Der Schutz der Daten – DSGVO im Überblick und in der Praxis (Teil 1)

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?

Nachdem nun einige Monate mit der DSGVO vergangen sind, kann man etwas Ordnung in die Einschätzungen bringen, einen nüchternen Blick auf notwendige Maßnahmen werfen und Situationen beurteilen. Grundlegende notwendige Theorie (Teil 1 in dieser Ausgabe) wird ergänzt durch plakative Beispiele (Teil 2).

Anmerkung: Eine abschließende und rechtssichere Darstellung ist leider nicht möglich, da letztinstanzliche Urteile erst viel später zu erwarten sind.

Historie der DSGVO

Der deutsche Europaabgeordnete Jan-Philipp Albrecht (Grüne) hat in enger Zusammenarbeit mit der Luxemburgerin Viviane Reding (ehem. Vizepräsidentin der Europäischen Kommission und Kommissarin für das Ressort Justiz, Grundrechte und Bürgerschaft) die neue europäische Datenschutzgrundverordnung maßgeblich auf den Weg gebracht und gegen viele Widrigkeiten und starke Lobbyarbeit im Laufe von vier Jahren durchgesetzt. Die Umsetzung der Vorlage war durch eine enorme Anzahl von Änderungsanträgen (> 4.000) eigentlich schon „tot". Doch im Sommer 2013 kam die NSA-Affäre durch die Enthüllungen von Edward Snowden. Ab dem Zeitpunkt wurde die Umsetzung doch deutlich beschleunigt, im März 2014 durch das EU-Parlament verabschiedet und im April 2016 beschlossen und veröffentlicht. Sie ersetzt die Richtlinie 95/46/EG aus 1995.

Seit dem 25.05.2018 ist die europäische Datenschutzgrundverordnung (DSGVO), nach einer zweijährigen Übergangszeit, nun vollständig in Kraft. Erst wenige Monate vor diesem Termin schlugen die Wellen in den meisten Unternehmen hoch, obwohl die Einzelheiten der Verordnung bereits mindestens seit dem 25.05.2016 bekannt waren. Vermutlich beruht dieses Vorgehen auf dem Umgang mit den bisherigen Datenschutzregelungen der einzelnen Länder. Diese wurden schlicht nicht gefürchtet, da Kontrollen praktisch nicht vorkamen und die dort möglichen Strafen gering waren. In Deutschland z. B. wurde das „BDSG alt" im Zuge der Wirksamkeit der DSGVO durch das angepasste „BDSG neu" ersetzt, welches die Datenschutzgrundverordnung jetzt ergänzt.

Was soll durch die DSGVO erreicht werden?

Mehrere Absichten werden verfolgt. An erster Stelle steht der Schutz der Person bzw. der Schutz des Verbrauchers. Die einzelne Person soll die Kontrolle über ihre Daten erhalten. Weiter sind die europaweite Vereinheitlichung des Datenschutzes, die Anpassung an die fortschreitende Digitalisierung und technikneutrale Ausgestaltung wichtige Ziele. Um die Ernsthaftigkeit zu bekräftigen, wurde die Haftung für das Management von Unternehmen sowie die möglichen Strafen deutlich verschärft.

Durch die Ausgestaltung der Regelungen müssen als „Hauptziele" (Targets) die großen Internet-Unternehmen wie Amazon, Facebook, Google und Co. betrachtet werden. Es gibt allerdings keine Staffelung oder Ausgestaltung der Regeln nach Betriebsgröße. Die Anforderung an den Datenschutz ist prinzipiell nicht teilbar.

Datenschutz ist ein Grundrecht

Jeder Mensch soll im Grundsatz (also weitestgehend) selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen. Hieraus resultieren die Grundsätze für die Verarbeitung von personenbezogenen Daten nach Artikel 5 DSGVO:

- Rechtmäßigkeit, Treu und Glauben (vom Betroffenen nachvollziehbar)
- Transparenz (Auskunftsmöglichkeit, Dateneinsicht)
- Zweckbindung (eindeutig, zweckmäßig, Verbot der Weitergabe)
- Datensparsamkeit (Minimierung, nur nötige Daten dürfen erhoben werden)
- Richtigkeit (und damit auch aktueller Stand)
- Begrenzte Speicherung (Befristung, Löschung wenn nicht mehr benötigt)
- Integrität und Vertraulichkeit (Technische Maßnahmen zum Schutz).

