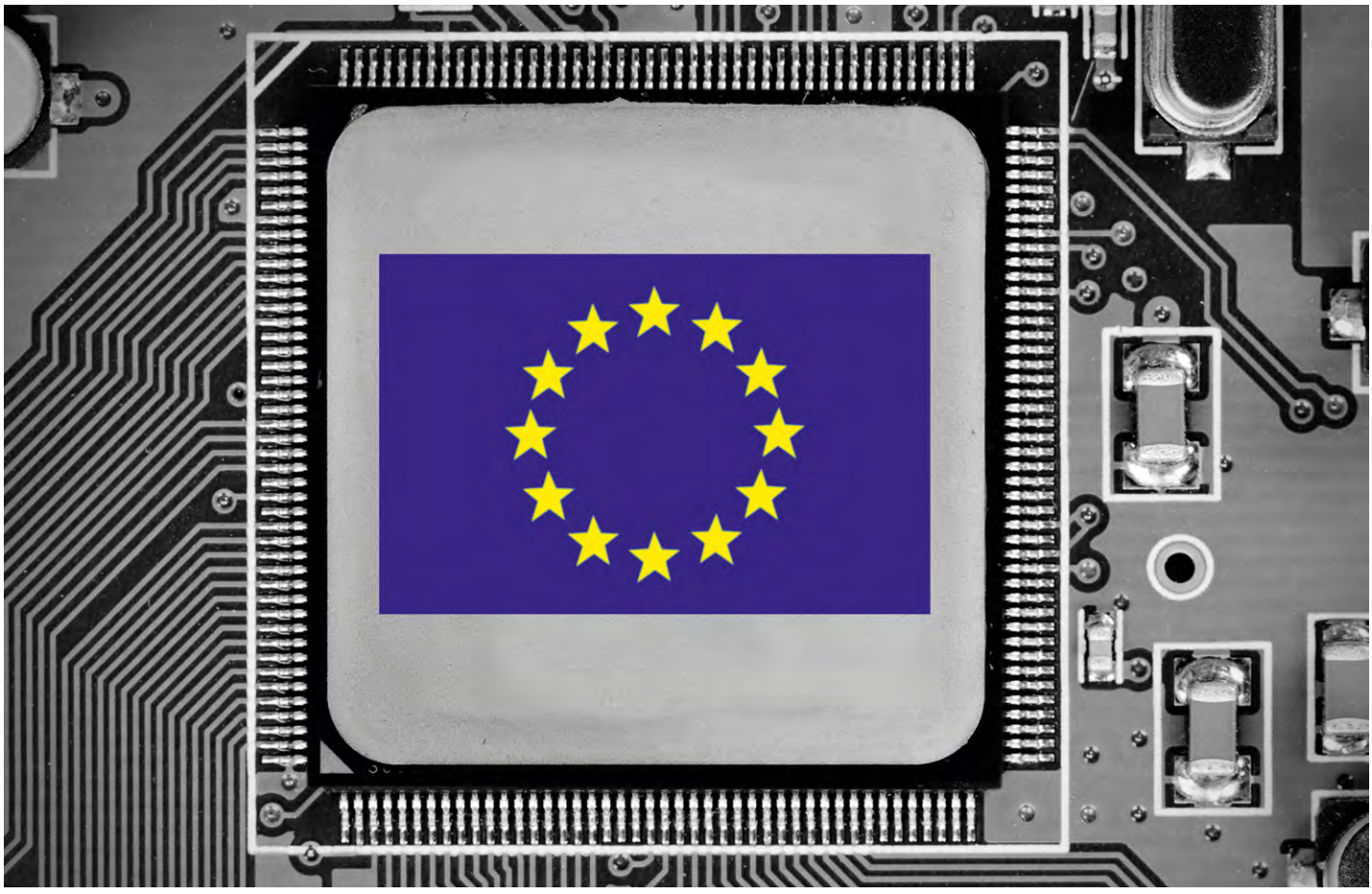


Europa schützt nun Ihre Daten

Ein langer **Machtkampf zwischen Lobbyisten und Datenschützern** geht zu Ende. Aber was bedeutet die Datenschutz-Grundverordnung für betroffene Bürger und Unternehmen?

