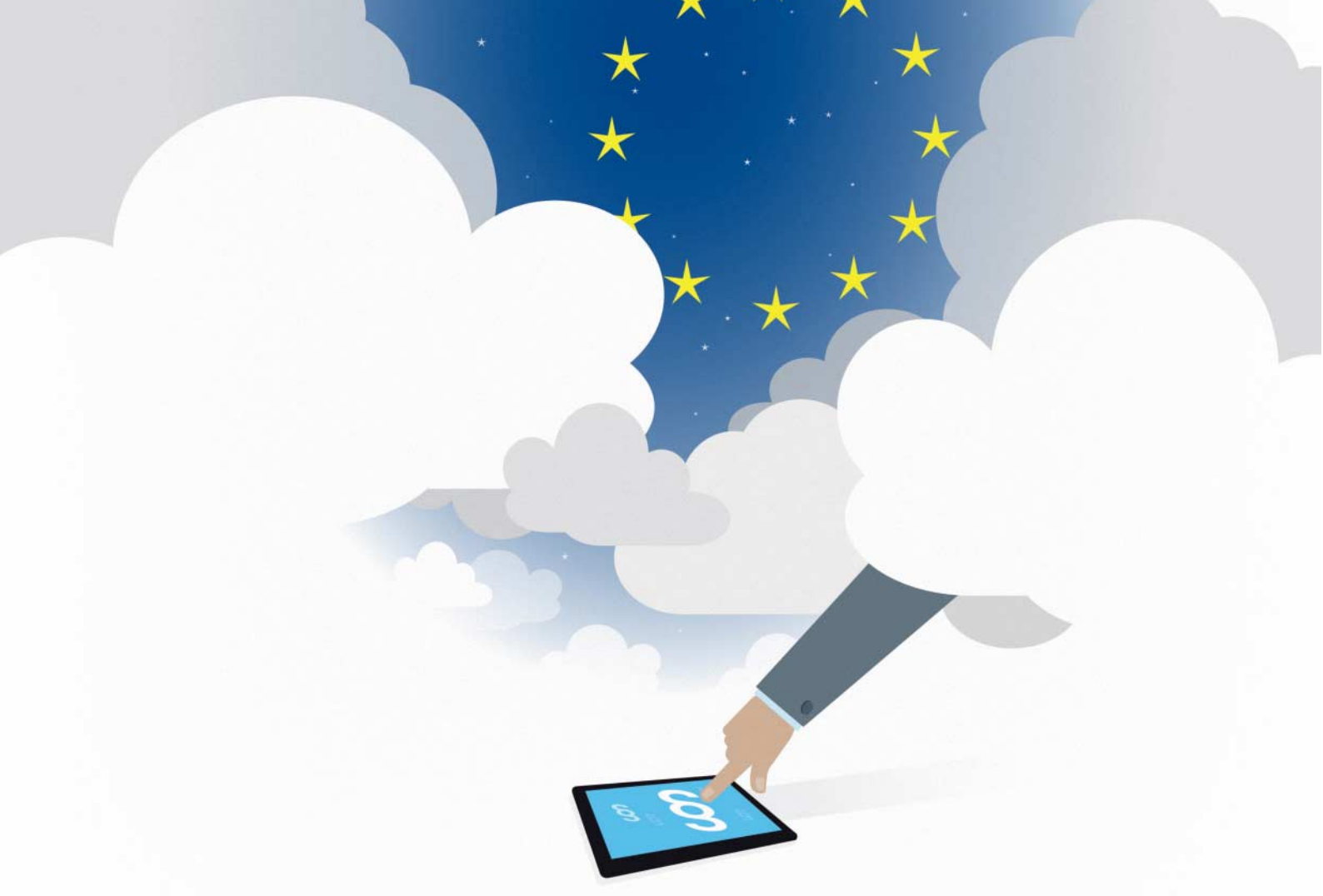

Neu verordnet

Welche Änderungen die neue EU-Datenschutz-Regulierung in Deutschland bringen wird

Ein europäischer Datenschutzpakt wird den Umgang mit persönlichen Daten auf dem gesamten Kontinent völlig neu regeln. Obwohl viele der Paragrafen an deutsches Recht angelehnt sind, forciereneinige Elemente der künftigen EU-Grundverordnung auch hierzulande Änderungen. Gut ist es, schon heute zu wissen, was auf Unternehmen, Behörden und Freiberufler, aber auch auf alle Privatpersonen Mitte 2018 zukommt.

