Der Schutz der Daten – DSGVO im Überblick und in der Praxis (Teil 2)

von **Peter Klatecki**

Datenschutz nach der DSGVO betrifft alle Bürger der EU; ausnahmslos. Als Betroffener, dessen Daten geschützt werden, und natürlich als Unternehmer oder Mitarbeiter von Betrieben, die diese Verordnung erfüllen müssen. Was ist wirklich wichtig, was braucht man für die tägliche Arbeit?

In Teil 1 (PW 8/2018) ging es um die Grundlagen, folgend aus den Regelungen der DSGVO. Hier folgt die Bedeutung für die Praxis, grundlegende Maßnahmen und Umsetzungsvorschläge. Anmerkung: Eine abschließende und rechtssichere Darstellung ist leider nicht möglich, da letztinstanzliche Urteile erst viel später zu erwarten sind.

Technische und organisatorische Maßnahmen (TOM)

Es gibt zwei Grundforderungen im aktuellen Datenschutzrecht:

„Privacy by Design", also Schutz durch Technikgestaltung. Dahinter steht der Gedanke, dass Datenschutz am besten zu gewährleisten ist, wenn das im Verarbeitungsvorgang technisch berücksichtigt und integriert ist.

„Privacy by Default", Schutz durch datenschutzfreundliche Voreinstellungen. Danach sind Grundeinstellungen eben schutzfreundlich vorzusehen. Hiermit sollen insbesondere jene Nutzer geschützt werde, welche sich weniger mit der Technik auskennen und befassen und dadurch eventuell Einstellungen wählen, die nicht ihren Wünschen entsprechen.

Beide Forderungen zielen aber auch auf grundsätzliche Konzepte wie die Nutzerauthentifizierung, Pseudonymisierung, Anonymisierung, Verschlüsselung und Weiteres.

Beispiel: DNS

Als einfaches Beispiel für „Privacy by Default" ist die Voreinstellung des DNS-Servers im (firmen-)eigenen Router zu nennen.

DNS: Das Internet funktioniert mithilfe von Adressen im TCP/IP-Protokoll. Diese werden durch Nummern gebildet. Jeder Anbieter (Server) im Internet muss über eine eindeutige IP-Adresse erreichbar sein. Menschen merken sich (Domain-)Namen allerdings viel leichter. Die Webseite des Verlages ist im Internet über die V4-IP 136.243.165.142 zu erreichen. Die Anfrage in einem Browser nach „www.vulkan-verlag.de" wird vom angesprochenen DNS-Server in diese Nummer übersetzt. Dann kann die Seite aufgerufen und dargestellt werden.

Nun kann das Nutzerverhalten an dem jeweils zuständigen DNS-Server protokolliert und ausgewertet werden, was auch ausführlich geschieht.

IBM, die Global Cypher Alliance und Andere betreiben seit einiger Zeit eigene DNS-Server unter dem Namen Quad9, die ausdrücklich keinerlei Daten sammeln und auch Phishingseiten oder Seiten mit Malware (Schadsoftware) blockieren sollen. Der Betrieb finanziert sich durch Spenden und durch Beiträge der öffentlichen Hand.

In jedem Router (und auch in jedem Endgerät) kann der DNS-Server manuell voreingestellt werden. Die Adresse der Quad9 Server lautet: 9.9.9.9 (IP V4) bzw. 2620:fe::fe (IP V6). Ein weiterer Anbieter von geschützten DNS Diensten ist Cloudflare. Die versprechen ebenso „Privacy First". Die Adressen der Cloudflare Server lauten: 1.1.1.1 (IP V4) und 2606:4700:4700::1111 (IP V6). Die gewählten Adressen erinnern vermutlich nicht zufällig an den Server von Google (8.8.8.8).

Wer all diesen Servern nicht vertraut, kann es mit den Servern von OpenDNS versuchen. Bei den Hauptadressen (IP-V4 208.67.222.222 und 208.67.220.220) wird Schutz gegen Phishing versprochen. Familienschutz gibt es über 208.67.222.123 und 208.67.220.123. Dort werden dann zusätzlich die s.g. „Erwachsenenseiten" blockiert. OpenDNS gehört inzwischen allerdings zum US-Unternehmen Cisco.

Beispiel: Strava

Ein Beispiel, wie unvorteilhafte Voreinstellungen ernsthafte Konsequenzen haben können, zeigt das Beispiel des Social-Network Strava. Strava sammelt die GPS-Daten von Fitnesstrackern. Benutzer können über diese Geräte ihre Lieblingsrouten für das tägliche Jogging oder ihre Fahrradausflüge an das Network melden und damit den anderen Benutzern bekannt machen. Strava erzeugt daraus eine Weltkarte mit den eingezeichneten Strecken. Auf dunklem Hintergrund werden die Wege als „helle" Linien dargestellt. Je heller die Linie, desto mehr Personen nutzen diese Strecke.