Als Beispiel für Minimierung sei die Versendung eines s. g. Newsletters per E-Mail angeführt. Um das durchführen zu können, ist als Datum die E-Mail-Adresse des Empfängers ausreichend. Weitere Daten sind nicht notwendig.

Geltung

Geschützt nach DSGVO werden alle natürlichen Personen innerhalb der EU. Diese können sich auf die Anwendung der Verordnung berufen und dies auch rechtlich durchsetzen.

Geregelt wird die Verarbeitung von personenbezogenen Daten durch Organisationen (Unternehmen, Behörden, Vereine, …). Sie gilt ausdrücklich nicht für Privatpersonen als Verarbeiter, wenn diese Daten für persönliche oder familiäre Zwecke verwendet werden. Der Grad ist jedoch schmal. Werden mit privater Verarbeitung Einkünfte

erzielt, wenn auch nur marginal, ist die Verordnung anzuwenden. Dies ist z. B. der Fall bei Einblendung von Werbung auf einer privaten Webseite gegen Bezahlung, auch wenn die übrige Seite ausschließlich private Darstellungen enthält und nicht kommerziell ausgerichtet ist.

Sie ist auch nicht auf die Daten Verstorbener anzuwenden, solange der jeweilige Mitgliedsstaat keine Sonderregelung erlässt (Erwägungsgrund 27).

Die bisherigen nationalen Gesetze (in Deutschland „BDSG alt" und „TMG alt") sind weggefallen und wurden jeweils durch überarbeitete Regelungen ersetzt, um mit der DSGVO konform zu sein.

Die DSGVO gilt für Unternehmen mit Niederlassung in der EU, auch wenn die Daten außerhalb der EU verarbeitet werden. Sie gilt für Unternehmen mit Niederlassung außerhalb der EU bei Datenverarbeitung im Zusammenhang mit dem (auch kostenlosen) Anbieten von Waren oder Dienstleistungen innerhalb der EU und/oder der Beobachtung des Verhaltens von Bürgern innerhalb der EU.

Erläuterungen über die Gründe, welche zu einem jeweiligen Artikel der Verordnung geführt haben, oder Auslegungshinweise, findet man in den sogenannten Erwägungsgründen. Davon gibt es allein 173.

Geregelt wird also der Umgang mit personenbezogenen Daten, also Daten, die einem (lebenden) Menschen zugeordnet werden können. Daten von juristischen Personen, Vereinen, Verbänden etc. sind durch die DSGVO nicht geschützt.

Nach Erwägungsgrund 26 findet die Verordnung auch keine Anwendung auf anonymisierte Daten. Diese sollten aber wirklich sicher anonymisiert sein. Es sind durchaus Situationen denkbar, in denen durch EDV-Einsatz, eventuell mit großen Datenmengen, durch Kombination wieder auf den oder die einzelnen Betroffenen zu schließen ist.

Personenbezogen / Identifizierbar

Die DSGVO nennt den Begriff der Identifizierbarkeit. Personenbezogene Daten sind alle Angaben, die eine Person identifizierbar (bisher bestimmbar) machen. Beispielsweise Name, Adresse, Geburtsdatum, Telefonnummer (jeweils offensichtlich), Vermögen, Gehalt, Bankkonten usw. Aber auch eine IP-Adresse bei der Nutzung des Internets, selbst eine variable, wird schon als ausreichend betrachtet.

Identifizierbar ist also eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt. Identifizierbar wird eine Person, wenn ihre Identität durch die Kombination des Datums mit einer anderen Information feststellbar wird (Bsp.: IP-Adresse kombiniert mit Providerdaten). Identifikation ist natürlich auch durch andere Merkmale wie der physischen, physiologischen, psychischen, genetischen, wirtschaftlichen, kulturellen oder sozialen Identität denkbar und möglich.

Die Erhebung und Verarbeitung dieser Daten ist nur unter bestimmten Voraussetzungen erlaubt (Art. 6 DSGVO). Gemeint ist jeder Vorgang und die Formulierung bezieht sich nicht nur auf elektronische Verarbeitung.