VON FELIX KNOKE

Am 25. Mai wird die europäische Datenschutz-Grundverordnung (DSGVO) wirksam. Dann gelten europaweit strenge Regeln für alle, die mit personenbezogenen Daten arbeiten. Aber vielen Unternehmen droht damit juristischer Ärger: Weil sie sich zu spät, zu schlecht oder überhaupt nicht auf die Datenschutznovelle vorbereitet haben, könnten sie mit Abmahnungen überzogen, von Auskunftsansprüchen überrollt und mit empfindlichen Strafen belegt werden.

Immer so weiter wie bisher

Die Misere haben sie sich teilweise selbst eingebrockt. Zwar verlangt die neue Verordnung Unternehmen viel ab: Sie müssen ihre Prozesse durchleuchten, neues Personal einstellen und sich – bis zur eventuellen gerichtlichen Klärung – auf juristische und technische Unklarheiten einstellen. Indessen hatte das der Gesetzgeber vorhergesehen und allen Betroffenen zwei Jahre Übergangszeit zur Vorbereitung eingeräumt. Und in Deutschland gilt: Wer sich bis dahin schon eng an das Bundesdatenschutzgesetz hielt, auf den warteten auch keine große Überraschungen, sondern vor allem Anpassungen.

Aber anstatt sich in der Übergangszeit um den Datenschutz zu kümmern, machten viele Unternehmen offenbar weiter wie bisher. Das zeigen mehrere Umfragen zum Umsetzungsstand der DSGVO in Deutschland und dem EU-Ausland (siehe rechte Seite). Dabei ist Compliance nicht nur für die Firmen wichtig: Sie ist auch die Grundlage dafür, dass man als EU-Bürger ab dem 25. Mai von seinen zahlreichen neuen Rechten auf Auskunft, Löschung und Portabilität seiner Daten Gebrauch machen kann. Aber spätestens, wenn die ersten Abmahnwellen rollen und die Aufsichtsbehörden durchgreifen, wird dieser Datenschluder ein Ende haben. Davon sind alle Experten überzeugt, mit denen CHIP gesprochen hat. Datenschutz, das wird

Foto: EtiAmmos/Getty Images

sich dann herumsprechen, ist wirklich Pflicht. Dafür sollen letztlich auch drastische Strafen sorgen. Für Datenschutzverletzungen drohen dann Bußgelder von bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes – je nachdem, welcher Betrag höher ist. Solche Strafen sollen nicht nur kleinere und mittlere Unternehmen motivieren, sondern auch auf milliardenschwere Datenkonzerne eine abschreckende Wirkung haben.

Mehr Datenschutz für alle

Vier Jahre lang kämpften Datenschützer, Politiker, Lobbyverbände um jede Formulierung. Selbst Washington mischte sich mit 50 eigenen Lobbyisten in die Gesetzgebung ein. Aber der Gesetzestext, der vor zwei Jahren in Kraft trat, ist letztlich ein großer Schritt für den Datenschutz. Strenger und moderner ist kein Datenschutzgesetz der Welt. Auch wenn das erhebliche Einschränkungen für das datenverarbeitende Gewerbe, gerade die Online-Werbeindustrie mit ihren Tracking- und Profilingmaschen, bedeutet. Transparenz und Datenminimierung ist dann zum Schutz der Bürger europaweit Pflicht. Und das könnte sogar für Internetnutzer außerhalb der EU hilfreich sein: Um den europäischen Markt nicht zu verlieren, müssen auch ausländische Firmen, die hier Datengeschäfte machen wollen, ihre Prozesse an die Anforderungen der DSGVO anpassen.