Nun nutzen auch Soldaten solche Tracker bei ihrem täglichen Training, teilweise haben sie diese vom Dienstherrn erhalten, um die Fitness der Truppe zu fördern. Befindet man sich im Auslandseinsatz ist die Wahl der Strecke eingeschränkt, unter Umständen sogar gefährlich. Auf Strava waren plötzlich Laufstrecken zu sehen, welche eindeutig auf militärische Anlagen in Krisengebieten schließen ließen. Angezeigt wurden Routen in der Einöde von Afghanistan und anderen Konfliktgebieten. Die Soldaten liefen eben um ihr Lager herum, immer am Zaun lang. Es waren auch Rückschlüsse auf die Art der Einrichtung möglich, indem etwa abgelaufene Start- und Landebahnen zu erkennen waren. Eine namhafte Anzahl von Geheimbasen des Militärs wurde so offengelegt.

Strava, der Dienst selbst, verweist darauf, dass man die Einstellung ja auf „Privat" ändern könne. Diese Strecken würden dann nicht veröffentlicht. Mit dieser Einstellung ist die Nutzung des Netzwerks jedoch nahezu ohne Sinn, die Protokollierung könnte dann auch unterbleiben.

Sicherheit der Verarbeitung

Die genutzte Technik muss nach dem aktuellen Datenschutzrecht risikoadäquat, unter Beachtung des „Stands der Technik" sein, so die Forderung. Ist bei einem freien Autor noch ein Router seines Providers als ausreichender Schutz anzusehen, gilt das mit Sicherheit nicht für das Gesundheitswesen. Hier ist als Grenze/Zugang zum Internet eine deutlich komplexere Router/Firewall-Kombination erforderlich. E-Mail-Verschlüsselung und die Nutzung von VPN-Zugängen beim Zugriff auf Unternehmensinformationen sind Standard. Die Unternehmens-IT muss die Vertraulichkeit (beschränkter Zugriff), die Integrität und die Verfügbarkeit (Backup) von Daten sicherstellen.

Mobile Geräte

Notebooks, Tablets, Smartphones, USB-Sticks und Rechner in betriebsfremder Umgebung unterliegen einer höheren Gefährdung bzgl. Diebstahl und Ausspähung. Die Benutzung darf nur nach Passwort / Pin / Biometrie möglich sein. Die Geräte sollten nur für den Einsatzfall notwendige Daten enthalten und Verschlüsselung (Bitlocker/Veracrypt) nutzen. Auch sollte nur für den Einsatzfall notwendige Software installiert sein.

Die Rechner sind beim Verlassen immer zu sperren und bei Nichtbenutzung sicher zu verwahren (vor fremdem Zugriff wegschließen). Unmittelbare Sperrung des Rechners, ohne die Programme zu beenden, erreicht man durch die Tastenkombination WIN+L (Windows). Nach erneutem Login ist ein Weiterarbeiten direkt möglich. Unter Mac OS kann man Ähnliches erreichen, indem man unter „Einstellungen" die Eingabe eines Passwortes nach Bildschirmschoner oder Bildschirmabschaltung verlangt. Der Bildschirm kann mit der Tastenkombination Shift+Ctrl+Eject abgeschaltet werden.
Die Umsetzung obiger Maßnahmen schützt nicht nur persönliche Daten, sondern auch gespeicherte Firmengeheimnisse.

Datenschutzverletzungen und Verstöße

Typische Schwachstellen

An erster Stelle sind hier die Mitarbeiter zu nennen. Diese müssen regelmäßig unterwiesen und auf entsprechende Verhaltensregeln eingeschworen werden. Die Mitarbeiter sind auf die dargestellten Aspekte im Folgenden zu sensibilisieren.

Eine große Schwachstelle ist die Entsorgung von Dokumenten mit personenbezogenen Daten, ohne diese zu schreddern. Für Hacker und Detektive ist der Papierabfall immer ein erfolgversprechender Angriffsvektor und erste Wahl für den Einstieg in das sogenannte Social-Engineering. Es sind viele Informationen zu finden, welche das Bild von Personen ergänzen können (Abonnements, Bankverbindungen, Kundenbeziehungen, politische Meinung usw.).

Eine weitere Gefährdung stellen die heutigen mobilen Speichermedien dar (USB-Sticks, Speicherkarten und sonstige Datenträger), und dies gleich in mehrfacher Hinsicht. Diese Datenträger werden leicht verloren oder gestohlen und damit ist keine Kontrolle mehr über die gespeicherten Daten möglich, es sei denn effektive Verschlüsselung verhindert den Zugriff.

Ein beliebter Angriffsvektor, um Schadsoftware in Unternehmen einzuschleusen, ist nach wie vor einen speziell präparierten USB-Stick im Unternehmensbereich zu „verlieren". Angefangen mit dem Parkplatz bis hin zum Waschraum der Geschäftsleitung. Irgendjemand wird diesen finden und am Firmen-PC neugierig prüfen, was wohl darauf zu finden ist. Oder Betriebsfremde haben die Möglichkeit, Sticks direkt an Rechnern zu platzieren (etwa bei Wartung oder Reinigung). Je nach Berechtigungsstufe können die Schäden durch dann automatisch ausgeführte Software erheblich sein. Auf diese Art wurden 2010 Uranzentrifugen im Iran zerstört (StuxNet), das interne Netzwerk der Anlage war nicht mit der Außenwelt verbunden.

