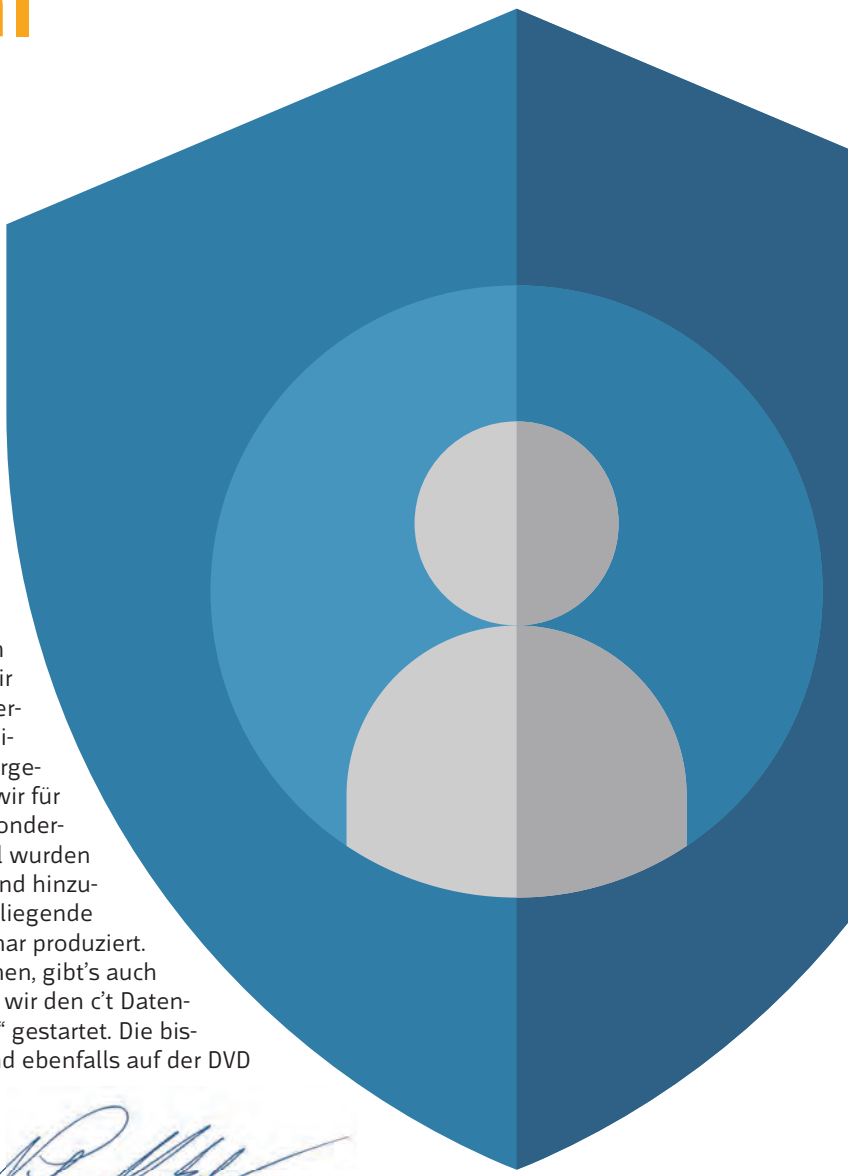
Editorial



Liebe Leserin, lieber Leser,

ein ereignisreiches Datenschutz-Jahr ist seit der Veröffentlichung der ersten Auflage unseres DSGVO-Sonderhefts verstrichen. Es hat sich viel getan. Die Datenschutzbehörden haben die ersten Millionenbußgelder verhängt, etliche Datenskandale haben für großes Aufsehen gesorgt und Gerichte hatten über DSGVO-Streitigkeiten zu entscheiden. Von Rechtssicherheit im Bereich des Datenschutzes kann jedoch noch lange keine Rede sein. Deswegen heißt es: Am Ball bleiben! Daher waren auch wir nicht untätig und haben uns weiterhin intensiv mit datenschutzrechtlichen Fragestellungen auseinandergesetzt. Unsere Erfahrungen haben wir für Sie in die zweite Auflage dieses Sonderhefts einfließen lassen. Alle Artikel wurden aktualisiert, viele neue Beiträge sind hinzugekommen und eigens für die beiliegende DVD haben wir ein weiteres Webinar produziert. Um wirklich alle Sinne anzusprechen, gibt's auch noch was zum Hören. 2019 haben wir den c't Datenschutz-Podcast „Auslegungssache" gestartet. Die bislang veröffentlichten Episoden sind ebenfalls auf der DVD enthalten.

Joerg Heidrich & Nicolas Maekeler

Im Alltag angekommen?

Datenschutzverantwortliche haben sich durch Verarbeitungsverzeichnisse gekämpft, mit Datenschutzerklärungen gerungen und Cookies gebändigt. Und nun können alle wieder zur Tagesordnung übergehen, oder? Mitnichten, denn die DSGVO ist ein Dauerbegleiter. Die Gefahr saftiger Strafen sorgt für die notwendige Aufmerksamkeit.