Nach der DSGVO bedeutet „Verarbeiten" das: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen, Abgleichen, Verknüpfen, Einschränken, Löschen, Vernichten, …

Also alles, was man mit Daten anstellen kann. Es gilt ein „Verbot mit Erlaubnisvorbehalt", die Verarbeitung ist grundsätzlich unzulässig, sofern keine Ausnahme oder Erlaubnis vorliegt. Das klingt sehr einschränkend, wir werden noch sehen, dass nach wie vor eine Menge möglich ist.

Es gilt: *Es ist nur noch datenschutzkonform, was der DSGVO entspricht.* Die Bußgelder bei Verstößen sind erheblich erhöht worden. Maximal sind jetzt € 20 Mio. oder 4 % des weltweiten Jahresumsatzes möglich; je nachdem was höher ist.

Abgrenzung bzw. Überschneidung

Natürlich behalten übergeordnete (nationale) Gesetze ihre Gültigkeit. Etwa das Persönlichkeitsrecht, das Recht am eigenen Bild, das Recht auf Privatsphäre oder die Unverletzlichkeit der Wohnung, das Recht auf Selbstbestimmung, -bewahrung und -darstellung. Diese Rechte sind obligatorisch.

Erlaubte Datenverarbeitung

Würde die Datenverarbeitung nur noch erlaubt sein, wenn der jeweilige Betroffene seine ausdrückliche Erlaubnis dazu erteilt hat, würde unsere Wirtschaft zum Erliegen kommen. Ohne Verarbeitung personenbezogener Daten ist das Geschäftswesen schlicht nicht denkbar. Dies war den Verordnungsgebern auch bewusst.

Nach Artikel 6 ist die Verarbeitung grundsätzlich erlaubt, auch ohne ausdrückliche Einwilligung des Betroffenen, wenn ein sogenanntes berechtigtes Interesse vorliegt und schutzwürdige Interessen der Person nicht dagegen sprechen. Laut Verordnung sind „die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen", zu berücksichtigen. Das ist z. B. bei einer Kundenbeziehung der Fall oder der Beziehung Arbeitgeber – Mitarbeiter. Ebenfalls erlaubt ist die Verarbeitung zur Erfüllung eines Vertrages oder für vorvertragliche Maßnahmen, bei rechtlicher Verpflichtung zum Schutz lebenswichtiger Interessen natürlicher Personen und in jedem Fall zur Ausübung öffentlicher Gewalt (Legislative, Judikative, Exekutive).

Daten, welche bis hierher nicht abgedeckt sind, dürfen verarbeitet werden, wenn der jeweilige Betroffene hierzu seine Einwilligung erklärt. In dem Fall ist die Verarbeitung beliebiger Daten möglich. Wichtig hierbei ist, dass die Einwilligung nachweisbar ist und die Person über ihr Widerrufsrecht aufgeklärt wurde. Dieser Widerruf muss so einfach wie die Einwilligung erreichbar und umsetzbar sein. Zusätzlich gilt ein Kopplungsverbot mit anderen Einwilligungen, etwa der Zustimmung zu AGB und es gilt das s. g. Opt-In. Die Einwilligung muss aktiv erteilt werden und darf, etwa auf Webseiten, nicht zur Bestätigung voreinstellt sein, auch wenn man diese Voreinstellung abwählen kann.

Einwilligung zur Verarbeitung sensibler Daten

In Artikel 9 definiert die DSGVO besondere Arten von Daten, oder auch sensible Daten. Hierzu zählen die Religion, die sexuelle Orientierung, die ethnische Herkunft, die politische Meinung, Daten zur Gesundheit,

Gewerkschaftsangehörigkeit und jetzt auch Genetik und Biometrie. Hier muss jeweils die ausdrückliche Einwilligung zur Verarbeitung vorliegen. Bei Kindern unter 16 Jahren ist generell die Einwilligung der Eltern erforderlich.

Es sei denn …

§ 26 BDSG regelt die Verarbeitung von personenbezogenen Daten bei Beschäftigungsverhältnissen, sowohl für Begründung, Durchführung und Beendigung. Etwa die Verarbeitung des Kennzeichens der Religionsangehörigkeit (oder eben nicht) ist zur Erfüllung rechtlicher Vorgaben (Abrechnung) notwendig und damit ohne ausdrückliche Einwilligung erlaubt.