Auf der anderen Seite können durch mobile Datenträger unbemerkt große Datenmengen aus dem Unternehmen gebracht werden.

Viele Daten werden versehentlich offengelegt, indem z. B. beim E-Mail-Versand eine falsche Adresse angegeben wird, ohne es zu bemerken, oder leichtfertig „an alle" geantwortet wird.

Von Seiten der Infrastruktur ist ein zu kompliziertes, vielleicht auch historisch gewachsenes Rechtesystem in Servern zu nennen. Damit können Mitarbeiter unbeabsichtigt Zugriff auf Daten erlangen, für die sie keine Berechtigung besitzen sollten.

Natürlich muss die Datensicherung gewährleistet sein und eine Erfolgskontrolle die Wiederherstellung im Fehlerfall sicherstellen. Es gilt: keine Datensicherung, kein Mitleid!

BYOD (Bring Your Own Device)

Hierunter sind nicht nur die privaten Geräte der Mitarbeiter zu fassen, sondern auch Geräte von Geschäftspartnern, Kunden und Lieferanten etc. Diese Geräte entziehen sich der Kontrolle durch die IT-Abteilung. Möchte man diesem Personenkreis Zugang zum Internet über die firmeneigene Infrastruktur ermöglichen, so sind diese Geräte mit spezieller Firewall vom Produktionsnetz zu trennen. Für die WLAN-Struktur gilt das Gleiche. Hier wird dann nur identifizierten Geräten und Benutzern Zugriff gestattet.

Fehler beim Datenschutz

Eindeutige Fehler liegen in folgenden Fällen vor:

Es ist ein unkontrollierter Zugang zu Betriebsräumen, und damit zu Rechnern am Firmennetz, möglich. In diesen Büros liegen vielleicht noch vertrauliche Unterlagen offen auf dem Tisch. Schwache Passwörter und deren „Speicherung" auf Zetteln unter der Tastatur leisten ein Übriges. Schlecht gewartete Hard- und Software erlaubt ungewollten Zugriff auf Informationen.

Am Telefon oder im Gespräch werden nicht nur unbedingt nötige Informationen weitergegeben. Für einen Anrufer ist es nicht von Belang, aus welchem Grund jemand nicht zu erreichen ist. Diskussionen oder Informationsaustausch auf dem Flur sollten sich nicht um Interna und schon gar nicht um personenbezogene Daten drehen.

Es befinden sich unnötige Daten auf Arbeitsrechnern. Diese Daten sind, nachdem kein Zugriff mehr nötig ist, in der firmeninternen Serverstruktur zu archivieren und vom Arbeitsrechner zu löschen.

Angriffsszenarien

Entgegen der allgemeinen Ansicht finden typische Angriffe auf Daten im Unternehmen nicht durch technisches Hacking,

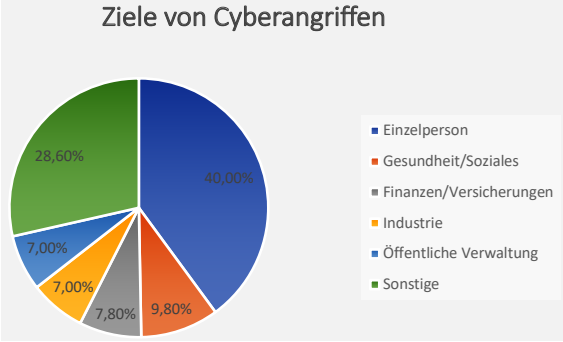

Bild 1: Ziele von Cyberangriffen (Quelle: hackmageddon.com)

die Ausnutzung von Softwarefehlern und Schwachstellen über die Netzwerkverbindung, also über das Kabel, statt. In mehr als 90 % aller Fälle geschieht dies über das s. g. Social-Engineering (später Social Hacking), über Datenklau mithilfe von Datenträgern oder durch persönlichen Einsatz. Social-Engineering verfolgt den Ansatz durch spezifische, sehr persönliche Ansprache den Nutzer zu bestimmten Handlungen zu überreden. Je spezifischer die Informationen über eine Person sind, desto einfacher kann dieses Ziel in der Regel erreicht werden.

Nur der Rest (< 10 %) erfolgt über das Einschleusen von Trojanern, Viren oder Erpressungssoftware (s. g. RansomWare) durch Massenmails. Gegen die meisten dieser Angriffe hilft die Sensibilisierung und Schulung von Mitarbeitern ungemein, da alle aktuellen E-Mail-Programme angehängte Software oder Skripte nicht mehr automatisch ausführen. Der Angreifer ist hier immer auf die Mithilfe des Benutzers angewiesen, um diese Routinen zur Ausführung zu bringen oder eine bestimmte Webseite zu besuchen und Code von dort zu starten. Durch die unspezifische Ansprache des Nutzers sind diese Versuche normalerweise leicht zu identifizieren.