Von Joerg Heidrich

Nachdem zunächst über ein Jahr lang so gut wie keine Geldbußen durch die Aufsichtsbehörden verhängt wurden und auch die fälschlicherweise prophezeiten Abmahnwellen nicht stattgefunden haben, ist vielerorts das Interesse am Datenschutz schlagartig wieder erlahmt. Doch das Vertrauen darauf, dass dieser Zustand auf Dauer anhält, wird sich als einigermaßen naiv erweisen. Dies zeigt nicht nur der Blick ins europäische Ausland, in dem die Strafen bereits mühelos sieben- und achtstellige Höhen erreicht haben. Auch hierzulande gibt es inzwischen Bußgelder im achtstelligen Bereich, die jedem Unternehmen wehtun und die sich zudem auch nicht gerade rufördernd auswirken.

Ohnehin wendet sich der anfangs eher gütige Blick der Aufsichtsbehörden zunehmend Bereichen zu, die in vielen Unternehmen immer noch nicht oder nur ansatzweise umgesetzt sind. Doch auch die bisher im Rahmen etwa von TOMs oder den Verzeichnissen der Verarbeitungstätigkeiten gefertigten Dokumentationen dürfen nicht für alle Zeiten in den Tiefen der Büroschränke verschwinden. Vielmehr müssen sie regelmäßig überholt und angepasst werden. Das Jubiläum zur zweijährigen Anwendung der DSGVO könnte hier einen angemessenen Zeitpunkt bieten, die Unterlagen einmal durchzusehen und zu überarbeiten.

Stand der Technik umsetzen

Dies gilt etwa für die TOMs: Diese technisch-organisatorischen Maßnahmen muss ein Datenverarbeiter zum Schutz der von ihm vorgehaltenen Daten nicht nur umsetzen, sondern auch detailliert dokumentieren. Einfluss auf diese Strukturen hat dabei vor allem die zentrale Vorgabe zur IT-Sicherheit in Art. 32 DSGVO. Vereinfacht gesagt kann man sich diese Vorgaben als Waage vorstellen. Auf der einen Seite liegen dabei die Daten. Je sensibler diese sind und auch je mehr Informationen vorhanden sind, desto höher sind auf der anderen Seite die Anforderungen an die IT-Sicherheit.

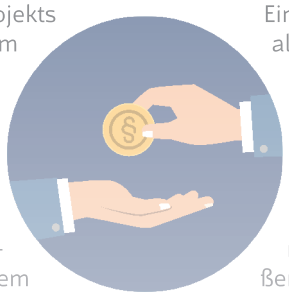
Gerade bei hoch schützenswerten Daten, wie solchen aus dem Bereich der Gesundheit, entstehen enorm hohe Vorgaben, die bisweilen auch einem reibungslosen Betrieb des Unternehmens nicht immer förderlich sind. Zugleich enthält Art. 32 DSGVO noch die Anforderung, den „Stand der Technik“ zu beachten, was in sehr vielen Unternehmen immer noch nicht umgesetzt wurde (siehe dazu den Artikel ab S. 94).

Gut abgeschätzt

Ebenso große Defizite weisen die meisten Unternehmen im Bereich der Folgenabschätzung auf. Dies sind Gutachten, die Unternehmen zur Risikobeurteilung abfassen müssen, wenn sie bei geplanten Vorhaben Risiken feststellen (siehe Artikel ab S. 98). Wichtig dabei: Die Risiken sind nicht aus der Perspektive des Verarbeiters, sondern aus derjenigen der Betroffenen zu beurteilen, also etwa der Kunden oder der Mitarbeiter.

Darüber hinaus hat der Gesetzgeber eine Reihe von Sachverhalten festgelegt, in denen immer eine Folgenabschätzung durchzuführen ist. Hierzu gehört insbesondere der praxisrelevante Bereich der großflächigen Videoüberwachung, aber auch die „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 DSGVO“, also etwa von Krankendaten.

Praktisch ist dabei, das bestehende Risiko der Datenverarbeitung zu analysieren und das Ergebnis in ein Verhältnis zu den Gefahren für die Betroffenen zu stellen. Die Analyse und das Ergebnis sind zu dokumentieren. Je nach Komplexität des Projekts kann der Umfang einigen Blättern, einem Reclam-Heft oder auch einer Buddenbrooks-Ausgabe entsprechen.



Diese Analysen verschwinden nach ihrer Auswertung im günstigsten Fall für immer in der Schublade des Datenschutzbeauftragten und werden nie wieder benötigt. Wehe aber dem Verantwortlichen, dem etwas passiert und der in diesem Fall keine ordentliche Folgenabschätzung vorweisen kann! Diese Verfehlung kann leicht eine zusätzliche Null bei der Bemessung der Geldstrafe durch die Aufsichtsbehörde nach sich ziehen. So gab es bereits in Schweden eine Strafe gegen eine Schule, welche die Anforderungen nach Art. 35 DSGVO ignoriert hat.

Vervielfachte Strafen

Überhaupt, die Strafen: Ein halbes Jahr dauerte es, bis es im Fall „Knuddels“ überhaupt die erste in Deutschland verhängte Strafe gab – und die war mit 20.000 Euro angesichts der im Raum stehen-

gegen die bereits in anderen europäischen Ländern üblichen sechs-, sieben- oder gar achtstelligen Geldbußen (siehe Artikel ab S. 68).