Mit der Verordnung gibt es erstmals einen einheitlichen Rechtsrahmen, der den Umgang mit personenbezogenen Daten für Unternehmen und Behörden in der EU regelt. Wer dann in Europa mit solchen Daten arbeitet, unterliegt strengen Auflagen zur Dokumentation, Transparenz und Kontrolle. Nationale Ausnahmen, sogenannte Öffnungsklauseln, gibt es nur wenige. So können zum Beispiel die Länder festlegen, ab welchem Alter man der Datenverarbeitung zustimmen kann. In Deutschland gilt dazu der EU-Standard 16 Jahre, in Österreich 14 Jahre. Unter 13 Jahren darf es aber in keinem EU-Land sein.

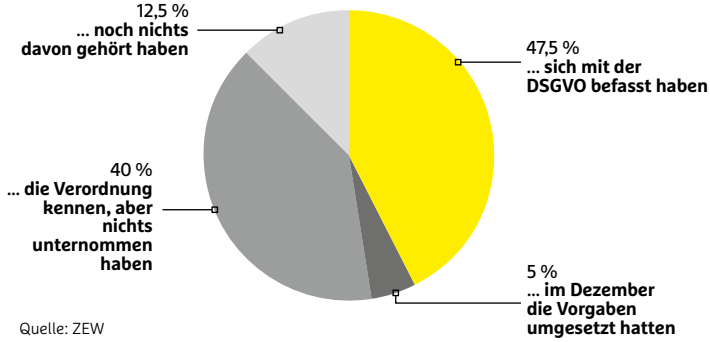
Im Gegenzug ermöglicht das Gesetz den freien Datenverkehr innerhalb der EU-Grenzen und eine Stärkung europäischer Unternehmen: Starker Datenschutz als Gütesiegel für Kundenfreundlichkeit. So ist zum Beispiel auch streng geregelt, unter welchen Umständen Daten überhaupt die EU verlassen dürfen. Nämlich nur, wenn in den Zielländern ein angemessener Datenschutz herrscht, Menschrenrechte eingehalten werden oder wenn die Daten im Firmenverbund mit verbindlichen Selbstverpflichtungen verbleiben.

Bürgerrechte statt Firmen-Wehwehchen

Die Reichweite der DSGVO ist enorm. „Jeder, der personenbezogene Daten verarbeitet, unterliegt der DSGVO“, warnt Rebekka Weiß, juristische Referentin für Datenschutz und Verbraucherrecht beim Branchenverband Bitkom. „Das können Personaldaten sein, Kundendaten, aber auch jegliche Kommunikation, die über eine Website läuft.“ Sie gilt für den Internetriesen genau so wie für den Kegelverein mit seinem Newsletter. Sie gilt für Kitas, Handwerker, Kirchen und Selbstständige – überall dort, wo personenbezogene Daten erhoben und verarbeitet werden oder durch Kombination unverfänglicher Fakten entstehen. Der Florist, der personalisierte Briefe über einen Dienstleister versendet, muss ebenso aufpassen wie das Unternehmen, das Festplatten zum Shreddern an einen Datenentsorger schickt – auch das kann eine Verarbeitung personenbezogener Daten darstellen.
Für EU-Bürger bedeutet all das vor allem eine unmittelbare Stärkung ihrer Rechte: Sie bekommen deutlich erweiterte Aus- →

Das bisschen Datenschutz...

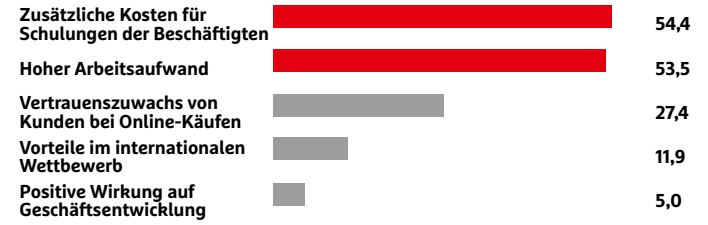
Anteil der Unternehmen der Informationswirtschaft, welche ...



Quelle: ZEW

Erheblicher Mehraufwand

Mit diesen Konsequenzen rechnen Unternehmen (in Prozent) durch die Einführung der Datenschutz-Grundverordnung



Quelle: ZEW

Die Betroffenenrechte

Obwohl in Deutschland bereits viele Regelungen gültig sind, baut die DSGVO die Betroffenenrechte weiter aus.