Die nächste Stufe sind automatisierte Angriffe, welche auf bestimmte Hardware- oder Softwarefehler zielen, um Zugriff auf die Datenbestände zu erlangen. Dies ist das erwartete technische Hacking. Es ist unstrittig, dass in Schubladen von Behörden oder auch kommerziell agierenden Unternehmen s. g. Zero-Day-Exploits liegen und auf ihren Einsatz warten. Diese werden mit „Zero-Day" bezeichnet, da sie noch nicht im Einsatz waren und so auch nicht öffentlich wurden. Die Schwachstelle des Zielsystems ist in der Öffentlichkeit unbekannt und demzufolge gibt es dagegen in der Regel keinerlei Verteidigung oder Softwareupdates, welche die Lücke schließen könnten.

Die israelische Firma Cellebrite bietet Software an, mit der angeblich jedes Smartphone geknackt werden kann, auch die neuesten Apple Modelle. Dies bedeutet Kenntnis über Sicherheitslücken, die dem Hersteller selbst nicht bekannt sind, sonst könnten diese durch ein Update geschlossen werden. Nach eigenen Angaben machen sie vor einem Verkauf der Software so eine Art „Ethikprüfung". Eine Abgabe an zweifelhafte Kunden soll so unterbunden werden. Behörden können gegen Bezahlung auch einzelne Geräte entsperren lassen. Nach eigenen Angaben hat Cellebrite ca. 15.000 Kunden aus dem Bereich Strafverfolgung und Militär.

Die Ziele aller sonstigen Angriffe liegen hauptsächlich im gewinnen (stehlen) von Daten oder in der Beschädigung der Reputation des Unternehmens. DDoS Attacken (Distributed Denial of Service) machen Webzugänge/Webseiten durch Überlastung zeitweise unbenutzbar und schaden so. Man denke nur an Online Casinos. In allen Fällen sind die Angriffe finanziell motiviert. **Bild 1** zeigt den prozentualen Anteil verschiedener Angriffsziele. Nach den Einzelpersonen (40 %), führt der Bereich Gesundheit/Soziales (9,6 %), gefolgt von Finanzen/Versicherungen (7,8 %) und der Industrie (7,0 %) sowie der öffentlichen Verwaltung/Verteidigung/Sozialsysteme (auch 7,0 %).

Mitarbeiterschulung und Sensibilisierung ist Aufgabe der Firmen-Orga. Es ist Aufgabe der IT-Infrastruktur, technisch ein möglichst hohes, dem Bedarf angepasstes Schutzniveau zu bieten. Aus den Forderungen der DSGVO kann man durchaus die Pflicht zur Bereitstellung ausreichender Finanzmittel ableiten.

Was tun, wenn man Verstöße bemerkt?

Nach Artikel 33 DSGVO sind Verstöße gegen den Datenschutz innerhalb von 72 h der zuständigen Aufsichtsbehörde bekannt zu machen. Diese Pflicht entfällt, wenn der Verstoß „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt". Ein Beispiel: eine Personalakte wird, ohne sie zu schreddern, in den Papiermüll entsorgt. Dort verbleibt sie mehrere Stunden, kann aber noch vor der Abholung (Entsorger) wieder geborgen werden. In diesem Fall kann eine Meldung wohl unterbleiben. Die Akte hat das Firmengelände nicht verlassen, die erhaltene Aufmerksamkeit in der Zeit im Papiermüll dürfte gegen Null gehen. Damit bestand keine Gefahr für die Rechte des Betroffenen.

Allgemein gesprochen: Jeder einzelne Mitarbeiter ist gefordert, falls er Verstöße bemerkt. Bei personellen Vorgängen, etwa die mündliche Weitergabe von geschützten Daten, ist der jeweilige Vorgesetzte zu informieren. Bei IT-bezogenen Vorfällen die EDV-Abteilung. Weiterhin sollte der Datenschutzbeauftrage informiert werden. Dort kann jeweils entschieden werden, ob eine Meldung an die Landesbehörden notwendig ist oder nicht. Durch die knappe Fristsetzung (mit erheblicher Strafandrohung s.u.) ist in solchen Fällen immer umgehendes Handeln erforderlich, um drohende schmerzliche Konsequenzen für das Unternehmen und damit u. U. für den eigenen Arbeitsplatz zu vermeiden.

Bußgelder

Je nach Verstoß, je nach verletztem Artikel reichen die Bußgelder bis zu € 10 Mio. /2 % des weltweiten Jahresumsatzes oder bis zu € 20 Mio. /4 % des weltweiten Jahresumsatzes, je nachdem was höher ist. Die eigentliche Höhe legen die Datenschutzbehörden im Einzelfall fest. Gefordert in der Verordnung ist aber, dass Bußgelder in jedem Fall „wirksam, verhältnismäßig und abschreckend" sein sollen. Damit sind, unternehmensabhängig, deutliche Bescheide zu erwarten.

(DSGVO-) Abmahnungen

Die befürchtete Abmahnwelle ist bis heute (in Deutschland, Stand Oktober 2018) ausgeblieben. Dies mag daran liegen, dass es eine direkte Abmahnung nach DSGVO

wahrscheinlich gar nicht gibt. Bei dem Instrument der (kommerziellen) Abmahnung handelt es sich um einen Weg, welcher nur in Deutschland gegangen werden kann. Wenn, dann sind Abmahnungen nach Wettbewerbsrecht, speziell dem Gesetz gegen den unlauteren Wettbewerb, zu erwarten. Eben wie bisher auch. Allerdings ist Datenschutz ein Menschenrecht und nicht ein Recht als Marktteilnehmer.

Einige Juristen vertreten auch die Auffassung, dass die DSGVO eine s. g. abschließende Regelung darstellt. Das heißt sie enthält alle Sanktionsmöglichkeiten. Damit bliebe dem Abmahnwilligen bei festgestellten Verstößen die Meldung an die Datenschutzbehörden. Ob die DSGVO wirklich „abschließend" ist, ist jedoch aktuell noch strittig.

Generell bei Abmahnungen gilt: Die Abwehr einer Abmahnung sollte immer über einen Anwalt erfolgen. Zuerst muss geprüft werden, ob der behauptete Verstoß überhaupt vorliegt und dann, ob die Abmahnung selbst einwandfrei ist. Auf keinen Fall sind unmittelbar Unterlassungserklärungen zu unterschreiben (die gelten lebenslang) oder Zahlungen, auch keine Teilzahlungen, zu leisten. Das könnte schon eine Anerkenntnis darstellen. Ist der Hinweis auf einen abmahnfähigen Regelverstoß berechtigt, sollte dieser Verstoß umgehend beseitigt werden und anschließend eine eigenformulierte (Anwalt) Unterlassungserklärung abgegeben werden.

Merke auch: Eine unberechtigte Abmahnung stellt selbst einen Wettbewerbsverstoß dar!

Kritik an der Verordnung

In der Presse wurde Kritik laut, dass z. B. ein Blogger mit ein paar Euro Einkommen im Monat (nahezu) die gleichen Pflichten hat wie ein multinationaler Konzern. Wenn man Datenschutz als Menschenrecht begreift, können die Anforderungen auch nicht abweichend geregelt sein. Natürlich muss dieser Blogger keine so großen Investitionen in Abläufe, Mitarbeiterschulung und Hardware vornehmen wie ein Konzern, aber er muss den Datenschutz nach DSGVO in seinem Verantwortungsbereich gewährleisten. Erläuterungen findet man im Erwägungsgrund 13.

Dazu handelt es sich bei der DSGVO um regionale (EU) Regeln, die auf ein globales Netz anzuwenden sind. Dies sorgte bei den EU-Unternehmen für Stress, meistens auch für Aktionismus, während Unternehmen außerhalb der EU doch deutlich entspannter mit dem Thema umgehen.

Nach der EU-Verordnung für die Verarbeitung von Daten von Personen vor dem 16. Lebensjahr hat immer die Einwilligung der Eltern (Erziehungsberechtigten) vorzuliegen. Die Diskussionen mit den Eltern und ihren pubertierenden Kindern, wenn diese z. B. ein neues Spiel auf ihrem Smartphone spielen möchten und dafür Daten abgeben sollen, sind bestimmt amüsant. Diese Altersgrenze liegt in vielen Ländern darunter, in den USA beispielsweise bei 13 Jahren. Das Social-Network SnapChat hat eine deutliche Anzahl von Nutzern, welche jünger als 16 Jahre sind. Nach dem 25. Mai hätten all diese Konten bis zur ausdrücklichen Einwilligung durch die Eltern gesperrt werden müssen. Davon ist mir nichts bekannt. Es bleibt natürlich auch die Frage, ob bei gemeinsamem Erziehungsrecht auch beide Elternteile Einverständnis erklären müssen. Diese rechtliche Klärung wird spannend sein.

Auswirkungen

Die Sache mit den Fotos

Digitalfotografie ist Datenverarbeitung nach DSGVO, wenn Gesichter von Personen abgebildet sind oder Personen an anderen Merkmalen eindeutig identifiziert werden können. Diese Fotografie ist erlaubt für „hauptberufliche, angestellte Fotojournalisten".

Also für die freien Journalisten und für die anderen nicht?

Vor dem 25. Mai wurde dies durch das Kunst-Urheber-Gesetz (KUG), erlassen 1907, letzte Änderung von 2001, geregelt. Bilder und deren Veröffentlichung waren erlaubt, wenn einzelne Personen nicht erkennbar als Hauptmotiv dargestellt wurden. Also in Berichten von Demonstrationen, über Konzerte und Festivals oder bei Dorffesten usw. Dieses Gesetz stand über dem Recht auf das eigene Bild, wenn man selbst nur „zufällig" mit abgebildet wurde. Personen des öffentlichen Lebens und Interesses, Prominente, müssen dies sowieso dulden.

Das KUG sollte bei Kunst und Meinungsfreiheit weiter Vorrang haben. Es gab die Möglichkeit, dies „offiziell" zu regeln, nach Öffnungsklausel 85. In Schweden ist es so umgesetzt worden. Immerhin hat das Bundesinnenministerium am 14. Mai in einer Stellungnahme bekannt gegeben, dass das KUG weiterhin Vorrang haben soll. Eine solche Stellungnahme ist allerdings juristisch nicht bindend.

Im privaten Bereich (also ohne wirtschaftlichen Hintergrund) ist die DSGVO ja ohnehin nicht anwendbar. Damit ist ausdrücklich die private Verwendung sozialer Netze davon auch nicht erfasst. Hochladen und damit Veröffentlichen von Bildern aus dem Urlaub, von daheim oder auf der Straße ist nach wie vor vom KUG gedeckt. Bilder mit einzelnen oder einer kleinen Gruppe von Personen als Hauptmotiv unterliegen wie bisher dem Recht am eigenen Bild (Persönlichkeitsrecht) und diese müssen ihr Einverständnis zur Veröffentlichung erklären.

Rechtlich in den Vordergrund tritt in der beruflichen (= nicht privaten) Fotografie immer mehr die Datenverarbeitung zur Erfüllung von Verträgen oder zur Wahrung berechtigter Interessen, die ausdrückliche Einwilligung tritt zurück. Soll ein Fotograf etwa eine Hochzeit ablichten oder Passfotos anfertigen, bedarf es keiner gesonderten Einwilligung des oder der Betroffenen fotografiert zu werden. Zur Veröffentlichung, z. B. im Schaufenster oder auf der Webseite des Fotografen, hingegen schon.

Bilder auf Webseiten vom Sommerfest, von nicht kommerziellen Vereinen, sollten unproblematisch sein (berechtigtes Interesse). Es ist jedoch eine gute Idee, eine ausdrückliche Einwilligung von den in der Öffentlichkeit handelnden Personen (etwa dem Vorstand) einzuholen. Die Meldung zur Veröffentlichung an eine Tageszeitung mit einem Bild wäre dann rechtlich gesichert. Bei Bildern von Kindern (Kita) ist die Einwilligung der Erziehungsberechtigten vor der Veröffentlichung, besser vor dem Fotografieren, einzuholen. Dies ist aber keine Folge der DSGVO, das galt bisher auch.

Am 18.06.2018 urteilte das Oberlandesgericht Köln hierüber (Az.: 15 W 27/18). Als Kern des Urteilsspruches kann man sagen: Fotos als Dokument der Zeitgeschichte oder im öffentlichen Interesse unterliegen nicht der DSGVO sondern dem Kunsturheberrechtsgesetz als übergeordnetem Recht, möglich nach Klausel 85 DSGVO. Unter besonderer Berücksichtigung der Pressefreiheit gelte hier ausschließlich deutsches Recht.

Einwilligung nach DSGVO ist also nötig, wenn:

- der/die Abgebildete(n) erkennbar ist/sind und keine Ausnahme des KUG greift
- das Foto einem unbeschränkten Personenkreis zugänglich gemacht wird
- wenn Kinder fotografiert werden, intime Situationen abgebildet sind, sensible Daten erkennbar sind

Einwilligung ist nicht nötig, wenn:

- eine der Ausnahmen des KUG greift (Person der Zeitgeschichte, Personen als Beiwerk etc.)
- ein berechtigtes Interesse des Veranstalters oder Fotografen besteht (etwa bei Vereinen oder Sportveranstaltungen)

Absolut tabu ist (ohne Einwilligung):

- wenn Kinder fotografiert werden, intime Situationen abgebildet sind, sensible Daten erkennbar sind oder eine Person diskreditiert wird.

Das „WhatsApp-Problem“

Dies nur als Bezeichnung, es umfasst auch verschiedene andere Messenger, Social-Media Dienste, Online-Spiele usw., welche ungefragt Daten transferieren.

Das Adressbuch (z. B.) eines Nutzers mit allen Kontakten einschließlich E-Mail-Adresse und Telefonnummern wird an WhatsApp und damit an Facebook übertragen. Es ist völlig unklar, wohin und zu welchem Zweck diese Daten übertragen und verarbeitet werden.

Aus Datenschutzsicht ergeben sich folgende Probleme:

Die ausdrückliche Einwilligung jedes einzelnen Betroffenen dazu fehlt (in der Regel), das Informationsrecht des jeweiligen Betroffenen kann nicht erfüllt werden („Download my Data“ ist nicht ausreichend), das Recht auf „Vergessen werden“ und das Recht auf „Übertragen werden“ können nicht erfüllt werden. Außerdem ergibt sich durch den Datentransfer in die USA ein geringeres Schutzniveau. Seit 2016 verschlüsselt WhatsApp „Ende zu Ende“ und wirbt damit. Den wenigsten Nutzern ist bekannt, dass nur die Texte und nicht übertragene Bilder verschlüsselt werden. Die Bundesbehörden in den USA werden vermutlich nach wie vor Zugriff auf die Texte haben. Amerika hat immerhin sogar Exportbeschränkungen für Verschlüsselungssoftware erlassen und das Schutzniveau beschränkt. Entsprechende Software, auch Open-Source, wird vorab vom BIS (Bureau of Industry and Security) überprüft.

Es sind keinerlei Maßnahmen bekannt, welche diese Schwierigkeiten abschließend beseitigen können, um DSGVO-konform zu werden.

Dies führt dazu, dass Firmen dazu übergehen, die Installation und Nutzung von WhatsApp auf Firmen-Handys zu untersagen. Continental setzte es im Juni dieses Jahres um und untersagte die Nutzung auf mehr als 36.000 Mobilgeräten.

Die Hinweis-Flut und der Einwilligungs-Tsunami

Seit dem 25. Mai werden die E-Mail-Postfächer überschwemmt mit Meldungen, man möchte doch bitte bestätigen, dass man die „wichtigen Nachrichten“ (Newsletter) weiter erhalten möchte; also die Frage nach dem Re-Opt-In. Dabei war den meisten handelnden Unternehmen wohl nicht bewusst, dass einmal nach dem alten BDSG gültig eingeholte Einwilligungen weiter ihre Gültigkeit behalten. Für die Empfänger dieser Mails ist es auf jeden Fall interessant, bei wie vielen solcher Newsletter man sich bereits „angemeldet“ hatte. Meistens war es doch überraschend. Bei einigen wurde mit Sicherheit erst die Einwilligung erteilt, indem man den „weiteren Bezug“ bestätigte. Ähnlich inflationär sind die Anfragen nach der Erlaubnis zum Setzen von Cookies beim Besuch von Webseiten.

Die große Anzahl von beidem führt dazu, dass Benutzer genervt diese Meldungen einfach reflexartig mit OK bestätigen um sich nicht aus Versehen von Informationen auszusperren oder die aufgerufene Webseite nutzen zu können, ohne sich mit den angezeigten Datenschutzinformationen zu befassen und diese Genehmigung etwa einzuschränken. Die Schutzabsicht der Verordnung, der Betroffene als Herr über seine Daten, wird damit natürlich völlig unterlaufen.

Warum nun das Ganze?

Daten sind das neue Gold. Inzwischen werden unfassbare Mengen an Informationen täglich gesammelt, ausgewertet und gespeichert. Über jeden, der jemals das Internet genutzt hat, gibt es Profile.

Google ist keine Suchmaschine, Facebook ist kein Darstellungsmedium, WhatsApp ist keine Kommunikationssoftware. Dies sind Werbeagenturen mit Zusatzfunktionen, um die Nutzer zu gewinnen und zu halten. Anders sind die jährlich gemeldeten Milliardengewinne mit kostenfreien Diensten auch nicht zu erreichen.

Je spezifizierter ein Datensatz ist, desto wertvoller ist er für die Werbeindustrie. **Tabelle 1** zeigt die Kosten eines Kennzeichens beim Erwerb von Datensätzen. Auch wenn die genannten Preise vielleicht nicht exakt sind, so verdeutlichen sie doch die Relationen.

Je gezielter Werbung platziert wird, desto teurer ist die Einblendung. Dafür werden heute keine s. g. Cookies mehr benötigt. Die bisher auf dem Rechner abgelegten kleinen Textdateien zum Verfolgen des Nutzers werden durch aktuellere Methoden abgelöst. Stichworte sind hier

Tabelle 1: Quelle: WDR Mediathek: Die tägliche Datenspur, Wie das digitale Ich entsteht

Rabattkarte X vorhanden	€ 0,80
Politikinteresse	€ 1,40
Wohnort	€ 5,00
Jobwechsel	€ 5,50
Umzug	€ 6,20
Abnehmwunsch	€ 8,00
Kinder	€ 8,40
Heirat	€ 8,80
Krankheit	€ 19,00

Browser-Fingerprinting und Machine-Fingerprinting. Hierbei wird aus verschiedenen Parametern (Hardware, installierte Software, Betriebssystem, Patchlevel u. a.) eine möglichst eindeutige Identifikationsnummer gebildet. Der Werbeindustrie kommt hier entgegen, dass Computer (PC, Tablet, Smartphone usw.) fast immer von nur einer Person benutzt werden. Aber selbst wenn nicht, ist eine Identifikation über das Login und die persönliche Art die Tastatur zu bedienen (Anschlagsrhythmus) möglich. Als kleiner Test dieser Funktionen eignen sich für jeden persönlich außergewöhnliche Suchbegriffe, etwa Treppenlift oder Brautkleid. Ein paar Seiten im Ergebnis der Suche anklicken und man wird erstaunt sein, wie lange auf beliebigen Webseiten passende Werbung eingeblendet wird. (Kennzeichen Heirat: € 8,80, Krankheit wie gesagt: € 19,00).

Das größte Problem ist aber die Korrelation von Daten. Ein einziges Datum lässt noch keine Aussage über die Person zu, aber jeder weitere Aspekt verfeinert das Bild. Familie, Beruf, Einkommen, Hobbies, Vorlieben im Urlaub, Kaufverhalten, Zahlungsmethoden, Kunstverständnis, Bildungsstand, …, je detaillierter das Bild, desto besser die Voraussage. Google ist heute in der Lage eine prozentuale Wahrscheinlichkeit anzugeben, mit der ein beworbenes Produkt vom Werbungsempfänger gekauft wird. Unter anderem durch Kennzeichen, welche nicht bedacht werden, da diese nicht offensichtlich sind.