VON STEPHAN HANSEN-OEST
UND JOERG HEIDRICH

Selbst für EU-Verhältnisse war es ein Mammutprojekt: Viele Jahre des Diskutierens gingen ins Land, Horden von Lobbyisten durften mitwerkeln, zuletzt musste das Europäische Parlament nicht weniger als 3100 Änderungsanträge abarbeiten. Nun steht sie, die neue Datenschutzgrundverordnung (DSGVO), und sie bringt eine umfassende Neuordnung des gesamten Datenschutzes in Europa [1].

Unüblich ist schon der gewählte regulatorische Weg. Bislang operierte die EU gerade im Bereich Internet und Datenschutz mit Richtlinien. Das sind europäische Vorgaben, die von allen nationalen Gesetzgebern in der EU in das jeweilige Recht des Landes umzusetzen sind.

Bei Verordnungen wie der DSGVO erlangen die beschlossenen Regelungen dagegen unmittelbar Geltung in den Mitgliedstaaten. Verordnungen gehen nationalem Recht vor und ersetzen es. Die Staaten passen ihre nationalen Gesetze in aller Regel dennoch an Verordnungen an. Mit der Datenschutzreform will die EU ein gleich hohes Datenschutzniveau in ganz Europa herstellen. Bestehende Wettbewerbsverzerrungen infolge unterschiedlicher nationaler Datenschutzbestimmungen wollte man unbedingt beseitigen.

Am 21. April wird der EU-Ministerrat aller Voraussicht nach die Verordnung durchwinken. Im Mai folgt das Parlament, kurz darauf erscheint die DSGVO im Eu-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

ropäischen Amtsblatt. 24 Monate später – also im Sommer 2018 – wird die Verordnung in Kraft treten. Bis dahin müssen alle nationalen Gesetzgeber ihre Regulierung angepasst haben. Sämtliche innerstaatlichen Regelungen im Bereich des Datenschutzes müssen durchgesehen und entweder aufgehoben oder zumindest angepasst werden. So arbeiten die Ministerien in Berlin gerade an einem umfassenden Rechtsbereinigungsgesetz. Über 200 verschiedene Gesetze hat man identifiziert, die nun verändert werden sollen.

Vorbild Deutschland

Die neue DSGVO enthält Dutzende sogenannte Öffnungsklauseln, die zwar einen regulatorischen Rahmen vorgeben, aber die konkrete Umsetzung den Mitgliedsstaaten überlassen. Sie sorgen dafür, dass die nationalen Gesetzgeber einzelne Bereiche völlig neu regeln dürfen beziehungsweise müssen, beispielsweise die Rolle der Datenschutzbeauftragten. Immerhin: Verglichen mit anderen Ländern wird sich in Deutschland nicht alles grundsätzlich ändern, da die EU einige Fundamente der DSGVO dem deutschen Recht nachempfunden hat.

Dies gilt insbesondere für den ehernen Grundsatz des „Verbots mit Erlaubnisvorbehalt“. Danach sind alle Arten des Umgangs mit persönlichen Informationen so lange verboten, bis der Gesetzgeber die Handlung explizit erlaubt oder der Betroffene ausdrücklich einwilligt. Ebenso behält die neue DSGVO die elementaren Grundsätze des Datenschutzes – Datensparsamkeit und Transparenz – bei, und dies sogar in verschärfter Form.