> Informationspflichten
Unternehmen müssen von sich aus viele Informationen zur Datenverarbeitung preisgeben, unter anderem Ansprechpartner für Datenfragen, Quellen und Kategorien von Datenempfängern und Details bei der Übermittlung in Länder außerhalb der EU. Bei algorithmischen Ansätzen müssen die verwendete Logik, die Tragweite und Auswirkung der Entscheidung erklärt werden.

> Recht auf Auskunft
Unternehmen müssen auf Anfrage mitteilen, welche Datenkategorien wie, wie lange und zu welchem Zweck gespeichert werden. Dazu kommen ihre eventuellen Empfänger. Maximal einen Monat haben Unternehmen Zeit, auf die Anfrage zu reagieren, im Regelfall unentgeltlich.

> Recht auf Vergessenwerden
Nicht nur Suchmaschinen, sondern jeder Datenverarbeiter muss auf Anfrage öffentliche, personenbezogene Daten löschen – und auch weitere Datenverarbeiter über den Löschwunsch informieren. Hier wird es rechtlich und technisch aber etwas schwammig.

> Recht auf Datenübertragung
Internetnutzer sollen ihre Daten zu einem neuen Anbieter in einem gängigen Format mitnehmen können. Hier sehen Experten noch großen Klärungsbedarf.

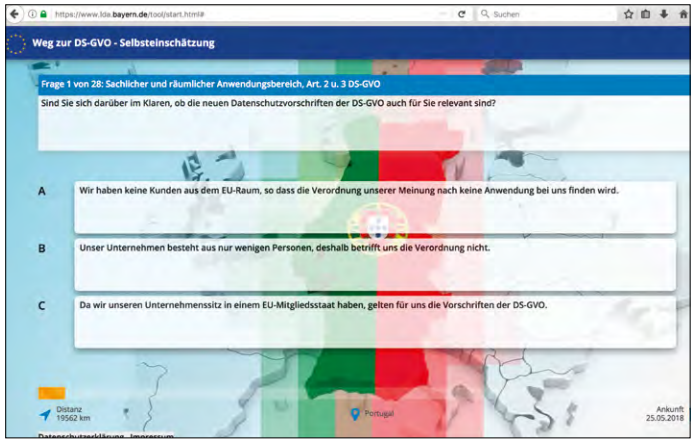
> One-Stop-Shop-Prinzip
EU-Bürger können sich bei Beschwerden immer an die eigene Datenschutzbehörde wenden, egal wo die betreffende Firma ihren Sitz hat. Das gilt ebenso für die Unternehmen.

INTERVIEW

Nicht das Ende der Welt

Guillaume Hersemeyer ist Rechtsanwalt und Datenschutzberater bei intersoft consulting services AG in Hamburg

> Wie erleben Sie die letzten Monate vor der DSGVO?
Wir stellen ein bisher ungekanntes Interesse für das Thema fest. In der Vergangenheit wurde Datenschutz in vielen Firmen eher stiefmütterlich behandelt. Das hat sich mit Inkrafttreten der Verordnung – nicht zuletzt aufgrund der dramatisch gestiegenen Bußgelder – geändert.
> Was ändert sich am 25. Mai?
Das Stichwort heißt Transparenz: Für Unternehmen bedeutet das erst einmal einen sehr hohen Umsetzungsaufwand, insbesondere durch die gestiegenen Dokumentations- und Nachweispflichten. Dabei hat das auch Vorteile: Speziell das Verzeichnis der Verarbeitungstätigkeiten kann einen grundlegenden Überblick über gelebte Prozesse geben und Optimierungspotenzial aufzeigen. Für die betroffenen Endkunden und Beschäftigten gibt es umfassende, teils neue Rechte. Gerade die gesteigerten Informationspflichten und Betroffenenrechte sollen dafür sorgen, dass sie Herr ihrer Daten bleiben.
> Wie nehmen Unternehmen die Auflagen auf?
Ein großer Kritikpunkt der Wirtschaft ist, dass die DSGVO keine Unterscheidung im Anwendungsbereich macht. Sie trifft das Reisebüro um die Ecke – mit einigen Ausnahmen – erst mal mit der gleichen Wucht wie Facebook oder Google. Viele Regelungen enthalten auch noch einigen Interpretationsspielraum. Zudem bleibt abzuwarten, inwieweit Betroffene tatsächlich von ihren Rechten Gebrauch machen. Hier wird erst die Praxis Antworten liefern.
> Erwarten Sie großes Chaos?
Nein. Die Welt wird sich auch nach dem 25. Mai noch weiterdrehen. Grundsätzlich bringt die DSGVO – zumindest in Deutschland – gar nicht so viele Neuerungen mit sich, wie mancher vielleicht befürchtet. Für viele Unternehmen ist die größte Herausforderung, dass sie sich mit Datenschutz in der Vergangenheit häufig nicht oder kaum befasst haben.



Das Bayerische Landesamt für Datenschutz hilft mit einem Quiz bei der Selbsteinschätzung: https://www.lda.bayern.de/tool/start.html

kunftsansprüche gegen Unternehmen und Behörden und können besser bestimmen, was mit ihren persönlichen Daten geschieht (siehe Kasten Seite 37). Und mehr als zuvor können sie hoffen, dass Unternehmen nicht nur von Datenschutz sprechen, sondern auch den dafür nötigen Aufwand betreiben: Die neuen Regeln fordern pauschal privacy by design und privacy by default ein. So sollen der Datenschutz ins Fundament neuer und alter Internetdienste verankert und datenschutzfreundliche Einstellungen standardmäßig vorausgewählt sein. Wer weniger Datenschutz will, soll das ausdrücklich mitteilen.

Bestrafen und beraten

Gerade diese Pflicht, von den Nutzern jeweils gültige Einwilligungen einzuholen, ist vielen Internetfirmen ein Dorn im Auge. Thomas Duhr, Vizepräsident beim Bundesverband Digitale Wirtschaft (BVDW), deutet das sogar als Nachteil für Verbraucher: „Die Erfahrung zeigt, dass sich kaum jemand mit den Bestandteilen solcher Vereinbarungen auseinandersetzt und stattdessen blind zustimmt." Besser wäre es ihm zufolge gewesen, „einwilligungslos, aber wie bisher in einem klar gesteckten Regelrahmen" die Datenverarbeitung zu ermöglichen. Nutzungsdaten im Internet würden praktisch gleichgesetzt mit Vitaldaten aus dem Bereich digitale Gesundheit. Genauso argumentiert auch schon die neue Staatsministerin für Digitales, Dorothee Bär (siehe Seite 8).

Tatsächlich ist die Umsetzung der DSGVO für Unternehmen alles andere als trivial. In 99 Kapiteln fordert sie ein hohes Verständnis für die technischen, juristischen und prozessualen Aspekte des praktischen Datenschutzes ein. „Grundsätzlich kann das jeder", so Rebekka Weiß vom Bitkom. „Aber das hängt auch eng mit der personellen Aufstellung zusammen: Wie viele Mitarbeiter beschäftigen sich bereits mit dem Datenschutz? Hab ich überhaupt jemanden, der sich damit beschäftigt?" Für viele Unternehmen bedeutet das, dass sie auf externe Hilfe zurückgreifen müssen: Datenschutzberater und externe Datenschutzbeauftragte haben deswegen gerade Konjunktur. „In der Geschäftsstelle erleben wir eine starke Nachfrage nach unserer Liste von Datenschutzbeauftragen", berichtet Jürgen Hartz, stellvertretender Vorsitzender des Berufsverbands der Datenschutzbeauftragten. Aber er warnt, die Aufgabe zu unterschätzen. Derzeit würden Seminare und Fortbildungen für zertifizierte Datenschutzbeauftragte „an fast jeder Ecke" angeboten. Aber das sei kein Job, den man mal eben nebenbei machen könne: „Die reine Bestellung einer Person zum Datenschutzbeauftragten macht ja keinen Datenschutz – und die Verantwortung und Haftung bleibt immer bei der Geschäftsleitung."

Unklarheiten beseitigen

Der erste Schritt zum Datenschutz nach DSGVO ist Nabelschau. Wer personenbezogene Daten verarbeitet, muss ein Verarbeitungsverzeichnis mit allen Datenverarbeitungsvorgängen aufbauen. Dazu gehören der Zweck der Datenverarbeitung, eine Liste aller beteiligter Unternehmen, wenn möglich Löschfristen und eine allgemeine Beschreibung der technischen und organisatorischen Datenschutzmaßnahmen wie Pseudonymisierung und Backups. Zumindest in Deutschland ist das zwar nicht alles neu – ähnlich war das schon im bis jetzt gültigen Bundesdatenschutz geregelt. Aber erst durch die harschen Sanktionsmöglichkeiten und den erklärten Willen, diese auch zu verhängen, wird eine breite Umsetzung auch realistisch.

Foto: Intersoft Consulting Services

Aber nicht alle Auflagen gelten in allen Fällen: So muss ein Datenschutzbeauftragter nur einbestellt werden, wenn die Datenarbeit aus datenschutzrechtlicher Sicht besonders kontrollbedürftig ist. Und nur Unternehmen, deren Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen darstellt, müssen eine aufwendige – und von Unternehmen viel kritisierte – Datenschutz-Folgenabschätzung durchführen, zum Beispiel bei Scoring, Profiling oder algorithmischen Entscheidungsfindungen mit rechtlichen Folgen für die Betroffenen.

Wer sich von dem möglichen Aufwand, den Unklarheiten und den Sanktionen der DSGVO verunsichert fühlt, sollte sich an seine zuständige Datenschutzbehörde wenden: Ihr kommt in der neuen Regelung nicht nur eine kontrollierende und strafende, sondern auch eine beratende Rolle zu. Und wer überhaupt nicht weiß, ob er oder seine Organisation überhaupt von der Verordnung betroffen ist, kann zum Beispiel mit einem Fragebogen des Bayerischen Landesamts für Datenschutzaufsicht einen Selbsttest durchführen (siehe links unten).

„Wer den Datenschutz bisher völlig ignoriert hat, wird es schwer haben, bis zum 25. Mai seine Hausaufgaben fertig zu bekommen.“

Eine neue Zeit des Datenschutzes

Die DSGVO stellt viele alte Gewissheiten auf den Kopf. Für Unternehmen, die intensiv mit personenbezogenen Daten im Internet arbeiten, könnte sich die Situation aber nächstes Jahr noch deutlich verschärfen. Dann soll die ergänzende ePrivacy-Verordnung in Kraft treten, die – eventuell (noch steht nichts fest) – zum Beispiel bisher gültige Regelungen zu Cookies und Tracking über den Haufen werfen könnte: Wer dann das Verhalten von Nutzern im Internet messen und verfolgen will, braucht dazu deren explizite Einwilligung. Unterschieden wird dabei zwischen Cookies, die zur Funktionalität eines Netzdienstes unabdingbar sind und Tracking-Cookies, die Nutzer im Netz verfolgen sollen. Die individuellen Datenschutzvorlieben sollen dabei über den Brower festgelegt werden können. Das ist ein Albtraum – gerade für die Daten- und Werbeindustrie, deren Geschäftsmodelle häufig nur auf dem Nachverfolgen, Profiling und der zielgerichteten Ansprache der Internetnutzer – also deren Überwachung – beruht.

Die EU steht dabei für einen bürgerfreundlichen, scharfen Datenschutz. Die Industrie, die alte Bundesregierung (und nach dem Koalitionsvertrag auch die neue) stehen aber für eine Aufweichung. Je nachdem, wie die ePrivacy-Verordnung ausfällt, ist das auch ein Maßstab für die Netzpolitik der neuen Bundesregierung. In jedem Fall aber gilt: Dank DSGVO und ePrivacy-Verordnung ist auch für kleinere Unternehmen die Zeit des schludrigen Umgangs mit personenbezogenen Daten vorbei.

redaktion@chip.de