Pixabay.com / TheDigitalArtist

Informationspflicht

Da Rechte nur wahrgenommen werden können, wenn man sich auch über die zu Grunde liegenden Umstände bewusst ist, sieht die DSGVO ausführliche Informationspflichten vor. Bei direkter Datenerhebung beim Betroffenen ist dies in der Regel auch unproblematisch. Mitgeteilt werden muss demjenigen u. a., wer die Daten verantwortlich erhebt, die Rechtsgrundlage, die Dauer der Speicherung, ggf. eine Übermittlungsabsicht und der zugehörige Empfänger als auch die Widerrufbarkeit. Dokumentation nicht vergessen! Bei indirekter Datenerhebung (Erhalt von einem Dritten) soll die betroffene Person innerhalb eines Monats entsprechend informiert werden.

… oder doch nicht?

In der Verordnung werden Ausnahmefälle genannt. So entfällt die Informationspflicht, wenn diese „unmöglich" oder „unverhältnismäßig aufwendig" ist, die Erhebung gesetzlich vorgeschrieben ist oder eine Geheimhaltungspflicht besteht. Ebenso entfällt die Pflicht, wenn der Betroffene bereits über diese Informationen verfügt (z. B. wurde dieser bei der Datenerhebung informiert, inklusive Übermittlungsabsicht).

In der Praxis wird die Information damit in der Mehrzahl der Fälle unterbleiben. Man betrachte nur als Beispiel einen Bezahlvorgang mit einer Kontokarte. Niemand erwartet vernünftigerweise, dass er vor der Bezahlung ein Formular mit umfassender Darstellung des Datenverarbeitungsvorgangs unterschreiben muss. Auf der einen Seite kann man annehmen, dass der Zahlende weiß, dass Daten gesammelt und übertragen werden, auf der anderen Seite wäre es auch unverhältnismäßig aufwendig.

Datengeheimnis

Mit Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt (!) zu erheben, zu verarbeiten oder zu nutzen. Bei Aufnahme ihrer Tätigkeit sind diese Personen nach DSGVO durch den Unternehmer auf das Datengeheimnis zu verpflichten. Dies geschieht sinnvollerweise als Anlage zum Arbeitsvertrag, als getrennte schriftliche Vereinbarung. Diese ist nicht widerrufbar und besteht auch nach Beendigung der Tätigkeit, auch nach dem Ausscheiden aus dem Unternehmen, fort. Der Personenkreis mit dieser Verpflichtung sollte nicht unnötigerweise eingeschränkt werden. So sind normalerweise auch Reinigungskräfte zu verpflichten, da diese auch bei der Reinigung der Büroräume oder speziell bei der Entsorgung mit personenbezogenen Daten in Kontakt kommen können, und sei es nur ohne Absicht. Löschen bzw. Entsorgen von Daten zählt eben auch als Verarbeitung.

Betroffenenrechte, Rechte im Einzelnen

Aufklärung

Als erstes Recht ist die umfassende Aufklärung zu nennen. Der Betroffene soll wissen, in welchem Umfang Daten zu seiner Person erhoben und verarbeitet werden. Nun ist es sicherlich nicht im Sinne des Ordnungsgebers, dass bei jedem Vorgang zusätzlich mehrere Seiten mit einer entsprechenden Belehrung ausgedruckt und verteilt werden. Aktueller Stand der Beurteilung läuft auf eine, jeweils spezielle Webseite des Unternehmens hinaus, welche die Person einsehen und sich informieren kann. Es wird davon ausgegangen, dass ein Anteil von deutlich über 90 % der Personen heute unmittelbaren Zugang zum Internet hat. Der Link zu dieser Seite wird dann in jeder Kommunikation angegeben. Angefangen von der E-Mail in der Signatur bis hin zu Lieferscheinen oder Rechnungen. Dies ist in meinen Augen auch viel sinnvoller als Berge von Papier zu bedrucken, mit Hinweisen, welche die meisten Bürger ungelesen akzeptieren. Diese Datenverarbeitungshinweise sind nicht mit der Datenschutzerklärung zu verwechseln. Diese muss auf jeder geschäftlichen Internetpräsenz, an prominenter Stelle, direkt für den Benutzer erreichbar sein. Also als eigene Seite gleichberechtigt neben dem Impressum.

Auskunft

Jeder hat das Recht, eine Kopie der Daten zu erhalten, welche über ihn gespeichert sind. Was sich so leicht fordern lässt, ist unter Umständen nur schwierig umzuset-

Pixabay.com / TPHeinz

zen. Man denke nur an gescannte Dokumente mit personenbezogenen Daten. Sind diese nicht entsprechend indiziert, sind sie u. U. nur mit extremem Aufwand (manuelle Einsicht) auffindbar.