Auch das Gebot der Zweckbindung bleibt, obwohl es im Rahmen des Gesetzgebungsverfahrens immer wieder Gegenstand heftiger Auseinandersetzungen war. Danach dürfen personenbezogene Daten nur für „festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden“. Die DSGVO erwähnt einige Ausnahmen von der engen Zweckbindung, beispielsweise eine Nutzung der Daten in der Forschung.

Diese Beschränkung auf einen konkreten Zweck der Erhebung steht vor allem einer unbeschränkten Nutzung von Informationen für Big-Data-Prozesse entgegen. Detailliert regelt dies Artikel 6 der DSGVO. Wenn ein Unternehmen beispielsweise zum Zweck der Abwicklung eines Kaufvertrags personenbezogene Daten von Kunden erhebt, ergibt sich daraus künftig nicht automatisch die Erlaubnis, diese Daten zu anderen Zwecken zu nutzen.

Auf US-Konzerne, die in Europa ihre Dienste anbieten, kommen härtere Zeiten zu. Bisher galt für sie das sogenannte Sitzlandprinzip. Danach griffen im Falle von juristischen Konflikten die Gesetze des Landes, in dem das beteiligte Unternehmen seinen Hauptsitz hat. Dies war beispielsweise für Facebook immer Irland, wo der Social-Media-Gigant seine europäische Zentrale betreibt. Zuständig für Auseinandersetzungen mit Facebook war daher in den meisten Fällen die irische Aufsichtsbehörde, der nicht unbedingt ein Ruf als unnachgiebige Verfechterin des Datenschutzes vorauseilt.

Diese Praxis ändert sich nun, es gilt ab Sommer 2018 das Marktortprinzip. Wer EU-Bürgern dann Leistungen anbieten will, muss zwingend die DSGVO in der Version beachten, die im jeweiligen Zielland gilt. Dies umfasst ausdrücklich auch kostenlose Dienste – also Gratis-Services von Konzernen wie Google, Facebook oder Microsoft. Unternehmen aus Drittstaaten müssen künftig sogar einen Vertreter für die EU benennen, der als Anlaufstelle und Ansprechpartner für Betroffene und Aufsichtsbehörden fungiert. Kritiker der Neuregelung befürchten nun, dass einigen US-Unternehmen das zu viel wird und sie deshalb EU-Bürger gänzlich von der Nutzung ihrer Dienste ausschließen könnten.

»Wichtige Fundamente der Grundverordnung sind dem deutschen Datenschutzrecht nachempfunden.«

Verbraucherrechte

Gewinner des neuen europäischen Rechts sind in vielen Punkten die Verbraucher. Mehr als zuvor hängt von ihrer persönlichen Erlaubnis ab. Artikel 7 und 8 der DSGVO regeln explizit die Voraussetzungen, die für eine Einwilligung zur Datenverarbeitung zu beachten sind. Diese muss wie bisher freiwillig und in Kenntnis der beabsichtigten Nutzung erfolgen. Der Verbraucher darf die Zustimmung jederzeit widerrufen. Sie unterfällt – wie aus dem deutschen Recht bekannt – einem Kopplungsverbot, wonach „die Erbringung einer Dienstleistung nicht von der Einwilligung zur Verarbeitung von Daten abhängig gemacht“ werden darf, die für die Erfüllung des Vertrags nicht erforderlich ist. Gemeint sind hier beispielsweise die berüchtigten „Gewinnspiel-Kopplungen“, bei denen man durch die Teilnahme an einer Verlosung einer Verwendung der persönlichen Daten zu Marketingzwecken mit zustimmen muss.

Ab welchem Alter ein Heranwachsender wirksam eine solche Einwilligung erteilen kann, ist der Regelung durch die einzelnen Mitgliedsstaaten überlassen. Artikel 8 nennt lediglich das Mindestalter von 13 Jahren. Eine bloße Angabe des Alters, um Einlass zu erhalten, dürfte aber bald nicht mehr ausreichen: Die DSGVO führt Prüfpflichten ein. So sollen die Unternehmen „unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen“ unternehmen, um nachzuprüfen, dass „die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde“. Tatsächlich könnten sich hinter dieser Formulierung neue Jugendschutzpflichten verbergen, die dem Datenschutz bisher weitgehend fremd waren. Ob beispielsweise Social-Media-Plattformen nun Altersverifikationssysteme vorschalten müssen, ist bislang unklar.