Viele Nutzer aktivieren (oder deaktivieren nicht) in ihrem mobilen Gerät die GPS-Funktion und die Protokollierung der Aufenthaltsorte in der Cloud. Natürlich werden sie im Gegenzug auf interessante Orte in unmittelbarer Nähe hingewiesen, erhalten Restaurantempfehlungen oder ähnliches. Diese Funktion verrät vieles, an das überhaupt nicht gedacht wird.

Aus dem Bewegungsprofil ist zu erkennen: der persönliche Aktionsradius, ist die Person eher lokal oder mobil (Lebensradius), an welchen Orten ist man regelmäßig oder nur vereinzelt (Urlaub oder beruflich), wie werden diese Orte erreicht (zu Fuß, ÖPNV, mit dem KFZ oder dem Flugzeug), mit welchen Geschwindigkeiten (speziell beim KFZ, Risikobereitschaft), Arbeitgeber, private Orte, beliebte Freizeitgestaltung, Frühaufsteher oder Langschläfer, alles kein Problem. Gleichzeitig ist so aber auch feststellbar, wer sich bei wem in der Nähe aufhält. Natürlich wiederholt oder nachts, ohne dass sich über Stunden der Aufenthaltsort ändert. Beziehungen zwischen Menschen werden so ersichtlich. Zahlt man noch bequem über einen der kommenden Mobile-Payment-Dienste, ist das Personenprofil nahezu komplett. Kaufkraft und Vorlieben bei Produkten, Spendenbereitschaft usw., alles protokolliert. Die persönlichen Ansichten werden aus den Social-Networks abgelesen.

Die verschiedenen zu erfassenden Parameter (Möglichkeiten) sind schier unbegrenzt. Letztlich wird sogar gemessen, wie lange man auf Webseiten bei bestimmten Bild-Motiven verweilt.

Bitte nicht missverstehen. Dies ist keine Wertung. Ohne Datennutzung wären alle liebgewonnenen Dienste und Funktionen schlicht nicht zu betreiben. Ich zeige hier nur auf was erfasst wird.

Fazit

Mit den personenbezogenen Daten wird Geld verdient, viel Geld. Die DSGVO mag vielen als Bürokratiemonster erscheinen, aber sie soll dem Nutzer in einem gewissen Maß die Kontrolle über seine Daten zurückgeben. Da das Dateneigentum im Vordergrund steht, ist auch eine Anpassung bzw. Abschwächung nach Firmengröße nicht sinnvoll. Für die meisten kleinen bis mittelständischen Unternehmen sind die zu ergreifenden Maßnahmen, um DSGVO-konform zu werden, aber auf jeden Fall überschaubar. Zentraler Punkt wird die umfassende Information an die Betroffenen sein, speziell wenn die Daten nicht nur im eigenen Haus verwertet werden sollen (Weitergabe, gegen Bezahlung). Eine ausdrückliche nachweisbare Einwilligung ist dann unerlässlich.

Jeder kann im privaten Bereich für sich entscheiden, wie weit die Bereitschaft geht, mit eigenen (manchmal auch nicht den eigenen) Daten zu bezahlen. Im Businessbereich ist dies nicht mehr zu akzeptieren. Da sind die Abläufe nun auf DSGVO-Konformität zu prüfen.

Jeder möge sich vor Augen führen, dass die Durchsetzbarkeit der Betroffenenrechte außerordentlich wichtig wird, wenn Daten über einen selbst kursieren, welche unrichtig oder sogar unwahr sind. Ein Handy-Vertrag wird abgelehnt, weil einem ein unbedienter Kredit zugeschrieben wird, den man niemals hatte oder es gibt persönliche Nachteile durch ein falsches, kursierendes Religionskennzeichen. Man kann etwa eine Stelle bei einem kirchlichen Träger nicht antreten, weil man als konfessionslos gilt, obwohl man durchaus seine Kirchensteuer zahlt. Hier hätte man jeweils das Recht auf Berichtigung, um darauf nicht ausschließlich maschinell beurteilt zu werden. Das kann auch bis zum Schadenersatz gehen.

Einen neuen Ansatz verfolgt der Browser „Brave“, welcher sich noch in der Entwicklung befindet. Brave verspricht hohen Schutz der Privatsphäre. Maßgabe ist zusätzlich: wenn der Benutzer (durch seine Daten) kommerziell genutzt wird, soll er selbst davon profitieren, indem er für geduldete, eingeblendete Werbung einen Teil der Bezahlung erhält.

Ist das ein Konzept für die Zukunft oder am Ende doch die völlige Aufgabe der Kontrolle über persönliche Daten durch erteilte Einwilligung?

AUTOR

Peter Klatecki
Jasper Gesellschaft für Energiewirtschaft und Kybernetik mbH
Geseke
Tel.: 02942 / 9747-0
p.klatecki@jasper-gmbh.de