Allerdings bleiben solche Strafen natürlich nicht unwidersprochen, sodass daraus Gerichtsurteile resultieren werden, die hoffentlich etwas mehr Licht in die bisweilen doch sehr trübe Rechtslage der DSGVO bringen. Dabei wird es auch spannend sein, zu sehen, in welchen Bereichen die immer noch personell stark unterbesetzten Aufsichtsbehörden die Prioritäten bei der Verfolgung von Verstößen sehen werden.

Still ruht der Abmahnsee

Währenddessen ist von den erwarteten Abmahnwellen in der Praxis bis auf einige bisweilen eher exotisch-komische Versuche wenig zu sehen. So sorgte ein Schreiben eines Anwalts aus Berlin in der Fachwelt für Schmunzeln, mit dem er versuchte, für seinen Mandanten eine fünfstellige Summe als Schadensersatz für das unverschlüsselte Senden von Kontaktdaten über ein Formular zu erbetteln.

Ein Grund für die bisherige Ruhe ist vor allem, dass der Abmahnanwalt ein eher scheues Tier ist, das vor allem auf eine klare und eindeutige Rechtslage setzt, um auf Beutezug zu gehen. Diese Rechtssicherheit fehlt jedoch, da immer noch nicht abschließend geklärt ist, ob Abmahnungen auf Basis von DSGVO-Verstößen tatsächlich wirksam sind. Nicht nur die Fachwelt ist sich hier uneins, auch die Gerichte kommen zu höchst unterschiedlichen Ergebnissen.

Auf zur nächsten Runde!

Insgesamt gilt also: Die DSGVO ist ein Dauerprojekt und unterliegt ständigem Wandel. Nicht nur die Dokumentationen müssen Unternehmen und andere Institutionen regelmäßig anpassen und bei Bedarf erneuern. Auch neue Entwicklungen und Herausforderungen müssen sie verfolgen und beachten. Denn eins ist sicher: Bußgelder werden nicht nur zahlreicher, sondern auch schmerzlicher. Auf der an-

Lesen Sie mehr in der c’t DSGVO 2020.

Mehr Rechte für Bürger

Ein wesentliches Ziel der Datenschutz-Grundverordnung ist der Schutz des Einzelnen bei der Verarbeitung personenbezogener Daten. Um diesen zu verbessern, hat sie die Rechte der Betroffenen erweitert.

Von Niklas Mühleis

Datenschutz bedeutet in erster Linie nicht den Schutz von Daten, sondern es geht um die Stärkung der Persönlichkeitsrechte des Betroffenen. Erreichen will die DSGVO dies durch mehr Pflichten für Unternehmen und mehr Rechte für Bürger.

Transparenz und Verständlichkeit

Zunächst stehen die Gebote der Transparenz und der Verständlichkeit über allem anderen. Verbraucher sollen nachvollziehen können, wer mit ihren Daten hantiert und was mit ihnen geschieht. Die Verantwortlichen für die Datenverarbeitung sind laut Artikel 12 der DSGVO dazu verpflichtet, Nutzer in einer transparenten, verständlichen und leicht zugänglichen Form über die Verarbeitung ihrer Daten zu informieren. Verantwortliche sind beispielsweise Unternehmen, Vereine und andere Organisationen. Diese Informationen dürfen also nicht in einem undurchdringlichen Wust sonstiger Hinweise versteckt oder in komplizierte Schachtel- und Negativsätze gepackt sein, deren Sinn sich kaum erschließen lässt. Ausdrücklich von der Verordnung gefordert ist daher eine klare und einfache Sprache.

Die Verordnung selbst hingegen ist alles andere als einsteigerfreundlich und dürfte selbst ambitionierten Jurastudenten noch einiges abverlangen. Auch ergibt sich der vollständige Sinn einzelner Vorschriften erst, nachdem man die Erwägungsgründe der DSGVO zu Rate gezogen hat. Diese sind eine Art Selbstkommentierung des Gesetzgebers, um einzelne Vorschriften näher zu erläutern.

Das Recht auf Auskunft und Löschung

Der Nutzer kann nun bei jeder Stelle, die seine Daten verarbeitet, gem. Art. 15 DSGVO kostenfrei Auskunft über Art und Umfang der gespeicherten Daten, die Verarbeitungszwecke, die Beteiligten der Datenverarbeitung und noch vieles weiteres verlangen. Mehr zu den Auskunftsrechten und wie diese geltend gemacht werden können, erfahren Sie ab Seite 24.

Darüber hinaus haben Verbraucher aufgrund der DSGVO europaweit mehr Rechte bezüglich der Lö-

schung ihrer Daten. Entfällt beispielsweise der Zweck der Verarbeitung, können sie auf Grundlage des Rechts auf Vergessenwerden die Löschung ihrer Daten verlangen. Einfacher ist es auch, Datenspuren im Internet löschen zu lassen (siehe Seite 38).

Umzug gesammelter Daten

Die Datenportabilität, also die Möglichkeit, mit den gesammelten Daten von einem Anbieter zum anderen umzuziehen, ist der geheime Herzenswunsch vieler Internetnutzer. Ob beim Wechsel von einem E-Mail-Service zum anderen oder zwischen Versicherungen, Telefonanbietern oder sozialen Netzwerken wie Facebook und Twitter. In all diesen Fällen hilft Artikel 20 DSGVO: Hiernach ist es Diensteanbietern gestattet, die gesammelten Daten dem Verbraucher zur Verfügung zu stellen oder direkt an den anderen Dienst zu versenden. Damit sollen Nutzer nicht durch komplizierte Wechselmodalitäten möglichst lange an den eigenen Dienst gebunden werden (Lock-in-Effekt).

Die zu versendenden Daten müssen darüber hinaus ein gängiges und interoperables Format haben, das auch vom neuen Diensteanbieter verarbeitet werden kann. Hieraus resultieren für die Diensteanbieter neue Herausforderungen. Die zu übertragenden Daten müssen sowohl auf anderen Systemen kompatibel sein als auch über eine ausreichende Verschlüsselung verfügen, um die Sicherheit der Daten beim Transfer zu gewährleisten.

Umgesetzt ist dies noch längst nicht überall. Prinzipiell müssten zum Beispiel auch Musik-Streaming-Anbieter den neuen Umzugsservice für personenbezogene Daten ermöglichen, sodass Nutzer ihre persönlichen Playlists mitnehmen können. In der Praxis lassen sich die Daten zwar herunterladen, jedoch nicht zum Konkurrenzunternehmen übertragen. Es fehlt an gemeinsamen Standards, interoperablen Systemen und offensichtlich auch am Willen der Streaming-Anbieter.

Privacy by Design und Privacy by Default

pflichtenden Vorgaben des Artikels 25 DSGVO für die Prinzipien *Privacy by Design* und *Privacy by Default* zielen zugleich darauf, dass nur noch das absolut notwendige Minimum an Daten erhoben und die Sicherheit maximiert wird (siehe Seite 16).

Privacy by Design verlangt hierfür, die Sicherheit von Daten bereits bei der Entwicklung von Technologien zu berücksichtigen. Beispiele für die Umsetzung dieser Vorgabe sind die Verwendung von Verschlüsselungstechnologien bei der Datenübertragung sowie die konsequente Pseudonymisierung von Daten.

Privacy by Default verpflichtet Datenverarbeiter dazu, in Programmen, Apps und anderen Anwendungen die datenschutzfreundlichsten Einstellungen vorausgewählt anzubieten. Hier war das Gegenteil lange Zeit Standard. Das bekannteste Beispiel dafür ist das soziale Netzwerk Facebook. Mit jedem Update seiner Nutzungsbedingungen musste man erneut die Verwendung seiner Nutzerdaten anpassen. Hier hat Facebook aufgrund der DSGVO schon etwas nachgebessert.

Hohe Strafen bei fehlender Umsetzung

Nicht alle Rechte sind neu, die mit der DSGVO gekommen sind. Viele Verbraucher stellen sich daher zu Recht die Frage, wie sie gegen Unternehmen vorgehen können, die sich beispielsweise weigern, Auskunft über die gesammelten Daten zu geben oder bei einem geplanten Datentransfer zu kooperieren. Hier sind die immensen Strafzahlungen, die zu den gravierendsten Änderungen in der Datenschutzgrundverordnung gehören, ein wirksamer Hebel zur Durchsetzung der Rechte.

Jeder mutmaßliche Verstoß gegen den Datenschutz kann fortan bei der nächsten Datenschutzbehörde gemeldet werden. Unabhängig vom Sitz des Datenverarbeiters kann sie Ermittlungen aufnehmen und bei vorliegenden Datenschutzverletzungen empfindliche Bußgelder verhängen. Außerdem haben Betroffene unter bestimmten Umständen ein Anrecht auf Schadensersatz (siehe auch Seite 68). (ilk) c't

Lesen Sie mehr in der c't DSGVO 2020.

Mehr Pflichten für Unternehmer

Die DSGVO bringt nach wie vor für Unternehmen eine Fülle an Pflichten mit sich. Grundsätzlich gelten diese vom Einzelunternehmer bis zum global tätigen Konzern gleichermaßen, mit bislang nur einer Ausnahme.

Von Brian Scheuch

Die Datenschutzgrundverordnung behandelt grundsätzlich alle Unternehmer gleich. Eine (teilweise) Privilegierung für Kleinunternehmen wäre zwar wünschenswert gewesen, ist bislang aber nur für die Personengrenze zur Bestellung eines Datenschutzbeauftragten vom Bundestag beschlossen worden (siehe Artikel ab S. 80). Eine weitere Nachbesserung ist seit dem Inkrafttreten vor anderthalb Jahren bisher nicht erfolgt, auch nicht in Hinblick auf die umfangreichen Dokumentationspflichten. Nach wie vor fällt daher auch „der Bäcker von nebenan“ unter die Regelungen der DSGVO, der bei Bestellungen die Kundennamen in eine Liste auf dem Computer einträgt.

Anwendung findet die DSGVO nur dann nicht, wenn die Verarbeitung personenbezogener Daten ausschließlich durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt. Teilweise ist die Abgrenzung zwischen privaten Hobbys und einer Unternehmung jedoch schwierig. Dies gilt beispielsweise für Blogger auf privaten Websites, die ihre laufenden Kosten aber mittels Bannerwerbung finanzieren.