Artikel 12 der neuen Verordnung legt außerdem strengere Informationspflichten fest. Unternehmen müssen den Nutzern die Rechtsgrundlage zur Verarbeitung der Daten ebenso mitteilen wie die Dauer der Speicherung, die Kriterien für die Dauer der Speicherung oder die Weitergabe an Auftragsdatenverarbeiter. Diesen Informationspflichten stehen Regeln zu Auskunft, Widerruf sowie Löschung zur Seite. In der Praxis dürfte dies zu neuen, seitenlangen Belehrungsschriften führen, die von den Betroffenen abzunicken sind, ohne jemals gelesen zu werden. Überdies dürften solche Informationspflichten immer neuen Stoff für Massen-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Bild: European Union, 2015

Mit Infografiken versucht die EU Verbraucher und Unternehmen zu überzeugen, dass die neuen Datenschutz-Regeln alles besser machen.

abmahner bereitstellen, die jeden Fehler mit teuren Anwaltsschreiben bestrafen.

Recht auf Vergessenwerden

Als „Recht auf Vergessenwerden" bekannt sind Löschansprüche, die Betroffenen zustehen. Anders als bei dem vom Europäischen Gerichtshof postulierten Recht zur Sperre von personenbezogenen Suchmaschinenergebnissen geht es in der DSGVO um die Löschung direkt bei der speichernden Stelle. Für Daten, die Unternehmen selbst über eine Person veröffentlicht haben, besteht künftig sogar eine Pflicht der Unternehmen, auch andere Stellen, die diese Daten ebenfalls verarbeiten, über den Löschungsanspruch des Betroffenen zu informieren. Kritiker befürchten angesichts dieser sehr weitgehenden Regelung, dass die Informations- und Meinungsfreiheit im Internet leiden könnte. Auf jeden Fall wird das Recht auf Vergessenwerden für neue Rechtsunsicherheit sorgen. Wie in vielen anderen Bereichen auch dürfte es Jahre dauern, bis die Gerichte hier für eine Auslegung der wenig konkreten Rechtsnormen sorgen werden.

Eine echte Neuerung ist das in Artikel 18 DSGVO geregelte Recht auf Datenportabilität. Hieraus entsteht ein Anspruch des Betroffenen, seine im Rahmen einer Einwilligung oder eines Vertrags übertragenen personenbezogenen Daten vom Vertragspartner in einem „strukturierten, gängigen und maschinenlesbaren Format zu erhalten" und diese Daten einem anderen Anbieter zu übermitteln.

Damit nicht genug: Der Nutzer wird sogar verlangen können, dass der bisherige Verwender seiner Daten diese direkt an den neuen Anbieter übermittelt – soweit dies technisch möglich ist. Mit dieser Regelung will die EU zugleich die Entwicklung interoperabler Formate fördern, die eine solche Datenübertragbarkeit ermöglichen. In eine ähnliche Richtung geht die in Artikel 23 enthaltene Verpflichtung zur Förderung von datenschutzfreundlichen Grundeinstellungen und von „Privacy by Design". Man wird sehen, ob etwa Google+-Konten inklusive aller hinterlegter Daten ab Sommer 2018 per Mausklick zu Facebook gezogen werden können – und umgekehrt.

Rechenschaftspflichten

Für Behörden, Unternehmen und Freiberufler hält die DSGVO einige Neuerungen bereit, die erheblichen Aufwand erzeugen werden. Dies gilt vor allem für die in Artikel 22 geregelte Rechenschaftspflicht für den Umgang mit Daten. Danach müssen je nach Art der Daten „geeignete technische und organisatorische Maßnahmen" ergriffen werden, um sicherzustellen und den Nachweis dafür erbringen zu können, dass personenbezogene Daten in Übereinstimmung mit den neuen EU-Regelungen verarbeitet werden.