Die großen Internetkonzerne mit entsprechenden Diensten bieten für ihre Mitglieder mit eigenem Login die Möglichkeit, über spezielle Webseiten Auskunft über die gespeicherten Daten zu erlangen. Bei Google etwa über myaccount.google.com, bei Apple über privacy.apple.com, usw. Alle Großen bieten so etwas. Spannender ist die Frage, welche Daten über Personen vorliegen, welche keinen Account beim jeweiligen Dienst besitzen oder die Datenabfrage, wenn keine entsprechende Seite angeboten wird. Für diese Fälle können im Internet Musterschreiben bei den Verbraucherzentralen heruntergeladen werden. Gerade bei den großen Social-Networks werden die gespeicherten Daten sehr umfangreich sein und als Ausdruck ggf. wohl mit Paketdienst/Spedition geliefert werden.

Jede Firma sollte sich darauf vorbereiten, wie mit entsprechenden Anfragen umzugehen ist, und die Mitarbeiter unterweisen. Wird Auskunft angefordert, so sind in jedem Fall unmittelbar die Identität der fordernden Person, und damit die Berechtigung zur Abfrage, zu verifizieren.

Löschung

Das s. g. Recht auf „Vergessen werden". Natürlich ist es möglich, die Löschung von Daten aktiv zu fordern. Gemeint ist aber, Daten nur solange zu speichern, bis diese nicht mehr benötigt werden. Ein Antrag auf Löschung kann also verweigert werden, wenn die Daten noch die Basis für andere Vorgänge, etwa als Nachweis für Finanzbehörden o. ä., bilden.

Datenübertragbarkeit

Dies zielt auf soziale Netzwerke im Allgemeinen, auf verschiedene Portale und E-Mail Provider. Die Daten müssen in einem „geeigneten Format" bereitgestellt werden, etwa auf mobilen Datenträgern oder als Download aus der Cloud. Dieses Recht soll einen Anbieterwechsel erleichtern und den s. g. „Lock-In Effekt", die Zwangsbindung an einen Anbieter, vermeiden. Es darf bezweifelt werden, dass dies häufig genutzt werden wird, denn Datenformate verschiedener Anbieter sind in der Regel stark unterschiedlich und damit inkompatibel.

Das Recht erlischt, wenn die Daten zur Wahrnehmung öffentlicher Aufgaben genutzt werden, Rechte und Freiheiten Anderer betroffen sind oder die Übertragung technisch unmöglich ist (siehe Inkompatibilität).

Während der Übergangsphase (2016–2018) wurde teilweise die Ansicht vertreten, Unternehmen sollten sich durch Schaffung entsprechender Schnittstellen darauf vorbereiten, dieses Recht erfüllen zu können. Dies halte ich schlicht für unmöglich und illusorisch. Abgesehen von den Standarddaten wie Adresse, Alter usw. Diese Daten können rein textlich übertragen werden.

Die Datenformate sind von Unternehmen zu Unternehmen unterschiedlich und auch abweichend verknüpft, sodass eine Übertragung von weitergehenden Daten wenig Sinn ergibt. Jedes Unternehmen, welches schon einmal die Software für Warenwirtschaft oder Ressource Planning gewechselt hat, weiß, welche Probleme schon innerhalb eines Unternehmens auftreten können.

Wenn überhaupt, sind Übertragungen nur bei ähnlichen Diensten sinnvoll, etwa die Mitnahme von aufgelaufenen E-Mails zu einem neuen Provider. Hier gab es aber bisher immer schon Möglichkeiten diese Daten lokal zu speichern und dann wieder zu übertragen. Außerdem sollte so ein Wechsel auch zum Anlass genommen werden, sich von nicht mehr benötigten Mails zu trennen. Man denke an das Recht auf Löschung. Daten sind zu entfernen, wenn diese nicht mehr benötigt werden.

Widerspruch

Personen können der Verarbeitung von über sie gespeicherten Daten widersprechen oder die Einwilligung zur Verarbeitung widerrufen. Stehen keine Hinderungsgründe entgegen, etwa die Daten werden noch benötigt oder es besteht noch eine Verpflichtung zur Aufbewahrung usw., müssen die Daten gelöscht werden. Zum Widerspruchsrecht gehört natürlich auch das Recht auf Berichtigung, falls festgestellt wird, dass die gespeicherten Daten falsch oder nicht aktuell sind.

