorlage steht zum Download und zur nichtkommerziellen Nutzung frei zur Verfügung. Unseriöse Versender oder Spammer benutzen Ihre Adresse? Foltern Sie sie! Unter ct.de/ycyu finden Sie als Beispiel auch eine Antwort,



Bei Google Takeout können Nutzer ihre persönlichen Daten und Arbeitsdaten per Web-Frontend herunterladen – einen Umzug der persönlichen Daten zu einem anderen Anbieter sieht das Werkzeug nicht vor.

die Sie erhalten, wenn Sie den Folterfragebogen an Heise senden.

Recht auf Vergessenwerden

Mit dem in den Artikeln 17 und 19 geregelten „Recht auf Vergessenwerden“ betreten die EU-Gesetzgeber juristisches Neuland. Es beruht im Grundsatz auf einem Urteil des Europäischen Gerichtshofs aus dem Jahr 2014. Das neue Recht regelt die Tilgung personenbezogener Daten, die einem breiten Publikum zugänglich gemacht worden sind – zum Beispiel indem sie im Internet veröffentlicht worden sind. Ist der ursprüngliche Verbreiter dieser Informationen verpflichtet, die veröffentlichten Daten zu löschen, so muss er Dritte, die sie ebenfalls verbreiten, davon unterrichten.

Dabei muss er Dritten aber nicht grenzenlos hinterherrennen. Es genügt, „angemessene Maßnahmen“ anzuwenden, die die verfügbare Technologie und die Implementierungskosten berücksichtigen. Ohnehin müssen Informationen nicht gelöscht werden, falls sie etwa zur Ausübung des Rechts auf freie Meinungsäußerung, zu Forschungszwecken oder der Erfüllung rechtlicher oder öffentlicher Aufgaben dienen. Wie sich daher das neu geschaffene „Recht auf Vergessenwerden“ in der Praxis auswirkt und wie weit die Löschbegehren an Dritte weitergegeben werden müssen, ist derzeit vollkommen offen.

Recht auf Datenübertragbarkeit

Neu ist auch das Recht auf Datenübertragbarkeit, das der Artikel 20 formuliert. Es soll Bürger in die Lage versetzen, ihre personenbezogenen Daten nach eigenem Ermessen von einer IT-Umgebung zu einer anderen zu transferieren. So beschreibt es die (nach einem Artikel der älteren EU-Datenschutzrichtlinie benannte) Artikel-29-Gruppe, welche die Europäische Kommission in Fragen des Datenschutzes berät.

Das Recht auf Datenübertragbarkeit soll den Wettbewerb um die datenschutzfreundlichste Technologie anstacheln, den Verbraucherschutz fördern und dem „Lock-in-Effekt“ entgegenwirken. Dabei fesselt ein Anbieter Verbraucher aufgrund von schwierigen Wechselmodalitäten an sich. Hier hat der europäische Gesetzgeber zum Beispiel Cloud-Angebote, soziale Netzwerke und E-Mail-Anbieter im Blick.

Verbraucher können von ihrem Anbieter verlangen, dass dieser ihre personenbezogenen Daten „in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format“ bereitstellt. Der Anbieter soll die Daten einem anderen Anbieter ohne Behinderung übermitteln – und zwar möglichst direkt zwischen den Unternehmen. Hierzu sollen die Anbieter gemeinsam „interoperable Formate entwickeln, die die Datenübertragbarkeit ermöglichen“. Für die Übertragung gelten dieselben Fristen wie für Auskünfte.

Das neue Recht birgt allerdings noch eine ganze Reihe von offenen Fragen. So erfasst der Wortlaut des Artikels 20 nur personenbezogene Daten, also etwa Vertragsdaten, Nutzerverhalten und Lokalisierungsinformationen. Andere Inhalte erfasst diese Regelung nicht, also etwa die bei Cloud-Diensten lagernden Dateien oder Playlists bei Streaming-Diensten.

Offen ist ebenso, welche technischen und organisatorischen Anstrengungen der Anbieter unternehmen muss, um einen Transfer der Daten in einem interoperablen Format zu ermöglichen und dabei zugleich die Anforderungen an die Sicherheit der Daten zu erfüllen. Zumutbar dürfte auf jeden Fall das Bereitstellen von Informationen in gängigen Formaten sein.

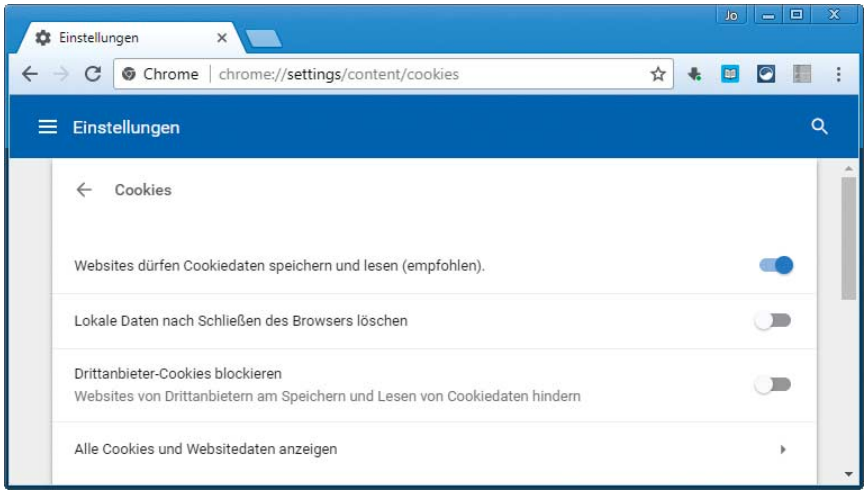
Privacy by design und default

Ähnlich ungeklärte Fragen gibt es bei zwei weiteren Neuerungen: Datenschutz durch Technikgestaltung sowie durch datenschutzfreundliche Voreinstellungen. Unternehmen sollen Probleme beim Umgang mit sensiblen Informationen schon bei der Entwicklung neuer Technologien berücksichtigen, anstatt diese erst im Nachhinein mit hohem Aufwand zu beseitigen.

Die DSGVO gibt vor, dass ein Unternehmen „geeignete technische und organisatorische Maßnahmen trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen“. Als Beispiel für solche Maßnahmen nennt die Verordnung explizit die Pseudonymisierung von Daten, also etwa durch die Bildung von Hashes auf IP-Adressen. Anbieter sollen nach Artikel 25 den Stand der Technik, die Kosten sowie die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten von Kunden bei der Planung berücksichtigen.

Derartige Vorgaben lassen sich vor allem im Online-Bereich gut umsetzen. So zählen zu den geschützten personenbezogenen Daten nach DSGVO auch IP-Adressen. Viele Programme und Funktionen erfassen und speichern diese, obwohl dieses vielfach gar nicht zwingend notwendig ist. Ein Privacy-by-design-Ansatz wäre hier, auf die Speicherung und Weitergabe der IP-Adressen zu verzichten und auf eine datenschutzfreundliche Lösung in Form einer Kürzung zu setzen, was für die allermeisten Zwecke ausreicht.

In eine ganz ähnliche Richtung gehen auch die Vorgaben zu „Privacy by default“, also die Verpflichtung zu datenschutzfreundlichen Voreinstellungen in Programmen, Apps oder sonstigen Anwendungen. Diese sollen grundsätzlich nur zwingend erforderliche personenbezogene Daten verarbeiten. Das umfasst die Menge der erhobenen Informationen, den Umfang ihrer Verarbeitung, die Speicherfrist sowie die Zugänglichkeit und Weitergabe.



Chrome lässt mit seinen Standardeinstellungen Drittanbieter-Cookies zu – DSGVO-konform?

Diese Vorgaben sind weitaus praxisrelevanter, als es auf den ersten Blick scheint. Man denke dabei zum Beispiel an die alles andere als datenschutzfreundlichen Voreinstellungen von Facebook, die erst aufwendig und mit Hilfe einer Anleitung umgestellt werden müssen, um zumindest die allerschlimmsten Überwachungsvorgaben auszuschalten.

Viele Juristen gehen davon aus, dass diese Regelung auch die Voreinstellungen von Browsern hinsichtlich der Akzeptanz von Cookies betrifft. Derzeit etwa akzeptiert Googles Chrome als meistgenutzter Browser in seinen Voreinstellungen beim Besuch einer Site auch die Cookies von Drittanbietern, also etwa von Werbedienstleistern. Würde das wegfallen, dann wäre das sicherlich verbraucherfreundlich, aber mit massiven Einbußen für Werbeindustrie und Medienhäuser verbunden.

Schutz von Kindern

Kinder sind sich der Risiken und Folgen und ihrer Rechte bei der Verarbeitung ihrer persönlichen Informationen weniger bewusst. Die DSGVO enthält daher Regelungen zum besonderen Schutz von Kindern, die im Bundesdatenschutzgesetz (BDSG) nicht enthalten waren. Der besondere Schutz gelte insbesondere bei einer Verwendung für Werbezwecke oder die Erstellung von Persönlichkeits- oder Nutzerprofilen.

Artikel 8 DSGVO etwa stellt klar, dass die Einwilligung eines Minderjährigen in die Verarbeitung der eigenen personenbezogenen Daten nur wirksam ist, „wenn das Kind das sechzehnte Lebensjahr vollendet hat“. Ist das Kind jünger, genügt dessen alleinige Entscheidung nicht. Vielmehr müssen die Eltern einwilligen. Daraus ergibt sich auch, dass eine nachträgliche Genehmigung der Eltern im Normalfall nicht ausreicht. Um dies herauszufinden, müssen Unternehmen „angemessene Anstrengungen“ unternehmen, um sich zu vergewissern, dass die Eltern tatsächlich ihren Segen gegeben haben. Wie dies in der Praxis umgesetzt werden soll, ist noch weitgehend offen. Nutzen Kinder Präventions- oder Beratungsdienste, müssen ihre Eltern dem nicht zustimmen.

Die besondere Rolle von Kindern spielt schließlich auch im Bereich der Informationspflichten bei der Erfassung von Daten eine Rolle. Richtet sich ein Angebot speziell an Kinder, so müssen Informationen in einer Form vermittelt werden, die auch Kinder verstehen können. Dies gilt auch für die Formulierungen im Rahmen von Datenschutzerklärungen.

Datenschutzrechtliche Selbstauskunft nach DSGVO
Betr: Name, Adresse, sonstige Identifikationsmöglichkeit (z. B. Kundennummer, verwendete E-Mail-Adresse)

Sehr geehrte Damen und Herren,

nach **Art. 15 DSGVO** habe ich das Recht, von Ihnen eine Bestätigung darüber zu verlangen, ob Sie personenbezogene Daten über meine Person gespeichert haben. Sofern dies der Fall ist, so habe ich ein Recht auf Auskunft über diese Daten.

1. Auskunft über meine bei Ihnen gespeicherten Daten
Ich darf Sie in diesem Fall bitten, mir gemäß Art. 15 Abs. 1 DSGVO folgende Informationen mitzuteilen:
a) Welche Daten über meine Person konkret bei Ihnen gespeichert oder verarbeitet werden (z.B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde).
b) Weiterhin wollen Sie mich bitte über die Verarbeitungszwecke meiner Daten ebenso informieren wie über
c) die Kategorien personenbezogener Daten, die bezüglich meiner Person verarbeitet werden;
d) die Empfänger oder Kategorien von Empfängern, die meine Daten bereits erhalten haben oder künftig noch erhalten werden;
e) die geplante Dauer für die Speicherung meiner Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
f) das Bestehen meiner Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung meiner Daten, ebenso wie über mein Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DSGVO und mein Beschwerderecht bei der zuständigen Aufsichtsbehörde.
g) Sofern die Daten nicht bei mir erhoben werden, fordere ich Sie auf, mir

ct5F – Die c’t-Fassung von Framstags freundlichem Folterfragebogen – erst ab 25. Mai verwendbar!

Recht mit Biss

Im Vergleich zu den weitgehend zahnlosen Sanktionen des BDSG droht die DSGVO mit hohen Bußgeldern. Dies gilt nach Artikel 83 auch für Verstöße gegen „die Rechte der betroffenen Person“, also insbesondere das Auskunfts- und Löschungsrecht. Hier drohen Unternehmen Geldbußen von bis zu 20.000.000 Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs – je nachdem, welcher der Beträge höher ist. Allerdings werden solche Summen natürlich nicht für schlampig handelnde Ersttäter, sondern nur als Ultima Ratio gegen bösartige und dauerhafte Datensünder verhängt.

Alles in allem erscheinen viele der Neuerungen aus Verbrauchersicht zumindest auf den ersten Blick begrüßenswert. Allerdings neigt der europäische Gesetzgeber dazu, Zugeständnisse an die Verbraucher vor allem in Form von überbordenden Informationspflichten zu machen. So werden die Pflichtbelehrungen in den Datenschutzerklärungen förmlich explodieren und sich deren Seitenanzahlen vervielfachen. Ob dies wirklich dem Interesse der Bürger dient, darf bezweifelt werden.

Das Recht auf Vergessenwerden, „Privacy by default“ und das Recht auf Datenübertragbarkeit sind neu. Hier wird sich erst zeigen müssen, wie sich diese innovativen Elemente in der Praxis auswirken werden. Dies gilt umso mehr, weil die Neuregelungen auch die Sanktionsmöglichkeiten gegen Datensünder ganz erheblich verschärfen. *(jo@ct.de)* c't

Download ct5F: ***ct.de/ycyu***