Diese neuen Rechenschaftspflichten bringen möglicherweise auch haftungsrechtliche Konsequenzen mit sich: Derzeit muss ein Betroffener vor Gericht selbst den Nachweis dafür erbringen, dass das Unternehmen oder die Behörde als verantwortliche Stelle für eine fehlerhafte Verarbeitung von Daten haftbar ist. Diese Pflicht obliegt nun nach dem neuen Artikel 22 der datenverarbeitenden Stelle. Und dies müsste durch Dokumente belegt werden können.

Hier kommt es de facto zu einer Beweislastumkehr, was viele Unternehmen derzeit noch nicht berücksichtigt haben. Die DSGVO stellt Methoden bereit, um die Einhaltung dieser Rechenschaftspflichten zu vereinfachen – insbesondere Zertifizierungsverfahren oder genehmigte Verhaltensregeln. In Zukunft werden Unternehmen folglich mehr von derlei Zertifizierungen Gebrauch machen, um die Einhaltung der Pflichten nach außen besser dokumentieren zu können.

Folgenabschätzung

Auch hinsichtlich der Datensicherheit gibt es neue Vorgaben durch die DSGVO. Es bleibt zwar dabei, dass Unternehmen abhängig vom Schutzbedarf der Daten und der wirtschaftlichen Zumutbarkeit technische und organisatorische Maßnahmen zur Datensicherheit zu treffen haben. Zu gewährleisten ist nun aber zusätzlich die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste, mit denen personenbezogene Daten verarbeitet werden. Denkbar ist etwa eine Zertifizierung nach derzeit aktuellen Standards der Informationssicherheit wie der internationalen Norm ISO/IEC 27001.

Die DSGVO sieht außerdem vor, dass Unternehmen künftig bei risikobehafteten Datenverarbeitungen eine „Datenschutz-Folgenabschätzung" nach bestimmten Kriterien durchzuführen haben. Doch nicht nur das: Falls sich aus der Folgen-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

abschätzung ergibt, dass ein Risiko für die Betroffenen besteht, müssen Unternehmen oder Behörden die für sie zuständige Aufsichtsbehörde darüber informieren. Diese soll dann binnen acht Wochen schriftliche Empfehlungen an das Unternehmen zur Risikominimierung geben; sie darf die Datenverarbeitung aber auch untersagen.

Diese in Artikel 34 geregelte „vorherige Konsultation“ ist eines der folgenreichsten „Institute“ des neuen EU-Datenschutzrechts. Kritiker bemängeln sich hieraus ergebende Innovationshemmnisse. Denn Unternehmen können in Zeiten von agiler Softwareentwicklung häufig nicht die Entscheidung von Aufsichtsbehörden abwarten, zumal deren Stellungnahmefrist von acht Wochen auch noch verlängert werden kann. Nur ein Beispiel: Google veröffentlicht alle sechs Wochen eine neue Version des Chrome-Browsers, oft durchaus mit Auswirkungen auf das Datenschutz-Design. Es bleibt abzuwarten, ob der Konzern nun jedes Mal den zuständigen Hamburgischen Datenschutzbeauftragten um seine Einschätzung bitten wird.

Nach dem Bundesdatenschutzgesetz (BDSG) müssen Unternehmen ab zehn Mitarbeitern einen Datenschutzbeauftragten abstellen. Diese Abhängigkeit zur Mitarbeiterzahl sieht die DSGVO nicht mehr vor. Behörden, öffentliche Stellen und Unternehmen, welche „eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen“, müssen auch künftig Datenschutzbeauftragte bestellen. Hier sieht die EU jedoch eine Öffnungsklausel für die Mitgliedstaaten vor. Sie dürfen die Bedingungen anpassen. Beobachter gehen davon aus, dass es die Bundesregierung wohl bei der alten Regelung aus dem noch gültigen BDSG belassen möchte.