Sobald ein Blogger mit seiner Tätigkeit Umsätze generiert – und seien es auch nur wenige Euro, zum Beispiel durch Google Adsense –, kann er sich nicht mehr auf die Ausnahme des Artikel 2 Abs. 2 DSGVO (private Tätigkeit) berufen. Er ist dann gewerblich tätig und muss sämtliche Pflichten aus der DSGVO erfüllen. Man sollte sich daher vorab genau überlegen, ob man gewerbliche Umsätze generieren will.

Übrigens sind auch Vereine nicht explizit von den Regelungen der DSGVO ausgenommen worden, weshalb sie grundsätzlich dieselben Verpflichtungen haben (siehe Seite 40).

Was ist zunächst zu tun?

Wer die DSGVO bisher eher stiefmütterlich behandelt hat, also diese noch nicht vollständig oder sogar überhaupt nicht umgesetzt hat, sollte möglichst schnell handeln. Inzwischen sind bereits erste Bußgelder verhängt worden, die zum Teil relativ empfindlich waren (siehe Seite 68). Einige Aufsichtsbehörden haben auch ein Bußgeldverfahren eingeleitet, nachdem sie durch aktive Nachfragen des Unternehmens Kenntnis von möglichen Verstößen erlangt haben. Darüber hinaus besteht nach wie vor die Gefahr, abgemahnt zu werden (siehe Seite 68).

Wer bei „null“ anfängt, sollte sich daher zeitnah von „außen nach innen“ vorarbeiten, um potenziellen Abmahnern keinen Ansatz zu bieten und den Aufsichtsbehörden zu signalisieren,

DSGVO-konforme Außendarstellung

Zu den datenschutzrelevanten Bereichen, die „nach außen sichtbar sind“, zählt insbesondere die Datenschutzerklärung (Privacy-Policy) auf der Unternehmens-Website. Eine DSGVO-konforme Datenschutzerklärung ist dabei meist deutlich umfangreicher im Vergleich zur alten Rechtslage (siehe Seite 52).

Weiterhin sollte man überall dort auf der Website, wo der Nutzer aktiv personenbezogene Daten an den Website-Betreiber übermittelt, entsprechende Einwilligungserklärungen per Opt-In einholen und dokumentieren. Klassische Beispiele hierfür sind Kontaktformulare und Newsletter-Anmeldeformulare. Übrigens: Auch vor Inkrafttreten der DSGVO war es bei Newslettern bereits erforderlich, den Nutzer über die Widerspruchsmöglichkeit zu informieren. Diese Pflicht hat ihren Ursprung im Wettbewerbsrecht.

Seit der neuesten Rechtsprechung des europäischen Gerichtshofs (EuGH) ist darüber hinaus insbesondere für die Nutzung von Tracking-Cookies eine aktive Einwilligung der Websitebesuchers erforderlich (siehe Artikel 128).

Interne Prozesse anpassen

Ist die Unternehmung nach außen DSGVO-konform gestaltet, folgen die internen Prozesse. Das Wichtigste sind die Anlage und Pflege eines Verzeichnisses über die Verarbeitungstätigkeiten, die Dokumentation der technisch-organisatorischen Maßnahmen (TOM), der Abschluss von Vereinbarungen zur Auftragsverarbeitung (AVV) mit externen Dienstleistern und gegebenenfalls die Bestellung eines Datenschutzbeauftragten.

Fortlaufende Dokumentation

Die Einhaltung der datenschutzrechtlichen Bestimmungen ist kein

Lesen Sie mehr in der c’t DSGVO 2020.

Ohne IT-Sicherheit kein Datenschutz

Ganz besonders wirkt sich die neue Rechtslage auf die IT-Sicherheit aus, die nun mit der DSGVO elementarer Bestandteil des Datenschutzes ist. Vernachlässigt man die Pflichten, in der technischen Praxis und mit dem Umgang von Daten, drohen hohe Bußgelder.

Von Joerg Heidrich

Das Thema IT-Sicherheit hat in der DSGVO einen weitaus höheren Stellenwert erhalten als bisher im BDSG. Zwar kannte auch das alte Recht schon den Bereich der Datensicherheit. Die neuen Regelungen erweitern jedoch die gesetzlichen Anforderungen an die Technik so erheblich, dass die IT-Sicherheit elementarer Bestandteil des Datenschutzes wird.

Nicht in die DSGVO übernommen wurden die aus dem alten Recht bekannten und inzwischen leicht verstaubt klingenden Grundsätze etwa der Zutritts-, Zugangs- und Zugriffskontrolle. Ersetzt wurden sie durch Begriffe wie Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Sicherheitssysteme. Was hier zu beachten ist, regelt zunächst Art. 5 DSGVO. Danach müssen personenbezogene Daten „in einer Weise verarbeitet werden, die eine angemessene Sicherheit“ der Daten gewährleistet, „einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“.

Konkreter wird hier Art. 32, der die technischen Anforderungen an die Verarbeitung von persönlichen Daten definiert. Diese kann man sich wie eine Waage vorstellen: Auf der einen Seite stehen die

zu schützenden Daten, auf der anderen die zu ergreifenden Maßnahmen. Zu berücksichtigen sind danach unter anderem Faktoren wie der Stand der Technik, die Implementierungskosten, die unterschiedlichen Eintrittswahrscheinlichkeiten sowie die Schwere des Risikos für die Betroffenen.

Wichtig hierbei ist die Tatsache, dass die Risikobewertung aus dem Blickwinkel der einzelnen Kunden und Mitarbeiter zu erfolgen hat – nicht aus der des Unternehmens. Es kommt also primär nicht darauf an, welche Schäden, etwa im Bereich der Reputation, ein Unternehmen oder ein Freiberufler durch eine Datenpanne aufweisen könnte. Entscheidend ist vielmehr, was den Inhabern der Daten, in der Regel Kunden und Mitarbeitern beispielsweise durch ein Datenleck drohen könnte, also etwa durch den Abfluss sensibler Krankendaten oder von Kreditkartennummern.

Backups werden verpflichtend

Von diesem Risiko für die Betroffenen ausgehend, müssen die für die Datenverarbeitung Verantwortlichen „geeignete technische und organisatorische Maßnahmen“ ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Als zu ergreifende Maßnahmen nennt das Gesetz sogar ein paar konkrete Methoden:

- Die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Praktisch bedeutet das nichts weniger, als dass zu verstehen. Es ist also nicht zwingend erforderlich, alle umzusetzen. Ausreichend ist ein überzeugendes Konzept zur IT-Sicherheit, das diese Teile enthalten kann und sollte, aber nicht zwingend muss, sofern das Konzept als Ganzes überzeugt.

Stand der Technik

Ebenfalls neu im Bereich des Datenschutzes sind die Anforderungen, bei der Konzeption des Schutzes der jeweils verarbeiteten Daten den Stand der Technik zu berücksichtigen. Darunter versteht man solche technischen Maßnahmen, die schon zur Verfügung stehen und die sich in der Praxis als geeignet und effektiv bewährt haben. Nicht gemeint sind dagegen die neuesten technischen Entwicklungen aus den Laboren. Der Stand der Technik ist jedoch nicht statisch, sondern muss immer wieder auf neue Entwicklungen geprüft werden, um die Datensicherheit gewährleisten zu können.

Daraus ergibt sich aber nicht, dass sich jedes kleine Unternehmen eine den neuesten und teuersten Anforderungen genügende IT-Infrastruktur einrichten muss. Denn der hier relevante Art. 32 DSGVO sieht unter anderem die Berücksichtigung der Implementierungskosten vor. Hierbei ist hinsichtlich der Auswahl von Hard- und Software eine Abwägung vorzunehmen, die auch zu dokumentieren ist. Sehr hilfreich zur Bestimmung der technischen Aspekte des Themas sind Vorgaben zum Stand der Technik wie die des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder die „Handreichung zum Stand der Technik“ des TeleTrust-Vereins (siehe ct.de/wnsj).

Als praktisches Beispiel für den Stand der Technik hat etwa das Landgericht Würzburg in einer der ersten Entscheidungen zur DSGVO (Az.: 11 O 1741/18 UWG) vom September 2018 ausgeführt, dass beim Erheben von Daten über ein Kontaktformular „zwingend auch eine Verschlüsselung der Homepage erforderlich“ sei. Gemeint ist hier offenbar die SSL/TLS-Verschlüsselung für Websites und insbesondere für Formulare, die laut Gericht stets vorliegen muss.

DSGVO für Website-Betreiber

Betreiber einer Website müssen mit der DSGVO etliche rechtliche Neuerungen berücksichtigen. Wir zeigen Ihnen, wie Sie Ihren Internetauftritt datenschutzkonform gestalten und welche Informationen gemäß dem Datenschutz weder fehlen noch falsch sein dürfen.

Von Nicolas Maekeler

Nicht nur Unternehmens-Websites oder Onlineshops müssen den Anforderungen der DSGVO genügen, sondern in den allermeisten Fällen auch Blogs und Internetseiten von Vereinen. Denn ohne die Verarbeitung personenbezogener Daten, also Informationen jeglicher Art, die sich auf eine zumindest theoretisch identifizierbare natürliche Person beziehen, lässt sich keine Website betreiben.

Erwägungsgrund 30 der DSGVO stellt klar, dass auch IP-Adressen als „Online-Kennungen“ und damit als personenbezogene Daten zu werten sind. Dies deckt sich auch mit der Rechtsprechung des Bundesgerichtshofs (BGH), der im Mai 2017 entschied, dass es sich auch bei dynamisch vergebenen IP-Adressen um personenbezogene Daten handelt. Da der Browser selbst bei einem reinen Lesezugriff auf eine Website die IP-Adresse übermittelt, ist allein schon deswegen der Anwendungsbereich der DSGVO eröffnet.

Wer seine Website immer noch nicht im Zuge der Neuregelung des Datenschutzrechts aktualisiert hat, muss damit rechnen, von Mitbewerbern abgemahnt zu werden. Hohe Streitwerte sind ein Anreiz sowohl für Unternehmen als auch für die anwaltliche Abmahnindustrie, im Web auf die Suche nach Datenschutzverstößen zu gehen.

Datenschutzerklärung

Website-Betreiber müssen ihre Besucher mit einer Datenschutzerklärung (auch „Privacy Policy“) über alle Vorgänge aufklären, bei denen sie personenbezogene Daten verarbeiten. Eine solche Erklärung ist

schon lange obligatorisch, allerdings muss diese nun mehr des DSGVO entsprechen.

Die Datenschutzerklärung muss etwa die konkrete Rechtsgrundlage für die Datenverarbeitung aus Artikel 6 der DSGVO nennen. Rechtsgründe für die Verarbeitung können zum Beispiel die Bearbeitung eines Kaufvertrages in einem Onlineshop sein, aber auch berechtigte Interessen des Website-Betreibers (siehe Seite 16).

Im letzten Fall ist dann auch das konkret verfolgte Interesse zu formulieren. Bei Website-Betreibern kann das beispielsweise das Interesse an der Betriebssicherheit ihrer Homepages sein. Um Angriffe erkennen und abwehren zu können, dürfen sie dafür die IP-Adressen der Besucher für maximal 14 Tage speichern. Darauf muss in der Datenschutzerklärung hingewiesen werden. Ob und wie lange IP-Adressen der Nutzer gespeichert werden, erfährt man beim Webhoster seines Vertrauens.

Website-Betreiber sollten die Besucher darüber informieren, wo auf Besucher beziehbare Daten erhoben und verarbeitet werden. Neben Logfiles zählen auch Geolokalisierungsfunktionen dazu, Registrierungsmöglichkeiten, Kommentarfunktionen, das Abonnement von Newslettern, die Verwendung von Cookies, die Nutzung von Social-Sharing-Funktionen und die Verwendung von Analyse- und Trackingdiensten.

Website-Betreiber müssen auf Basis der DSGVO die Besucher ihrer Site wesentlich ausführlicher über ihre Rechte aufklären als bisher. Bestand zuvor die Pflicht, sie über deren Rechte auf Auskunft, Löschung, Berichtigung von Daten und Widerruf zu informieren, verlangt die DSGVO die Information über das Recht auf Einschränkung der Verarbeitung, das Widerspruchsrecht, das Beschwerderecht bei einer Aufsichtsbehörde sowie das Recht auf Datenübertragbarkeit.

Informationen zum Widerspruchsrecht müssen sogar optisch hervorgehoben werden, etwa durch Fettdruck oder eine Umrahmung. Hat das Unternehmen einen Datenschutzbeauftragten, müssen dessen Kontaktdaten hinterlegt werden.

Die wichtigsten allgemeinen Pflichtangaben können den Checklisten für die Datenschutzerklä-

Letztlich muss die Privacy Policy „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ bereitgestellt werden. Bei umfangreichen Datenschutzerklärungen bietet es sich an, Details auszugliedern und über Links an separater Stelle verfügbar zu machen.

Wer für diese anspruchsvolle Aufgabe nicht gleich einen Datenschutzrechtler beauftragen möchte, kann einen Online-Generator nutzen. Mithilfe dieser Tools kann man sich die DSGVO-konforme Datenschutzerklärung in wenigen Schritten zusammenklicken. Empfehlenswert ist der Datenschutzgenerator von Rechtsanwalt Thomas Schwenke (siehe ct.de/wcc5).

Webformulare verschlüsseln

Bietet die Website Nutzern die Möglichkeit, ihre personenbezogenen Daten in Webformulare einzugeben – zum Beispiel in einem Onlineshop während des Bestellprozesses –, muss dieser Vorgang verschlüsselt ablaufen. Das folgt aus dem in der DSGVO geregelten Grundsatz der Integrität und Vertraulichkeit, wonach personenbezogene Daten in einer Weise verarbeitet werden müssen, „die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung […].“

Webmaster dürfen nach dem Grundsatz der Datenminimierung nur die Daten anfordern, die sie für die jeweilige Aufgabe benötigen (siehe Seite 16). Bei Newsletter-Anmeldungen sollten sie beispielsweise nicht das Geburtsdatum oder die postalische Adresse abfragen. Wie man die Versendung von Newslettern DSGVO-konform gestalten kann, erfahren Sie in dem Artikel auf Seite 124.

Cookies unerwünscht

Der Einsatz von Cookies sorgt schon länger für Verunsicherung bei Website-Verantwortlichen. Viele Sites weisen derzeit durch Banner oder Popup-Fenster Besucher darauf hin, dass sie Cookies

DSGVO für Fotografen

Ob auf Websites oder in Firmenzeitschriften und Flyern: Fotos sind ein gern genutztes Gestaltungselement. Lesen Sie, welche Bilder Sie unter welchen Voraussetzungen machen und veröffentlichen dürfen und welche Anforderungen die DSGVO sonst noch an Fotografen stellt.

Von Nicolas Maekeler

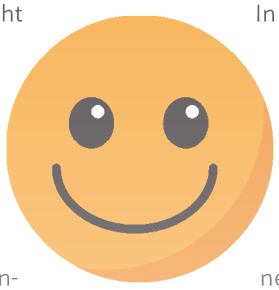
Vor dem 25. Mai 2018, dem Starttermin des neuen EU-weit geltenden Datenschutzrechts, konnten sich Fotografen auf eine solide Rechtslage und eine langjährige Rechtsprechung verlassen. Nun muss umgedacht werden, denn Menschen zu fotografieren, heißt personenbezogene Daten zu verarbeiten. Betätigt der Fotograf den Auslöser seiner Kamera und eine Person erscheint vor der Linse, benötigt er eine datenschutzrechtliche Legitimation. Das gilt in der Regel sogar dann, wenn die fotografierte Person nicht eindeutig zu erkennen ist. Denn bei moderner digitaler Fotografie kann davon ausgegangen werden, dass anhand zusätzlich gespeicherter Daten eine Person identifiziert werden kann. Datum, Uhrzeit und GPS-Daten einer Aufnahme lassen neben dem eigentlichen Bildnis Rückschlüsse zu, wann sich die betroffene Person wo befunden hat. Damit stehen auch Fotografen vor der Aufgabe, die Erfordernisse der DSGVO im Alltag praktikabel umzusetzen.

KUG Ade?

Dass die Personenfotografie gleichzeitig auch eine Datenverarbeitung darstellt, ist im Grunde nichts Neues. Zu Zeiten des alten Bundesdatenschutzgesetzes (BDSG) wurde die Veröffentlichung von Personenfotos als spezialgesetzlicher Bildnisschutz im Kunsturheberrechtsgesetz (KUG) geregelt. Äußerst praxisrelevant ist dabei § 23 KUG, wonach Bilder aus dem Bereich der Zeitgeschichte, von Versammlungen oder solche, auf denen Personen nur als

sogenanntes Beiwerk erscheinen, auch ohne Einwilligung des Abgelichteten veröffentlicht werden können. Und bislang galt der Grundsatz: Wenn Bildnisse nach dem KUG veröffentlicht werden durften, dann war es prinzipiell datenschutzrechtlich auch in Ordnung, entsprechende Fotos zu erstellen.

Seit dem Wirksamwerden der DSGVO wird jedoch darüber diskutiert, ob das KUG überhaupt noch anwendbar ist. Da die DSGVO den Bereich des Datenschutzes abschließend regelt und sich gegenüber anderen Vorschriften nicht mehr „wegduckt", stellt sich die Frage, ob sie bei der Anwendung aufgrund der Normenhierarchie Vorrang gegenüber dem KUG hat.



Im Bereich der gewerblichen, beziehungsweise kommerziellen Personenfotografie besteht weiterhin Rechtsunsicherheit. Der hamburgische Datenschutzbeauftragte Prof. Dr. Johannes Caspar ist der Ansicht, das KUG enthielte bereits keine Rechtsgrundlage für die Datenerhebung, sondern lediglich für die Veröffentlichung der Bilder. Auf der Seite des Gesetzgebers heißt es aus dem Bundesministerium des Innern (BMI) dagegen, für die Veröffentlichung von Fotografien bliebe das KUG erhalten, es werde nicht durch die DSGVO verdrängt.

Journalistische Zwecke

Das Oberlandesgericht (OLG) Köln kommt zu dem Ergebnis (OLG Köln, Beschl. v. 18.06.2018 – Az.: 15 W 27/18), dass die DSGVO für journalistische Zwecke abweichende nationale Gesetze erlaubt. Da der Beschluss nicht nur neue Gesetze, sondern auch bestehende Regelungen erfasst, könne das KUG fortgelten. Allerdings trifft das nur für die Nutzung personenbezogener Daten zu journalistischen Zwecken zu. In Bezug auf nicht journalistisch tätige Fotografen bleibt die Rechtslage weiterhin unklar.

Fotografieren

Möglich ist es laut DSGVO dennoch, wenn eine Erlaubnis vorliegt. Man spricht insoweit von einem Verbot mit Erlaubnisvorbehalt für die Verarbeitung personenbezogener Daten. Demnach ist eine Datenverarbeitung zulässig, wenn entweder eine Einwilligung des Betroffenen oder eine anderweitig gesetzlich geregelte Erlaubnis vorliegt.

Lächeln reicht nicht

In der Prä-DSGVO-Ära wurde ein Lächeln in die Kamera unter gewissen Umständen als konkludentes Einverständnis, also als stillschweigende Willenserklärung gewertet. Jetzt muss eine datenschutzrechtliche Einwilligung freiwillig, bestimmt, in informierter Weise und unmissverständlich eingeholt werden. Dafür sind dem Betroffenen gegenüber zunächst alle notwendigen Informationspflichten zu erfüllen. Im Zweifelsfall muss man nachweisen können, dass eine Einwilligung tatsächlich erteilt wurde. Der Fotograf sollte daher alles schriftlich dokumentieren. Ein unterschriebenes Einwilligungsformular nebst Datenschutzerklärung ist nötig.

Vorsicht vor Einwilligung

Allerdings sollte man nur auf die Einwilligung zurückgreifen, wenn man sich auf keine andere Rechtsgrundlage berufen kann. Denn diese kann frei widerrufen werden. Schlimmstenfalls müssten dann bereits veröffentlichte Fotos umständlich gelöscht oder geschwärzt werden. Insofern ist die Einwilligung ein eher unsicheres Instrument für Fotografen. Nach dem KUG war der Widerruf von Einwilligungen in Fotoaufnahmen, abgesehen von strengen Ausnahmen, fast unmöglich. Es mussten schon wichtige Gründe hierfür vorliegen, was der Rechtssicherheit zugutkam. Der Widerruf einer Einwilligung nach DSGVO kann hingegen ohne die Angabe von Gründen erfolgen.

Lesen Sie mehr in der c't DSGVO 2020.