Einschränkung der Verarbeitung

Daten werden von weiterer Verarbeitung als der unbedingt notwendigen, etwa für gesetzliche Anforderungen, ausgeschlossen. Dies z. B., wenn eine direkte Löschung nicht möglich ist, weil der Gesetzgeber eine Archivierungsfrist fordert.

Keine ausschließlich automatisierte Entscheidung

Dies ist in meinen Augen eines der spannendsten Rechte, wenn auch eines, welches wohl am wenigsten greifbar sein dürfte. Übersetzt sagt dies aus, dass Entscheidungen über Personen nicht nur von Algorithmen abhängen dürfen und zusätzlich jeweils eine natürliche (!) Person

diese Entscheidung überdacht haben soll. Während dies bei reinem Maschinenkontakt noch eindeutig ist, bleibt die Frage der Beweisbarkeit, wenn die Entscheidung im Gespräch übermittelt wird.

Hier zeigt sich, dass den Verordnungsgebern bewusst gewesen sein muss, dass Algorithmen auch gefärbt nach Meinung und Ansichten des Programmierers bewerten können. Algorithmen sind also nicht neutral, nur weil sie maschinell ausgeführt werden. Die Überprüfbarkeit der (geforderten) Neutralität ist aktuell in der Diskussion, technisch als auch ethisch. Amazon hat im Oktober 2018 die s. g. Künstliche Intelligenz zur Bewerberauswahl deaktiviert. weil es Frauen systematisch benachteiligte, selbst wenn das Geschlecht nur indirekt zu ermitteln war. Aus den zur Verfügung stehenden Daten zog das System den Schluss, dass Männer für die zu vergebenden Aufgaben besser geeignet seien. Auch nach einer Anpassung der Programmierung konnte eine Neutralität nicht gesichert angenommen werden. Ein ähnliches Phänomen ist die Benachteiligung von Afro-Amerikanern bei KI´s zur Verbrechensvorhersage in den USA.

Rechtsbehelf, Schadensersatz

Dies besagt nichts anderes, als dass die vorgenannten Rechte auch eingeklagt werden dürfen und bei rechtskräftig festgestellten Verstößen Schadenersatz zu leisten ist. Da hier ein Persönlichkeitsrecht jeweils Gegenstand ist, dürfte es interessant sein, die Höhe der verhängten Strafzahlungen in Zukunft zu beobachten.

Der Datenschutzbeauftragte (DSB)

Pflicht zur Bestellung eines DSB

Häufig besteht die Ansicht, dass eine Bestellung eines Datenschutzbeauftragten für das jeweilige Unternehmen immer aus der DSGVO folgt. Dies ist jedoch nur zum Teil richtig. Die Verordnung fordert einen DSB, wenn die Kerntätigkeit (eines Unternehmens) in der Verarbeitung von besonderen Kategorien von Daten (siehe oben), der Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten oder bei regelmäßiger systematischer Überwachung von betroffenen Personen besteht. Kerntätigkeit wird definiert als Tätigkeit, die für die Geschäfte des Unternehmens wichtig ist. Regelmäßige Überwachung bezieht sich auf Scoring- oder Profiling-Methoden zur Erfassung des Verhaltens von Internetnutzern, in der Markt- und Meinungsforschung, bei Sicherheitsunternehmen oder im Bereich Social-Media usw. Im Gesundheitsbereich und in der Rechtsberatung und -vertretung ist somit ein DSB obligatorisch.

Die Pflicht zur Bestellung eines DSB leitet sich bei den meisten Unternehmen vielmehr aus dem „BDSG neu" ab. Dieses fordert einen Datenschutzbeauftragten, wenn zehn Personen oder mehr (> 9) mit der automatisierten Verarbeitung personenbezogener Daten befasst sind. Der Umfang dieser Verarbeitung ist nicht näher definiert. Ein DSB ist auch zu bestellen, wenn Daten „mit Folgeabschätzung" vorliegen. Hierbei muss geprüft werden, ob die Datenverarbeitung besondere Risiken für die Rechte und Freiheiten eines Betroffenen bedeutet. Dies entspricht der Hervorhebung von „besonderen Kategorien" in der DSGVO.

Vor dem Hintergrund, dass nahezu keine betriebliche Funktion heute ohne Datenverarbeitung auskommt, ein entsprechender Arbeitsplatz in der Regel zumindest über die Möglichkeit zur E-Mail oder sonstige digitale Kommunikation verfügt, ist die 10-Personen-Grenze schnell erreicht. Selbst der (regelmäßige) Ausdruck von Adressaufklebern mit Namen von natürlichen Personen im Versand ist vermutlich zu berücksichtigen.

Kriterien für einen DSB

Im Prinzip kann jeder zum Datenschutzbeauftragten bestellt werden. Gefordert wird jedoch eine „gewisse berufliche Qualifikation", Fachwissen im Datenschutz und die Fähigkeit die Aufgabe wahrzunehmen. Neben der Grundqualifizierung geht man von etwa fünf Tagen an Weiterbildungsmaßnahmen (IT und juristischer Bereich) pro Jahr aus. Der DSB hat besonderen Kündigungsschutz, ein Zeugnisverweigerungsrecht und natürlich Verschwiegenheitspflicht.

Auf keinen Fall darf ein Interessenskonflikt innerhalb des Unternehmens vorliegen. Dies ist der Fall wenn der jeweilige Mitarbeiter in der IT, der Personalabteilung oder der Geschäftsführung beschäftigt ist, oder ähnliche Aufgaben wahrnimmt.

Die Bestellung ist intern (eigener Mitarbeiter) oder extern möglich. Der Umfang der Haftung ist jeweils unterschiedlich. Die Leitung von Unternehmen, welche nicht der Pflicht zum DSB unterliegen, sollte überlegen, doch einen (externen) Datenschutzbeauftragten zu bestellen, da dadurch ein großer Teil des Haftungsrisikos für die Geschäftsführung abgegeben wird. Die Regelungen der DSGVO sind ja unabhängig vom DSB zu erfüllen.

Aufgaben des DSB

Der Datenschutzbeauftrage ist die Schnittstelle zwischen den Mitarbeitern und der Geschäftsführung, Ansprechpartner für Kunden und sonstige Betroffene und natürlich auch für die Datenschutzbehörden. Hier ist er Zuständiger und Verantwortlicher. Die Position ist eine Stabsstelle direkt unterhalb der Leitung. Er berichtet dorthin, hat aber ansonsten keinerlei Weisungsbefugnis, also nur beratende Funktion. Wenn die Tätigkeit keine Vollzeitstelle erfordert, können durchaus andere Tätigkeiten im Unternehmen ausgeführt werden.

Meldung muss sein

Im Unterschied zum vorherigen „BDSG alt" muss der bestellte DSB der Aufsichtsbehörde im jeweiligen Bundesland bekannt gemacht werden. Dies erfolgt in der Regel online über vorgehaltene Formulare. Die Behörden erhalten somit einen direkten ersten Überblick, wie das Thema Datenschutz in den Unternehmen behandelt wird. Abhängig von der Betriebsgröße kann man die Pflicht zur Bestellung vermuten und entsprechende Kontrollmaßnahmen veranlassen.

Verfahrensverzeichnis

Pflicht zur Führung, eigentlich für alle

In Deutschland war ein Verfahrensverzeichnis bereits nach dem vorherigen Bundesdatenschutzgesetz für viele Unternehmen

Pflicht. Sogar als öffentlich einsehbares Verzeichnis. Die Öffentlichkeit entfällt mit der DSGVO.

Unternehmen ab 250 Mitarbeiter sind generell verpflichtet, ein solches Verzeichnis zu führen. In Erwägungsgrund 13 wird betont, diese Grenze bewusst gewählt zu haben, um „kleinere" Unternehmen zu entlasten. Obligatorisch ist es für alle Unternehmen mit der Verarbeitung besonderer Kategorien von Daten (s. o.), mit Risiko für Rechte und Freiheiten für Betroffene oder Daten über Straftaten und Verurteilungen.

Ein Verzeichnis benötigen aber auch alle Unternehmen, welche personenbezogene Daten „nicht nur gelegentlich" verarbeiten. Damit muss im Prinzip jedes Unternehmen, jede Organisation und jeder Verein, ein solches Verzeichnis führen. Eine Kunden- oder Mitgliederliste, Lieferschein- und Rechnungsschreibung oder ähnliches gibt es wohl immer und die werden hoffentlich regelmäßig genutzt.

Bei den meisten Unternehmen ist die Anzahl an zu dokumentierenden (Datenverarbeitungs-) Verfahren übersichtlich. Hier bietet sich zusätzlich die Chance bei der Verzeichniserstellung, eingefahrene Verarbeitungsabläufe zu überdenken und zu optimieren.

Auftragsverarbeitung

Datenübermittlung ist (eigentlich) nur zulässig, wenn die Einwilligung der betroffenen Person vorliegt oder Gesetz und Verordnung es ausdrücklich erlauben. Die meisten betroffenen Personen gehen somit davon aus, dass eine Übertragung bzw. ein Transfer von Daten ohne ihr Wissen nicht mehr statthaft ist.

Handelt es sich um s. g. Auftragsverarbeitung, ist stillschweigender Transfer jedoch wieder möglich. Dann sind weder eine Einwilligung noch eine gesetzliche Erlaubnis und auch keine Benachrichtigung erforderlich. Die Verarbeitung ist sogar auch außerhalb der EU möglich.

Auftragsverarbeitung ist es in folgenden Fällen:

Die Verarbeitung erfolgt „für den Auftraggeber", der Dienstleister hat kein eigenes Interesse an den Daten. Der Auftraggeber legt Zweck und Mittel fest. Der Datenverarbeiter hat nur eine Hilfs- oder Unterstützungsfunktion.

Allgemein gesprochen: Der Auftraggeber bleibt „Herr der Daten". Er entscheidet weiter über Erfassung, Löschung usw. Der Verarbeiter ist von den Weisungen des Auftraggebers abhängig.

Typische Fälle von Auftragsverarbeitung:

- Externe Lohn- oder Gehaltsabrechnung (nicht beim Steuerberater, s. u.)
- Newsletter-Versand durch eine Marketingagentur
- Nutzung von Cloud-Diensten zur Personal- und Kundenverwaltung
- Datenträgerentsorgung, Aktenvernichtung
- Webanalyse- und Tracking-Dienste (wie Google Analytics)
- Kunden-Helpdesks
- Ausgelagerte Rechenzentren
- Callcenter, die Kundendaten ohne wesentliche eigene Entscheidungsspielräume verarbeiten
- Daten erfassen und konvertieren oder Dokumente einscannen usw.

Keine Auftragsverarbeitung ist es in folgenden Fällen:

- Finanzberater
- Steuerberater (StBerG, weisungsfrei)
- Unternehmensberater
- Rechtsanwalt
- Wirtschaftsprüfer
- Externer Betriebsarzt
- Inkassobüro (mit Forderungsübertragung)
- Bankinstitut für den Geldtransfer
- Postdienst für den Brieftransport
- Installation und Wartung von Netzwerken
- Wartung von Hardware und Telefonanlagen
- Pflege von Software, Programmentwicklungen und Tests
- usw.

Hier nimmt man fremde Fachdienstleistungen in Anspruch, bei einem eigenständig Verantwortlichen. In der Regel gibt es eigene Rechtsgrundlagen oder die Empfänger der Daten unterliegen einer Schweigeverpflichtung (Berufsgeheimnis). Keine Auftragsverarbeitung ist es also, wenn die Datenhoheit abgegeben wird. Zusätzlich auch nicht, wenn spezielle Gesetze die Verarbeitung regeln, etwa im Bereich Telekommunikation, oder wenn es sich um eine rein technische Wartung handelt.

Ein Unternehmen hat mit einem Auftragsverarbeiter einen entsprechenden Vertrag zu schließen. Das empfangende Unternehmen sollte genau geprüft werden. Der Verarbeiter muss insbesondere den technischen Datenschutz beachten und hohe Sicherheitsstandards gewährleisten. Entweder liegt eine entsprechende Zertifizierung vor oder der Verarbeiter unterwirft sich den Verhaltensregeln nach Artikel 40 DSGVO. Anbieter aus den USA müssen entweder unter dem Privacy-Shield-Abkommen zertifiziert sein oder der Vertrag muss so genannte EU-Standardvertragsklauseln enthalten.

So weit die theoretische rechtliche Darstellung. In Teil 2 werden Maßnahmen und Empfehlungen zur Anwendung gegeben und Beispiele für ungünstige (der DSGVO nicht konforme) Datenverarbeitung aufgezeigt.

AUTOR

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