Teure Verstöße

Das neu geschaffene europäische Datenschutzrecht ändert nicht alles – aber doch vieles. Es erweitert in vielen Punkten die Rechte der Verbraucher. Für Unternehmen entstehen dagegen eine ganze Reihe von neuen Pflichten. Herauszuheben ist hier vor allem die Pflicht zur Schaffung eines Datenschutzmanagements, die viele betroffene Mittelstandsunternehmen oder Selbstständige vor erhebliche Herausforderungen stellen wird. Auch wenn das Inkrafttreten noch weit entfernt klingt, sollten sich Unternehmen rechtzeitig mit der Umsetzung beschäftigen und sich auf die anstehenden Änderungen vorbereiten.

Noch stehen die Datenschutz-Regeln in Deutschland im Ruf, ein weitgehend zahnloser Tiger zu sein. Über die im BDSG festgelegten Sanktionen schmunzelten viele Unternehmer. Das maximale Bußgeld in Höhe von 300 000 Euro pro Einzelfall wurde nur sehr selten abgerufen. Und gerade bei den US-Konzernen, die das deutsche Recht oft bewusst ignorieren, läuft eine solche Summe eher in der Kategorie „Portokasse“.

Bald drohen auf Basis der DSGVO ganz andere Hausnummern, was zweifellos die Akzeptanz des Datenschutzes und dessen Bedeutung im Compliance-Bereich erhöhen wird. Damit die drohenden Geldbußen wie in Artikel 79 verlangt auch „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein können, sind nun Strafzahlungen bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes eines Konzerns möglich.

Beendet hat die EU übrigens quasi en passant auch einen uralten Streit unter Juristen, nämlich die Frage, ob es sich bei IP-Adressen um personenbezogene Daten handelt, die dem Datenschutz unterfallen. In den Erwägungsgründen der Verordnung wird klargestellt, dass sich Nutzer beziehungsweise Anschlussinhaber anhand dieser Informationen identifizieren lassen. Es kommt nicht darauf an, ob dies beispielsweise nur für den Provider möglich ist, es reicht vielmehr die abstrakte Möglichkeit einer Identifikation.

Da in diesem Zusammenhang auch auf Cookies verwiesen wird, könnte dies weitgehende Auswirkungen fürs Online-Marketing haben, vor allem für die Identifikation von Nutzern im Rahmen von Behavioral Targeting. Es bleibt gleichwohl abzuwarten, ob und wie die Neuregelung der sogenannten E-Privacy-Richtlinie der EU hier Vorgaben vorsehen wird. Denn diese Richtlinie, mit der beispielsweise die Nutzung von Cookies in der EU geregelt wird, wird ab 2016 von der EU-Kommission überarbeitet. Wie man aus Brüssel hört, soll bei dieser Gelegenheit auch das Thema Cookie-Tracking noch einmal auf den Prüfstand kommen. *(hob@ct.de)* c't

Literatur

[1] Christiane Schulzki-Haddouti, Datenschutz europaweit, Was sich mit der EU-Grundverordnung ändern wird, c't 03/16, S. 86

Was Unternehmen schon jetzt für die Vorbereitung auf die DSGVO tun sollten

- Verschaffen Sie sich eine umfassende Übersicht über alle Datenverarbeitungsvorgänge in Ihrem Haus, die personenbezogene Daten betreffen.
- Erstellen Sie eine Dokumentation über diese Vorgänge.
- Prüfen Sie unter dem Gesichtspunkt der Datenminimierung, ob diese Datenverarbeitungen tatsächlich erforderlich sind.
- Erstellen Sie ein Konzept bezüglich der Umsetzung der Informationssicherheit in der eigenen Datenverarbeitung. Hier können Vorgaben wie die ISO 27001 herangezogen werden.
- Konzipieren Sie Richtlinien und neue Prozesse für die Einführung künftiger Verarbeitung von personenbezogenen Daten, die darauf ausgerichtet sind, Datenschutz-Folgeabschätzungen zu ermöglichen.
- Beschäftigen Sie sich mit Zertifizierungsangeboten und bereiten Sie deren Umsetzungen vor.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover