Neuerungen im Datenschutzrecht kennen und richtig umsetzen

Autor:

Steffen Grabowski
- Unternehmensberater & externer Datenschutzbeauftragter -

www.grabowski-beratung.de

Inhaltsverzeichnis

Kapitel 1: Einführung ins Thema

Neue Technologien halten immer mehr Einzug in unser Leben. Wir befinden uns inmitten eines digitalen Wandels und in einer Vielzahl an digitalen Disruptionen, in denen digitale Innovationen alte Produkte oder Dienstleistungen komplett ablösen. Einhergehend mit immer mehr Digitalisierung und Automatisierung steigen auch die Risiken eines Missbrauchs. Kaum ein Haushalt ist ohne ein Smartphone, das den aktuellen Aufenthaltsort trackt, einen Social-Media-Account, auf dem wir unsere Vorlieben und Bilder von uns teilen oder einen cleveren Assistenten, der auf Zurufen neues Toilettenpapier bestellt.

Fälle von Datenpannen bei zum Beispiel Facebook, der Telekom und Co. zeigen uns immer wieder, wie anfällig die vorhandenen Strukturen und Systeme seien können und sorgen für viel Aufsehen in der medialen Berichterstattung, bei den Betroffenen und natürlich auch in der Politik. Aber auch der wissentliche Missbrauch von Daten für eigene Zwecke ist einer der Gründe, weswegen der Gesetzgeber natürliche Personen mehr schützen will.

Das Europäische Parlament und der Rat der Europäischen Union veröffentlichte am 4. Mai 2016 die Verordnung (EU) 2016/679 vom 27. April 2016 im Amtsblatt der Europäischen Union. Diese Verordnung, auch Datenschutz-Grundverordnung genannt (kurz: „DS-GVO“), trat am 25. Mai 2016 in Kraft und ist seit dem 25. Mai 2018 unmittelbar anwendbar. Gegenstand der DS-GVO sind Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, aber auch ein freier Datenverkehr innerhalb der Europäischen Union soll ermöglicht werden. Die DS-GVO soll die Grundrechte und Grundfreiheiten natürlicher Personen schützen und insbesondere deren Recht auf den Schutz ihrer personenbezogener Daten gewährleisten.

Betroffen von der DS-GVO sind alle Unternehmen, Behörden oder Einrichtungen, die ihren Sitz in der Europäischen Union haben oder personenbezogene Daten von EU-Bürgern verarbeiten.

Sogenannte Öffnungsklauseln der Verordnung erlauben den einzelnen EU-Staaten zum Teil speziellere Vorschriften oder Vorschriften zu Punkten, die in der DS-GVO nicht abschließend geregelt sind. Hiervon hat die Bundesrepublik Deutschland Gebrauch gemacht und im neuen Bundesdatenschutzgesetz (BDSG-neu) nationale, ergänzende und konkretisierende Regelungen getroffen.

Inwieweit die DS-GVO und das BDSG-neu Unternehmen speziell in Deutschland betreffen, was sie nunmehr beachten müssen und wie sie DS-GVO- und BDSG-neu-konform werden können, soll Gegenstand dieser Arbeit sein.

Eines vorweg: Personenbezogen sind Daten immer dann, wenn sie sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dabei ist es egal, ob es sich um eine tatsächlich direkt identifizierbare oder nur theoretisch identifizierbare Person handelt. Es bleibt daher festzustellen, dass unter den Begriff personenbezogene Daten sowohl Namen, als auch IP-Adressen, Online-Kennungen, E-Mailadressen, Telefonnummern und genetische und biometrische Daten fallen, anhand derer man eine natürliche Person eindeutig identifizieren könnte – zum Beispiel durch Ermittlung des Anschlussinhabers bei einer Telefonnummer.

Kapitel 2: Datenschutzrecht durch DS-GVO & BDSG-neu

Betroffene Unternehmen müssen sich sowohl mit der DS-GVO, als auch mit dem BDSG-neu beschäftigen. Die DS-GVO hat dabei jedoch Vorrang vor anderen Rechtsvorschriften der Mitgliedsstaaten und wirkt unmittelbar und direkt in allen EU-Mitgliedsstaaten, ohne, dass es einer Umsetzung durch nationale Gesetze bedarf. Die nationalen Regelungen (BDSG-neu) müssen grundsätzlich der DS-GVO entsprechen, können deren Vorschriften jedoch ergänzen und konkretisieren, dürfen dabei den Umfang der Öffnungsklauseln jedoch nicht überschreiten.

Diese Kapitel stellt die wichtigsten Prinzipien, Inhalte und Vorschriften dar, die uns Unternehmer in Deutschland betreffen und dient damit der Vorbereitung auf den darauffolgenden Prozess zur Schaffung der Complience im Bereich Datenschutz.

2.1 Grundprinzipien des neuen Rechts

Im Artikel 5 der DS-GVO sind die Grundsätze für die Verarbeitung personenbezogener Daten definiert. Dies sind die Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit.

Rechtmäßigkeit

Die Verarbeitung personenbezogener Daten muss rechtmäßig sein. In diesem Zusammenhang ist von einem Verbot mit Erlaubnisvorbehalt die Rede. Das heißt, dass eine Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, es sei denn, sie erfüllt die Voraussetzungen einer Erlaubnisnorm gemäß Artikel 6 oder 9 DS-GVO (Konkretisierung im Kapitel 2.2 „Überblick der Erlaubnistatbestände“).

Verarbeitung nach Treu und Glauben

Dieses Grundprinzip ist rechtlich im Moment noch nicht eindeutig zu fassen. In der englischen Fassung der DS-GVO ist dieses Prinzip als „fairly“ bezeichnet. Eine Verarbeitung von personenbezogenen Daten muss zur Verwirklichung eines legitimen Zweckes geeignet sein. Sie muss zugleich das mildeste aller gleich effektiven Mittel zur Erreichung dieses Zweckes darstellen. Hierzu sollte eine Interessenabwägung durchgeführt werden, mit dem Interesse des Unternehmens an der Verarbeitung auf der einen Seite und den Rechten des Betroffenen auf der anderen Seite. Beides wird sinnbildlich auf einer Waage abgewogen. Ergibt diese Abwägung, dass die Verarbeitung zu dem verfolgten Zweck mit Blick auf die Folgen für den betroffene Person angemessen ist, kann man von einer Wahrung des Grundsatzes der Verarbeitung nach Treu und Glauben ausgehen.

Transparenz

Personenbezogene Daten müssen in einer für den Betroffenen nachvollziehbaren Weise verarbeitet werden. Für die Person muss nachvollziehbar sein ob und wie, von wem und in welchem Umfang ihre personenbezogenen Daten verarbeitet werden. Dieser Grundsatz spiegelt sich in den Informationspflichten wieder (Artikel 12 ff. DS-GVO). So hat das Unternehmen die Pflicht den Betroffenen bereits bei Erhebung von personenbezogenen Daten umfassend und verständlich zu informieren.

Zweckbindung

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden. Der Gesetzgeber sieht hier ferner eine Beschränkung der Datenverarbeitung auf Zwecke, die mit den ursprünglich verfolgten Verarbeitungszwecken vereinbar sind, vor.

Datenminimierung

Erhobene personenbezogene Daten müssen für den Zweck angemessen und erheblich sein und auf das für die Verarbeitung notwendige Maß beschränkt sein. Wünscht ein Interessent beispielsweise einen Newsletter per E-Mail zu erhalten, benötigt das Unternehmen hierfür im Grunde nur seine E-Mailadresse. Eine Erhebung des Geburtsdatums, Wohnortes etc. ist hierfür nicht erforderlich und durch die aktuelle Gesetzgebung so nicht zulässig. Eine Ausnahme stellt

hier eine ausdrückliche Einwilligung des Interessenten in die zusätzliche Erhebung dieser Daten dar. Zu beachten gilt hier zusätzlich das Kopplungsverbot. Das Erbringen einer Leistung darf demnach nicht von einer Einwilligung abhängig gemacht werden. Demnach dürfte bei dem Anmeldeformular für den Newsletter lediglich die E-Mailadresse als Pflichtfeld deklariert werden.

Richtigkeit

Verarbeitete personenbezogene Daten müssen sachlich richtig sein und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, um veraltete oder unrichtige Daten zu berichtigen oder zu löschen.

Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für die Erreichung der Zwecke, für die sie erhoben wurden, erforderlich ist. Dies überschneidet sich mit dem Grundsatz der Datenminimierung. Es sind also Routinen im Unternehmen zu implementieren, die nicht notwendige personenbezogene Daten löschen oder frühestmöglich anonymisieren, um den Personenbezug aufzuheben.

Integrität und Vertraulichkeit

Bei der Verarbeitung von personenbezogenen Daten ist sicherzustellen, dass jene vor unbefugter oder unrechtmäßiger Verarbeitung, Verlust, Zerstörung und Schädigung geschützt sind. Diesem Schutz wird durch geeignete technische und organisatorische Maßnahmen („TOMs“) sorge getragen.

2.2 Überblick der Erlaubnistatbestände

Im Artikel 6 Absatz 1 DS-GVO sind die Erlaubnistatbestände für die Verarbeitung personenbezogener Daten geregelt (Verbot mit Erlaubnisvorbehalt). Eine Verarbeitung ist demnach zulässig, wenn eine der folgenden Voraussetzungen erfüllt ist:

- die Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten erteilt

- die Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen
- die Verarbeitung ist zur Erfüllung rechtlicher Verpflichtungen erforderlich, der der Verantwortliche unterliegt (z.B. Aufbewahrungsfristen aus dem Steuerrecht)
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlich oder Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen

Grundsätzlich bleibt festzuhalten, dass eine Einwilligung des Betroffenen immer als die letzte Wahl angesehen werden sollte. Denn diese ist durch den Betroffenen jederzeit widerrufbar und birgt zahlreiche Stolperfallen für das Unternehmen (u.a. Informationspflichten & Kopplungsverbot). Ab dem Zeitpunkt des Widerrufs wäre die Verarbeitung einzustellen und die Daten ggf. zu löschen. Daher ist es durchaus sinnvoll, die Verarbeitung auf einen anderen Erlaubnistatbestand zu stützen, deren praktische Anwendung an ein paar Beispielen verdeutlicht werden soll.

Beschäftigungsverhältnis

Im Rahmen der Entgeltabrechnung von Mitarbeitern werden personenbezogene Daten verarbeitet (u.a. Name, Anschrift etc.). Nunmehr wäre eine Einwilligung des Mitarbeiters denkbar. Viel sinnvoller ist es aber, die Legitimation der Verarbeitung mit der Erfüllung einer gesetzlichen Verpflichtung zu begründen, denn der Arbeitgeber hat, im Falle einer sozialversicherungspflichtigen Beschäftigung, die Pflicht über das Arbeitnehmerentgelt abzurechnen und entsprechende Meldungen an das Finanzamt und die Krankenkassen durchzuführen.

Bestellung von Waren durch einen Neukunden

Wenn ein Neukunde bei einem Unternehmen Waren per E-Mail bestellt und das Unternehmen diesen Auftrag bestätigt, kommt ein Vertrag zustande und das Unternehmen verarbeitet personenbezogene Daten (z.B. Name, Anschrift). Die Legitimierung sollte auf den Erlaubnistatbestand der Erfüllung eines Vertrags gestützt werden. Auch die vorvertragliche Verarbeitung kann auf die Durchführung vorvertraglicher Maßnahmen auf Anfrage des Betroffenen gestützt werden.

Angebot an Bestandskunden

Hat ein Kunde ein Produkt bei einem Unternehmen bestellt und es gibt beispielweise ein Relaunch des Produktes, so könnte das Abwägen von dem berechtigten Interesse des Unternehmens an einem Zusatzverkauf und den Interessen des Kunden am Schutz seiner Grundrechte und Grundfreiheiten ergeben, dass das berechtigte Interesse des Unternehmens überwiegt und auch ohne Einwilligung ein Schreiben an den Kunden gesendet werden kann, in dem auf das Relaunch aufmerksam gemacht wird.

Die Abwägung des berechtigten Interesses muss hier mit viel Augenmaß erfolgen und im Zweifel sollte des Interesse des Betroffenen immer schwerer wiegen. Es sind gewiss Einzelfallentscheidungen, in denen die jeweiligen konkreten Aspekte des Einzelfalls berücksichtigt werden müssen. Hierzu zählen zum Beispiel, ob es sich um ein individuelles Anschreiben oder ein Massenmailing handelt, wie lange der Kunde schon Kunde beim Unternehmen ist und, ob es nach Treu und Glauben zu erwarten ist, dass der Kunde auch ein tatsächliches Interesse an der angebotenen Leistung haben könnte.

Neben den Erlaubnisnormen des Artikel 6 DS-GVO definiert der Artikel 9 DS-GVO Erlaubnisnormen für die Verarbeitung besonderer Datenkategorien. Hierzu wird im Kapitel 2.4 gesondert eingegangen.

2.3. Zulässige Zweckänderung

Grundsätzlich dürfen personenbezogene Daten nur zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden. Zusätzlich sieht der Gesetzgeber vor,

dass durch Einwilligung des Betroffenen eine Legalisierung der Zweckänderung erfolgen kann. Dieser kann zum Beispiel bei Abschluss eines Vertrages einwilligen, dass seine Daten, bei Bedarf, auch zu Werbezwecken verwendet werden dürfen und ihm so regelmäßig Werbung zugesendet werden darf.

Eine Zweckänderung kann auch durch die Paragraphen 23, 24 und 25 BDSG-neu erlaubt sein. In der Praxis für Unternehmen relevant ist hierbei aber lediglich der §24 Absatz 1 Punkt 2. Dieser erlaubt eine Zweckänderung in Verbindung einer Erforderlichkeit zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche. Also immer dann, wenn es zum Beispiel darum geht, eine Forderung gerichtlich durchzusetzen oder unberechtigte Ansprüche abzuwehren, dürfen personenbezogene Daten verarbeitet werden, die zu einem anderen Zweck erhoben wurden. Erhebt ein Unternehmen also zum Beispiel Daten zum Zwecke der Vertragserfüllung und der Kunde weigert sich später zu zahlen, dürfen die Daten auch zur Geltendmachung des Zahlungsanspruches genutzt werden.

Als Dritte Möglichkeit der Zweckänderung sieht der Gesetzgeber vor, dass diese zulässig ist, wenn der neue Zweck mit dem ursprünglichen Zweck vereinbar ist. Hierbei trifft das Unternehmen die Pflicht, die Vereinbarkeit zu prüfen. Es ist also zu schauen, inwieweit eine Verbindung zwischen dem alten und neuen Zweck besteht, insbesondere das Verhältnis zwischen dem Betroffenen und Unternehmen und die vernünftigen Erwartungen der betroffenen Person. Auch mögliche Folgen der Weiterverarbeitung für den Betroffenen müssen berücksichtigt werden und mit viel Augenmaß, Treu und Glauben entschieden werden. Diese Überlegungen und ggf. ergriffene Maßnahmen zum Schutz der Daten müssen dokumentiert werden. Diese Möglichkeit der Zweckänderung steht im engen Zusammenhang mit dem zuvor gebrachtem Beispiel der Direktwerbung aufgrund eines berechtigten Interesses am Beispiel des Relaunches („Angebot an Bestandskunden“).

2.4 Besonders geschützte Daten

Der Artikel 9 DS-GVO verbietet die Verarbeitung besonderer Kategorien personenbezogener Daten. Diese sind definiert als Daten aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische, biometrische, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Ausrichtung. Gesondert geregelt werden Daten über strafrechtliche Verurteilungen und Straftaten (Artikel 10 DS-GVO), auf die an dieser Stelle aber nicht weiter eingegangen werden soll.

Es gibt jedoch auch hier Erlaubnistatbestände im Absatz 2 des Artikel 9 DS-GVO. Die für Unternehmen relevanten sind die wirksame und ausdrückliche Einwilligung des Betroffenen, Erfüllung von Pflichten im Rahmen eines Arbeitsverhältnisses und Wahrnehmung von Rechten und Pflichten im Rahmen des Sozialschutzes oder der sozialen Sicherheit. Hinzu kommen besondere Erlaubnistatbestände für Tendenzbetreibe, öffentlich jedermann zugängliche Daten, die die Person offensichtlich selbst öffentlich zugänglich gemacht hat, die Geltendmachung von Rechtsansprüchen und die individuelle Gesundheits- und Sozialvorsorge.

Auch an dieser Stelle sollen praktische Beispiele gebracht werden, in denen die Verarbeitung besonderer Datenkategorien durch den Gesetzgeber legalisiert sind.

Religiöse Überzeugungen und Mitarbeiter

Der Arbeitgeber muss Daten zu religiösen Überzeugungen seiner Mitarbeiter verarbeiten, nämlich dann, wenn es sich um die Abrechnung und Abfuhr von Kirchensteuer handelt. Eine Verarbeitung zu diesem Zweck ist erlaubt.

Gesundheitsdaten

Ist die Verarbeitung notwendig, um eine Beurteilung der Arbeitsfähigkeit eines Beschäftigten zu prüfen, so können diese Daten verarbeitet werden. Hierzu muss jedoch eine entsprechende Grundlage im Unionsrecht oder in einem Vertrag mit einem Angehörigen eines Gesundheitsberufes (z.B. Arzt) vorliegen. Praktische Anwendung findet dies zum Beispiel im Rahmen der Einstellung von Auszubildenden im Betrieb. Denn gemäß §32 Absatz 1

Jugendarbeitsschutzgesetz darf ein Jugendlicher, der in das Berufsleben eintritt, nur beschäftigt werden, wenn er innerhalb der letzten 14 Monate von einem Arzt untersucht worden ist und dem Arbeitgeber eine von diesem Arzt ausgestellte Bescheinigung vorliegt.

2.5 Auftragsverarbeitung

Eine Auftragsverarbeitung liegt vor, wenn ein anderes Unternehmen, Behörde, Einrichtung oder andere Stelle personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet. Voraussetzung ist, dass der Auftragsverarbeiter nur als verlängerter Arm des Verantwortlichen handelt, also nach dessen Vorgaben. Praktische Beispiele hierfür sind zum Beispiel ein Webhostinganbieter, Callcenter oder Aktenvernichter.

Abzugrenzen ist die Auftragsverarbeitung von einer Funktionsübertragung. Bei einer Funktionsübertragung übernimmt ein Dritter eigenverantwortlich die Verarbeitung und entscheidet selbst über Art und Umfang der Verarbeitung. Ein praktisches Beispiel hier ist der Steuerberater. Der Steuerberater erledigt den Jahresabschluss nicht nach den Vorgaben des Verantwortlichen, sondern eigenverantwortlich nach den Vorgaben des Gesetzes.

Doch Vorsicht: Nach allgemeinem Rechtsverständnis, kann die reine Erledigung der Entgeltabrechnung für Mitarbeiter von einem Lohnbüro nicht als Funktionsübertragung angesehen werden. In diesem Falle erhält das Lohnbüro lediglich Daten und erstellt nach Vorgaben des Verantwortlichen die Meldung an die Krankenkassen und Finanzämter. Hier ist von einer Auftragsverarbeitung auszugehen.

Bei Vorliegen einer Auftragsverarbeitung obliegen dem Auftraggeber besondere Pflichten nach den Artikeln 28 und 29 DS-GVO. Diese beinhalten die sorgfältige Auswahl des Auftragsverarbeiters und Abschluss eines Auftragsverarbeitungsvertrages zur Sicherstellung der Einhaltung datenschutzrechtlicher Bedingungen. Zu diesem Vertrag gibt es definierte Mindestinhalte: Den Gegenstand der Verarbeitung, Zweck, Art, Dauer, Kategorien der Betroffenen, Regelungen zur Weisungsgebundenheit des

Verarbeiters, Informationspflichten, Vertraulichkeit, Datensicherheit, Unterauftragsverarbeiter, Unterstützung bei Transparenzpflichten und Betroffenenrechten, Rückgabe und Löschung der Daten sowie zur Unterstützung bei Nachweispflichten, Ermöglichung von Prüfungen und Kontrollen und Informationspflichten bei Verstößen.

2.6 Betroffenenrechte

Der Gesetzgeber hat Betroffenen eine ganze Hand voll Rechte geben, die das Recht auf informationelle Selbstbestimmung wahren sollen.

Informationspflicht

Unternehmen müssen die Betroffenen über die Verarbeitung von personenbezogenen Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache unterrichten.

Hierbei wird unterschieden, ob die Daten selbst erhoben wurden oder bei einem Dritten. Erhebt das Unternehmen selbst die Daten, so muss zum Zeitpunkt der Datenerhebung entsprechender Informationspflicht nachgekommen werden, es sei denn, der Betroffene verfügt bereits über die jeweilige Information. Bei Erhebung der Daten durch einen Dritten, muss die Information innerhalb einer für die Verarbeitung angemessenen Frist übermittelt werden, höchstens jedoch binnen eines Monats.

Inhalt der entsprechenden Erklärung muss mindestens sein:

- Name und Kontaktdaten des Verantwortlichen, des Vertreters und ggf. Kontaktdaten des Datenschutzbeauftragten
- Zwecke und Rechtsgrundlage der Verarbeitung
- Bei Verarbeitung aufgrund berechtigter Interessen eine Darlegung der berechtigten Interessen
- Erklärung darüber, ob eine Datenübermittlung an Dritte stattfindet und Kategorien der Empfänger
- Bei Datenübermittlung in Drittländer gesonderte Informationen über die Absicht, Information zum Vorhandensein oder Fehlen eines

Angemessenheitsbeschlusses der Kommission, Verweis auf geeignete Garantien und wie eine Kopie davon zu erhalten ist
- Dauer der Speicherung
- Information zu den Betroffenenrechten
- Hintergrund für die Bereitstellung der Daten
- Informationen zur automatisierten Entscheidungsfindung (falls genutzt)
- Informationen zu beabsichtigten Zweckänderungen

Werden die Daten bei einem Dritten erhoben, kommen Ausnahmen von der Informationspflicht in Betracht:

- Die Erlangung und Offenlegung der Daten ist ausdrücklich durch eine Rechtsvorschrift geregelt, die geeignete Garantien zum Schutz der Betroffenen Person vorsieht
- Wenn der Empfänger dem Berufsgeheimnis einschließlich seiner satzungsgemäßen Geheimhaltungspflicht unterliegt

Das bedeutet für die Praxis, dass wenn ein Unternehmen Buchhaltungsunterlagen an den Steuerberater weitergibt, in denen personenbezogene Daten enthalten sind, muss der Steuerberater die Betroffenen nicht informieren, da er seinem Berufsgeheimnis unterliegt. Gleiches trifft beispielsweise auch auf Rechtsanwälte zu.

Anders wäre es jedoch bei zum Beispiel der Weitergabe von Daten an ein anderes, befreundetes Unternehmen, dass Kundendaten dazu nutzen möchte, jene Kunden zu kontaktieren. Sofern die Weitergabe überhaupt zulässig sein sollte, muss das Empfängerunternehmen die betroffenen Kunden darüber informieren.

In der Praxis erfolgt die Information vom Betroffenen im Internet (bei Besuch der Website / Bestellung im Onlineshop) in der Regel durch eine öffentlich zugängliche Datenschutzerklärung. Zu dieser ist in der Regel jeder Website-Betreiber verpflichtet, da in der Regel bereits beim Besuchen der Website personenbezogene Daten verarbeitet werden, zum Beispiel durch Server-Logfiles, die die IP-Adresse des Besuchers verarbeiten und eine Identifikation der Person anhand jener wenigstens theoretisch möglich ist.

Bei urschriftlicher Unterzeichnung von Verträgen oder ähnlichem bietet es sich an, ein Beiblatt zum Vertrag anzufertigen und auf jenem über die Verarbeitung zu informieren und der Informationspflicht nachzukommen.

Recht auf Auskunft

Betroffene haben ein Recht auf Auskunft darüber, welche personenbezogenen Daten von ihnen zu welchem Zweck verarbeitet werden, woher die Daten stammen und ob Daten von ihnen an Dritte weitergegeben werden. Ein entsprechendes Ersuchen ist umgehend und binnen höchstens 4 Wochen nachzukommen.

Recht auf Berichtigung

Da aufgrund von falschen Daten erhebliche Nachteile für Betroffene entstehen können, sieht der Gesetzgeber die Gewährleistung des Grundsatzes der Richtigkeit der verarbeiteten Daten vor. Betroffene können eine unverzügliche Berichtigung personenbezogener Daten fordern und ferner eine Vervollständigung jener, soweit dies im Hinblick auf die jeweilige Verarbeitung angemessen ist. Zu beachten gilt hierbei, dass wenn der Betroffene die Richtigkeit der Daten bestritten hat, jene solange gesperrt werden müssen, bis der Verantwortliche eine Feststellung über die Richtigkeit oder Unrichtigkeit der Daten getroffen hat.

Recht auf Löschung

Ist der Zweck der, zudem die Daten erhoben wurden, erloschen, liegt ein Widerruf der Einwilligung in die Verarbeitung vor oder legt der Betroffene Widerspruch gegen die Verarbeitung ein, so ist der Verantwortliche verpflichtet die personenbezogenen Daten unverzüglich zu löschen.

Ausnahmen, die für Unternehmen relevant sein dürften, sind hier rechtliche Verpflichtungen und die Geltendmachung von Ansprüchen. Werden die Daten also noch zur Erfüllung gesetzlicher Pflichten (z.B. Aufbewahrungspflicht im Steuerrecht) oder zur Geltendmachung von Ansprüchen (z.B. Inkasso) benötigt, darf das Unternehmen die betroffenen Daten bis zur abschließenden Erfüllung dieser Pflicht oder Befriedigung des Anspruches weiter verarbeiten.

Recht auf das Vergessenwerden

Hat ein Verantwortlicher personenbezogene Daten öffentlich gemacht, hat er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten alle angemessene Maßnahmen zu treffen, um das Recht auf das Vergessenwerden umsetzen, wenn entsprechender Antrag der betroffenen Person erfolgt.

Recht auf Einschränkung der Verarbeitung

Der Verantwortliche hat die Verarbeitung von personenbezogenen Daten einzuschränken, wenn die Richtigkeit der Daten bestritten wird, die Verarbeitung unrechtmäßig ist oder ein Widerspruch der Person vorliegt und noch geprüft werden muss, ob ein Grund gegen die Löschung spricht.

Recht auf Datenübertragbarkeit

Betroffene können verlangen, von denjenigen personenbezogenen Daten, die sie dem Unternehmen bereitgestellt haben, eine Kopie in einem strukturierten, gängigen und maschinenlesbarem Format zu erhalten oder zu verlangen es einem anderen Verantwortlichen zu übermitteln.

Widerspruchsrecht in die Verarbeitung

Betroffene können gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einlegen. Die Folge ist, dass der Verantwortliche jene Daten nicht mehr verarbeiten darf. Es sei denn es liegen zwingende schutzwürdige Gründe des Verarbeiters vor (vergleiche Recht auf Löschung: Geltendmachung Ansprüche & gesetzliche Verpflichtungen)

Rechte bei automatisierten Entscheidungen

Betroffene haben bei automatisierte Entscheidungen, die ihnen gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise beeinträchtigen, das Recht, ein Eingreifen einer Person seitens des Verantwortlichen zu verlangen. Zusätzlich ist über die Vorgehensweise und Maßstäbe der automatisierten Entscheidungen zu informieren.

2.7 Datenübermittlung in Drittländer

Die DS-GVO erlaubt die Datenübermittlung von personenbezogenen Daten innerhalb der Europäischen Union und für eine rechtskonforme Übermittlung ist lediglich das Erfüllen eines Erlaubnistatbestandes gemäß Artikel 6 DS-GVO und ggf. ein Auftragsverarbeitungsvertrag notwendig. Dies wird durch die EU-weite Anwendung der DS-GVO und das damit einhergehende homogene Datenschutzrecht möglich.

Die DS-GVO regelt für die Weitergabe von personenbezogenen Daten in ein Land außerhalb der EU jedoch weitere Anforderungen, die im Artikel 44 ff. DS-GVO geregelt sind. Neben der Prüfung des allgemeinen Erlaubnistatbestandes nach Artikel 6 DS-GVO ist an zweiter Stelle eine Feststellung notwendig, ob in dem Drittland, oder zumindest bei dem konkreten Empfänger der Daten im Drittland, ein angemessenes Datenschutzniveau gegeben ist. Hiervon ist regelmäßig auszugehen, wenn Angemessenheitsbeschlüsse (Art. 45 DS-GVO) oder geeignete Garantien (Art. 46 DS-GVO) vorliegen.

Bei einem Angemessenheitsbeschluss stellt die EU-Kommission fest, ob ein bestimmtes Drittland, ein oder mehrere Sektoren in diesem Drittland oder eine internationale Organisation ein angemessenes Datenschutzniveau im Sinne der DS-GVO aufweist. Eine entsprechende Übersicht ist auf der Seite der EU-Kommission abrufbar.

Bezüglich des Datentransfers in die USA gibt es eine Besonderheit: Mit dem EU-US Privacy Shield haben die EU und USA sich auf ein Zertifizierungsverfahren von Unternehmen in den USA geeinigt, dass es EU-Unternehmen möglich macht, personenbezogene Daten an zertifizierte US-Unternehmen zu übermitteln. Unter privacyshield.gov/list kann man prüfen, ob eine Weitergabe von Daten an ein bestimmtes Unternehmen in den USA zulässig ist und es somit über ein angemessenes Datenschutzniveau verfügt. Diese Zertifizierung muss jährlich wiederholt werden. Daher muss das EU-Unternehmen sich regelmäßig vergewissern, ob das US-Unternehmen weiterhin über das Zertifikat verfügt.

Alternativ können Garantien, die geeignet sind, um ein ausreichendes Datenschutzniveau zu gewährleisten, vorhanden sein und die Übermittlung

ermöglichen. Dies sind zum Beispiel verbindliche interne Datenschutzvorschriften, EU-Standardvertragsklauseln, Standardvertragsklauseln der Aufsichtsbehörden oder anerkannte Zertifizierungen des Unternehmens.

2.8 Aufsichtsbehörden

Die DS-GVO macht es für jeden Staat zur Pflicht mindestens eine Aufsichtsbehörde für den Bereich Datenschutz zu errichten und jene personell, technisch und finanziell angemessen auszustatten. In Deutschland ist dies schon länger der Fall. Zuständig für das jeweilige Unternehmen in Deutschland ist die Datenschutzbehörde des jeweiligen Bundeslandes, in dem das Unternehmen seinen Sitz hat.

Der Aufgabenkatalog der Aufsichtsbehörden ist lang. Besonders herauszustellen sind aber die Sensibilisierung und Aufklärung der Öffentlichkeit, der Verantwortlichen und Auftragsverarbeiter, das Führen von internen Verzeichnissen über Verstöße und ergriffene Maßnahmen, das Erleichtern von Beschwerden und die Erstellung von jährlichen Tätigkeitsberichten. Zusätzlich sieht die DS-GVO im Artikel 58 Untersuchungs-, Abhilfe-, Genehmigungs- und beratende Befugnisse vor. So prüft die jeweilige Aufsichtsbehörde die Einhaltung einschlägiger Datenschutzgrundsätze und kann bei Verstößen auch Bußgelder verhängen.

2.9 Rechtsfolgen & Pflichten bei Verstößen

Kommt es im Unternehmen zu einem Datenschutzverstoß, trifft das Unternehmen eine Pflicht zur unverzüglichen Benachrichtigung der Datenschutzbehörde (binnen 72 Stunden), es sei denn, die Verletzung führt nicht zu einem Risiko für die Rechte und Freiheiten von natürlichen Personen.

Ein denkbares Beispiel, eines Verstoßes, der nicht zu einer Meldepflicht führt, ist der temporäre Verlust eines verschlüsselten USB-Sticks mit Kundendaten. Wurde dieser lediglich verlegt und lag einen Tag lang unentdeckt im Tresor und

es ist auszuschließen, dass Daten in Augenschein genommen oder geklaut werden konnten, ist davon auszugehen, dass kein Risiko für die Rechte und Freiheiten von natürlichen Personen entstanden ist. Dennoch trifft das Unternehmen die Pflicht dies zu prüfen und diese Prüfung umfassend zu dokumentieren.

Hat ein Datenleck ein hohes Risiko für Betroffene, müssen jene, neben der Datenschutzbehörde, ebenso informiert werden. Eine Ausnahme besteht nur, wenn eine individuelle Benachrichtigung bei einer großen Zahl von Betroffenen unverhältnismäßig ist. In diesem Fall ist eine öffentliche Bekanntmachung vorgesehen.

Unternehmer stehen bei Datenschutzverstößen im Risiko der zivilrechtlichen Haftung mit einer mit der Beweislastumkehr versehenen Verschuldenshaftung. Neu in der Gesetzgebung ist zusätzlich die ausdrücklich beschriebene Haftung auch auf immaterielle Schäden.

Zusätzlich haftet das Unternehmen auch im Rahmen von Ordnungswidrigkeiten. Das materielle Datenschutzrecht soll mit Zähnen versehen werden und kein Papiertiger bleiben. Die Bußgeldrahmen und die Zahl der Bußgeldtatbestände wurden bemerkenswert erhöht. Bußgelder betragen nunmehr bis zu 20 Millionen Euro oder 4% des weltweiten Vorjahresumsatzes. Sanktioniert werden können die Verantwortlichen, Auftragsverarbeiter sowie Überwachungs- und Zertifizierungsstellen.

Anhand der Höhe der Bußgelder kann man erkennen, dass die DS-GVO ein wichtiges Instrument ist, um auch Weltkonzerne bei Verstößen empfindlich treffen zu können.

Ferner drohen Unternehmen und deren Akteuren strafrechtliche Haftung. Hierzu gibt es zum Beispiel selbständige Straftatbestände aus dem Strafgesetzbuch oder dem BDSG-neu, wie zum Beispiel das Ausspähen von Daten, Datenhehlerei und die Verletzung des Briefgeheimnisses.

Derzeit verstärkt in der Diskussion ist die Abmahnfähigkeit von Verstößen durch Mitbewerber. Es gab zwar bereits die ersten Anwälte, die zum Beispiel wegen einer fehlenden Datenschutzerklärung auf der Website oder der externen Einbindung von Google-Fonts auf Websites abgemahnt haben, dennoch gibt es

Stimmen, die sagen, dass die DS-GVO keine Grundlage für Abmahnungen sein kann. Zusätzlich ist ein Schutz vor Abmahnungen durch den Gesetzgeber angedacht.

2.10 Dokumentationspflichten

Die DS-GVO schafft für Unternehmen umfassende Dokumentations- und Rechenschaftspflichten.

So muss unter anderem ein Verzeichnis der Verarbeitungstätigkeiten geführt werden. Eine Pflicht zum Führen entfällt nur für Unternehmen mit weniger als 250 Mitarbeitern, in denen die automatisierte Verarbeitung von personenbezogenen Daten nur gelegentlich erfolgt. Dank moderner Kommunikation u.Ä. dürfte diese Pflicht aber nahezu jedes Unternehmen betreffen, da bereits das Betreiben eines E-Mailaccounts zu einer nicht nur gelegentlichen Verarbeitung führen dürfte.

Vorgeschrieben ist eine schriftliche Form, was aber auch in einem elektronischen Format erfolgen kann. Das Verzeichnis ist der Aufsichtsbehörde auf Verlangen zur Verfügung zu stellen und dient jener dazu, sich einen ersten Einblick in das Unternehmen zu verschaffen.

In dem Verzeichnis der Verarbeitungstätigkeiten sind alle Prozesse im Unternehmen zu dokumentieren, in denen personenbezogene Daten verarbeitet werden. Der Mindestinhalt setzt sich wie folgt zusammen:

- Name und Kontaktdaten des Verantwortlichen, des ggf. gemeinsam Verantwortlichen, des Vertreters des Verantwortlichen sowie des Datenschutzbeauftragten
- Zweck der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und Kategorien der personenbezogenen Daten
- Kategorien an Empfängern der Daten
- Angaben zur Übermittlung ins Drittland
- Frist zur Löschung der Daten

- Beschreibung der allgemeinen technischen und organisatorischen Maßnahmen (TOMs) zum Schutz der Daten

Den TOMs kommt grundsätzlich eine sehr wichtige Rolle zu. Zum einen sind sie im Verarbeitungsverzeichnis zu benennen und zu dokumentieren, zum anderen sind Mechanismen im Unternehmen zu entwickeln, die die Wirksamkeit dieser sicherstellen. Die DS-GVO sieht die Vertraulichkeit und Integrität der personenbezogenen Daten vor. Um dies zu gewährleisten, sind der Einsatz sicherer Technologien (aktueller Virenschutz, verschlüsselte Übertragung & Speicherung), Zugriffs- und Zutrittsbeschränkungen, Backupkonzepte etc. notwendig.

Birgt eine Datenverarbeitung voraussichtliche hohe Risiken für die persönlichen Rechte und Freiheiten natürlicher Personen, muss der Verantwortliche vorab eine Datenschutz-Folgenabschätzung (DS-FA) durchführen. Dies ist regelmäßig beim Einsatz neuer Technologien, Verarbeitung großer Datenmengen, einer hohen Zahl von betroffenen Personen, Profiling, bei umfangreicher Verarbeitung besonderer Datenkategorien und systematischer Kameraüberwachung der Fall.

Die Datenschutzbehörden sind angehalten verbindliche Positiv- und Negativlisten für die Notwendigkeit einer Datenschutz-Folgenabschätzung anzufertigen. Dies ist bislang in Deutschland noch nicht geschehen und bleibt abzuwarten. Bis dahin ist es empfehlenswert im Zweifel immer eine Folgenabschätzung durchzuführen.

Die DS-FA muss zumindest eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und Zwecke der Verarbeitung sowie die vom Verantwortlichen verfolgten Interessen beinhalten. Es wird ferner die Notwendigkeit und Verhältnismäßigkeit der geplanten Vorgänge bewertet und die möglichen Risiken der Verarbeitung dargelegt. Die DS-FA umfasst auch die Maßnahmen zur Risikoverringerung und legt dar, ob diese auf das notwendige Maß reduziert wurden. Bei dem Prozess der Erstellung sind betroffene Personen und der Datenschutzbeauftragte im Unternehmen anzuhören und zu beteiligen.

Kommt die DS-FA zu dem Ergebnis, dass trotz der ergriffenen Maßnahmen ein hohes Risiko für die Betroffenen besteht, muss die zuständige Datenschutzbehörde konsultiert werden.

Zusätzlich zum Verzeichnis der Verarbeitungstätigkeiten und DS-FA sollte das Unternehmen auch alle anderen Tätigkeiten zum Thema Datenschutz, z.B. Mitarbeiterschulungen, Festlegung von IT-Sicherheitsrichtlinien etc., dokumentieren und jederzeit griffbereit haben.

2.11 Datenschutzbeauftragter

Die DS-GVO sieht die Bestellung eines Datenschutzbeauftragten auf jeden Fall in folgenden Fällen vor:

- die Verarbeitung erfolgt durch eine Behörde oder öffentlichen Stelle, mit Ausnahme von Gerichten
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters liegt in der Durchführung von Verarbeitungsvorgängen, welche aufgrund ihrer Art, ihres Umfangs oder Zwecke eine umfangreiche regelmäßige und systematische Überwachung von Personen erforderlich macht
- die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters liegt in der umfangreichen Verarbeitung besonderer Kategorien an Daten oder in der umfangreichen Verarbeitung von personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten

Das BDSG-neu geht im §38 ein wenig weiter und schreibt einen Datenschutzbeauftragten zusätzlich vor, wenn in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Dabei ist die Art und der Umfang der Beschäftigung der Personen egal. Es wird nach Köpfen gezählt, unabhängig davon, ob es sich um einen Mini-Jobber, Vollzeitkraft oder Freelancer handelt. Zusätzlich ist die Benennung obligatorisch, wenn eine Verarbeitung vorliegt, die einer Datenschutz-Folgenabschätzung bedarf oder personenbezogene Daten geschäftsmäßig zum Zweck der Markt- oder Meinungsforschung verarbeitet werden.

Ein Datenschutzbeauftragter (DSB) kann grundsätzlich intern oder extern bestellt werden. Gemeinsam haben aber beide, dass der DSB in der Lage sein muss seine Arbeit objektiv und unabhängig durchzuführen. Daher scheiden Abteilungsleiter oder die Geschäftsleitung des Unternehmens in der Regel aus. Der DSB muss ferner fachlich in der Lage sein, seinen Verpflichtungen nachzukommen (Datenschutzrecht & IT).

Der Gesetzgeber sieht Mindestpflichten für den DSB vor. Dies sind unter anderem die Information und Beratung des Verantwortlichen, die Überwachung der Einhaltung der Datenschutzvorschriften, Beteiligung bei einer DS-FA, die Zusammenarbeit mit den Aufsichtsbehörden und die Risikobeurteilung von Verarbeitungsvorgängen. Der DSB arbeitet auf die Einhaltung einschlägiger Datenschutzbestimmungen hin, ist aber nicht für den Erfolg der Maßnahmen verantwortlich. Diese bleibt beim Verantwortlichen.

Ist ein DSB bestellt, so muss dieser der Aufsichtsbehörde gemeldet und seine Kontaktdaten auf der Website und in der Datenschutzerklärung genannt werden.

Kapitel 3: Schaffung der Complience im Unternehmen

Nachdem die neue Gesetzeslage umfangreich betrachtet wurde, soll in diesem Kapitel die Umsetzung notwendiger Maßnahmen in der Praxis behandelt werden. In nahezu jedem Unternehmen sind durch die neuen Vorschriften Anpassungen notwendig.

Wie es bei jeder Veränderung in einem Unternehmen ist, gibt es auch auf dem Weg zur Datenschutz-Complience eine Vielzahl möglicher Konflikte. Denkbar sind Verteilkonflikte, da die Umsetzung der DS-GVO Zeit und ggf. Geld kostet, das auch an anderer Stelle benötigt wird, Zielkonflikte, da beispielsweise Ziele der Marketingabteilung in Konkurrenz zu Datenschutzzielen stehen (z.B. im Rahmen der Datenminimierung) und natürlich auch Rollenkonflikte. Zudem bedeutet die Umsetzung des neuen Datenschutzrechts natürlich auch Mehrarbeit. Dies kann zu Widerständen führen, insbesondere, wenn bei den Beteiligten die Erkenntnis über die Sinnhaftigkeit der Maßnahmen ausbleibt. Die Betroffenen im Unternehmen sollten daher umfangreich informiert und beteiligt werden.

In der Praxis zeigt sich, dass sich bei kleinen Unternehmen, meist ein einzelner Mitarbeiter um die Umsetzung notwendiger Maßnahmen kümmert. Vereinzelt werden noch IT-Dienstleister hinzugezogen.

Grundsätzlich stellt die Datenschutz-Complience keinen einmaligen Prozess dar, der einmalig Maßnahmen notwendig macht, sondern vielmehr einen kontinuierlichen Prozess. Denn sobald Neuerungen im Unternehmen anfallen, müssen diese ebenso geprüft werden. Der Fortschritt der Technik bringt neue Technologien hervor, die ggf. implementiert werden und auch die Erfüllung der Dokumentationspflichten sieht routinemäßige Checks und Aktualisierungen vor.

In größeren Unternehmen, in denen die Erbringung dieser Leistungen nicht mehr durch einen Einzelnen möglich ist, empfiehlt sich daher die Schaffung einer Matrixorganisation. Sodass die „Taskforce Datenschutz“ in jeder verrichtungsbezogenen Abteilung (Einkauf, Marketing, Buchhaltung etc.) auch über ein Mitarbeiter, der neben seiner eigentlichen Funktion in jener, zugleich

auch für den Bereich Datenschutz in dieser Abteilung zuständig ist, verfügt, der mit umfassenden Abteilungswissen über die anfallenden Prozesse in der Realität, regelmäßig berichterstatten und bei Bedarf direkt Handlungsempfehlungen aussprechen kann. Gesteuert und geführt werden sollte diese objektbezogene Ebene an Mitarbeitern, aus allen verrichtungsbezogenen Abteilungen, durch einen Datenschutzmanager, der ggf. zugleich auch Datenschutzbeauftragter des Unternehmens ist.

3.1 3-Phasen-Modell Kurt Lewin

Kurt Lewin formulierte 1947 in seinem Artikel „Frontiers in group dynamics“ ein 3-Phasen-Modell und stellt die Veränderung in Unternehmen in drei Phasen dar. Dieses Modell hat sich in der Realität bewährt und gliedert sich in die Phasen Unfreezing, Moving und Refreezing.

Für die Umsetzung der Datenschutz-Complience bietet sich ein Vorgehen nach diesem Muster an und soll an dieser Stelle beschrieben werden.

In der ersten Phase des Unfreezings werden bisherige Strukturen „aufgetaut“. Es geht vor allem um das Vorbereiten einer Veränderung und so werden Betroffene über die aktuellen Pläne informiert, in Diskussionen miteinbezogen und so zu Beteiligten gemacht. Zudem finden vorbereitende Analysen statt. Ziel dieser Phase ist es, eine Beteiligung der Mitarbeiter zu erreichen und möglichen Widerständen vorzubeugen. In dem durch mich dargestellten Vorgehen, findet sich diese Phase in den Unterkapiteln 3.2 „Kick-Off & Mitarbeiterinformation“ bis 3.5 „Bewertung & Analyse der Prozesse“ wieder.

Darauf folgt die Phase des Movings. Dies ist die Phase des Modells, in der es zur Umsetzung der eigentlichen Veränderungen kommt. In dieser Arbeit in den Kapiteln 3.6 bis 3.10 wiederzufinden.

Die letzte Phase nach Kurt Lewin, das Refreezing, dient dem Verfestigen der neuen Strukturen und Abläufe, sowie der Überwachung, ob das Neue auch funktioniert und aufrechterhalten wird. Dies findet sich in den Kapiteln 3.11 und 3.12 wieder.

Doch, wie schon beschrieben, darf danach nicht Schluss sein. Im Bereich des Datenschutzes ist eine ständige Evaluierung, Kontrolle und Anpassung notwendig, die über das beschriebene Maß des 3-Phasen-Modells hinaus geht und sich vielmehr als ein sich ständig wiederholender Prozess darstellt.

3.2 Kick-Off & Mitarbeiterinformation

Es geht in dieser Phase darum, die Mitarbeiter im Unternehmen über die bevorstehenden Veränderungen zu informieren und die Sinnhaftigkeit und Notwendigkeit dieser zu kommunizieren. Es sollte zu einer Kick-Off-Veranstaltung kommen, in der möglichst viele Mitarbeiter erreicht, zum neuen Datenschutzrecht informiert und aus Zuschauern Beteiligte gemacht werden. Fragen der Mitarbeiter sollten erlaubt sein und jene auch gefragt werden, welche Prozesse in ihren Abteilungen existieren, in denen personenbezogene Daten verarbeitet werden. Auch ein Vorschlagswesen sollte ermöglicht werden. Hat ein Mitarbeiter eine Idee zur Umsetzung oder eine Schwachstelle erkannt, sollte hierüber offen diskutiert werden können.

Dies hilft dabei Widerständen vorzubeugen und sorgt, bei guter Umsetzung, dafür, dass sich die Mitarbeiter auch eigenständig bereits Gedanken zum Thema Datenschutz machen, sodass, wenn ein Beauftragter zur Prüfung der Prozesse auf jenen Mitarbeiter trifft, er unter Umständen bereits mit sachdienlichen Informationen auftrumpfen kann. Dies kann den Prozess der Bestandsaufnahme und Analyse der Prozesse erheblich beschleunigen.

In kleinen Unternehmen mit bis zu 10 Mitarbeitern sollten alle Mitarbeiter direkt beteiligt und auch zur Kick-Off-Veranstaltung eingeladen werden. Bei einem größeren Personalstamm empfiehlt es sich die jeweiligen Abteilungsleiter und die Geschäftsführung in einer ersten Kick-Off-Veranstaltung zu beteiligen und jene dann in ihrer jeweiligen Abteilung die betreffenden Mitarbeiter zu informieren und beteiligen zu lassen. Kommt es dann in der jeweiligen Abteilung zu sachdienlichem Feedback, sollte das Abteilungs-Leiter-Event wiederholt werden und das erhaltene Feedback dort diskutiert und zusammengetragen werden.

3.3 Der Datenschutzbeauftragte

Schon vor der Bestandsaufnahme und Bewertung der Prozesse, sollte geprüft werden ob eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht (Kapitel 2.11) oder ob die Bereitschaft besteht auch ohne Pflicht einen zu benennen. Denn der Datenschutzbeauftragte (DSB) ist eine sehr nützliche Hilfe bei den bevorstehenden Vorgängen und kann jene durch sein Fachwissen beschleunigen.

Die Anforderungen an einen DSB wurden bereits in vorhergehenden Kapiteln beschrieben. Es stellt sich an dieser Stelle jedoch noch die Frage, ob er extern oder intern bestellt werden soll.

Die Vorteile der internen Bestellung liegen auf der Hand: Der Mitarbeiter kennt das Unternehmen bereits und Mitarbeiter haben in der Regel Vertrauen zu ihm. Die Nachteile jedoch können die Betriebsblindheit, der besondere Kündigungsschutz, geringe Haftung und die möglicherweise fehlende Fachkompetenz sein. Durch letztere wird eine Schulung / Weiterbildung des Mitarbeiters notwendig, die natürlich mit Kosten verbunden ist und Zeit kostet.

Vorteile einer externen Bestellung sind die in der Regel hohe die Fachkompetenz des externen DSB, die gesammelten Erfahrungen und der Blick von außen auf das Unternehmen. Der größte Vorteil jedoch ist die Haftung des externen DSB. Haftet der interne DSB lediglich für grobe Fahrlässigkeit und Vorsatz, kann der externe DSB umfangreicher in Haftung genommen werden. Daher sollte bei der Auswahl des externen DSB auf einen ausreichenden Versicherungsschutz (Vermögensschadenhaftpflicht) geachtet werden.

Die Zahl der externen DSB, die ihre Dienste anbieten ist derzeit explodiert. Nahezu jeder IT-Dienstleister hat einen Zertifikatslehrgang besucht und bietet nunmehr seine Dienste an. An dieser Stelle sei davor gewarnt, einen IT-Dienstleister als externen DSB zu bestellen. Zum einen kann es zu Interessenskonflikten und fehlender Objektivität kommen, wenn der Dienstleister zugleich auch die IT in dem Unternehmen wartet und zum Anderen darf offen bezweifelt werden, dass der jeweilige Dienstleister fachlich und methodisch das Handwerkszeug hat, um eine professionelle Beratung zu gewährleisten. Ganz sicher ist er im Bereich der Informationstechnologie fit.

Jedoch darf bezweifelt werden, dass z.B. in einem 3-tägigen Web-Based-Training oder Workshop die Komplexität des neuen Datenschutzrechts und das notwendige methodische Handwerkszeug ausreichend vermittelt wurde. Dennoch sind sie als zusätzliche Berater für den Bereich IT durchaus empfehlenswert. Besser für die Position als DSB geeignet sind Beratungsunternehmen, die seit Jahren im Bereich Datenschutz tätig sind und Rechtsanwälte, die sich auf den Bereich Datenschutz spezialisiert haben.

Ist ein DSB bestellt, so bietet es sich an, ihm auch die Aufgabe des Anlegens und Führens des Verzeichnisses der Verarbeitungstätigkeiten aufzuerlegen.

3.4 Bestandsaufnahme der betroffenen Prozesse

Als nächstes geht es an die Bestandsaufnahme aller Prozesse, in denen personenbezogene Daten verarbeitet werden. Personenbezogene Daten sind zum Beispiel Namen, Adressen, Telefonnummern, E-Mailadressen, IP-Adressen, Sozialversicherungs- und Steueridentifikationsnummern, KFZ-Kennzeichen und vieles mehr.

Es geht in dieser Phase darum, die betreffenden Prozesse zu identifizieren und aufzulisten. Empfehlenswert ist es, diesen Vorgang abteilungsweise durchzuführen. In Gesprächen mit den jeweiligen Abteilungsleitern und Mitarbeitern wird jeder Prozess angesehen und geschaut, ob in ihm personenbezogene Daten verarbeitet werden. So erhält man einen ersten Überblick darüber, wo personenbezogene Daten anfallen. Zudem können ähnliche oder identische Vorgänge geclustert werden, sodass jene ggf. gesammelt als ein Prozess in das Verzeichnis der Verarbeitungstätigkeiten eingehen und nicht doppelt geprüft werden müssen. Ebenso in der ggf. notwendigen Datenschutz-Folgenabschätzung dürfen gleiche oder ähnliche Prozesse zusammengeführt werden. Dies erspart unnötige Mehrarbeit.

Doch, was sind das für Prozesse, die typischerweise anfallen? An dieser Stelle folgt eine kleine Auflistung möglicher Verarbeitungstätigkeiten:

- Betreibern einer Website & Social-Media-Kanäle
- Bearbeitung von E-Mails

- Angebote schreiben
- Rechnungen schreiben
- Erledigung der Buchhaltung
- Entgeltabrechnung der Arbeitnehmer
- Betreiben eines CRM-Systems
- Beantworten von telefonischen Anfragen
- Abwicklung von Reklamationen
- Werbemailings an Kunden

Zusätzlich zu der reinen Auflistung der Tätigkeiten, sollten Verantwortlichkeiten mit angegeben oder, falls noch nicht geschehen, definiert werden. Dies soll Antwort darüber geben, wer z.B. für die Erledigung der Buchhaltung federführend und verantwortlich ist. Exakt diese Person ist dann auch Ansprechpartner für denjenigen, der das Verzeichnis der Verarbeitungstätigkeiten führt. Dies könnte zum Beispiel im Falle der Erledigung der Buchhaltung der Leiter der Buchhaltungsabteilung sein.

Grundsätzlich sieht die DS-GVO zwar vor, dass der jeweilige Verantwortliche für die Verarbeitung die Vorgangsbeschreibung im Verzeichnis der Verarbeitungstätigkeiten anlegt und pflegt, jedoch sieht sie auch vor, dass dies an den Datenschutzbeauftragten delegiert werden kann. Von dieser Möglichkeit sollte auch Gebrauch gemacht werden, da sonst jeder für die Verarbeitung Verantwortliche extra geschult werden müsste, um überhaupt in der Lage sein zu können, diese Dokumentation rechtlich einwandfrei durchzuführen.

Sobald diese Auflistung der Verarbeitungstätigkeiten vorliegt und die jeweiligen Verantwortlichen definiert sind, kann es an die Bewertung und Analyse der Prozesse gehen.

3.5 Bewertung & Analyse der Prozesse

Nunmehr geht es daran jeden Prozess einzeln für sich zu prüfen. Dies sollte, wenn möglich, gemeinsam mit dem Datenschutzbeauftragten erfolgen, der in dieser Phase beispielsweise von Tag zu Tag die nächste Abteilung besucht, konsultiert und gemeinsam mit dem Verantwortlichen diese Analyse durchführt.

Grundsätzlich sollte erst einmal geschaut werden, welche Daten überhaupt verarbeitet werden und zu welchem Zweck dies erfolgt. Es muss geprüft werden, ob alle dafür verarbeiteten Daten auch wirklich notwendig sind. Beispielsweise ist für eine Reservierung in einem Restaurant nicht das Geburtsdatum des Kunden notwendig. Daten, die für die Erfüllung des Zweckes nicht notwendig sind, sind fortan nicht mehr zu verarbeiten, bzw. eine Legitimation der Verarbeitung durch eine Einwilligung zu erwirken.

Nunmehr geht es daran, die Rechtsgrundlage der Verarbeitung zu definieren. An dieser Stelle sei nochmal an die Erlaubnistatbestände aus Kapitel 2.2 verwiesen. Beispielsweise könnte die Rechtsgrundlage die Erfüllung eines Vertrages sein.

Es muss ferner geprüft werden, wie lange die Daten gespeichert werden und ob Löschroutinen existieren, die sicherstellen, dass die Daten nur solange vorhanden sind, wie sie zum Zwecke der Verarbeitung benötigt werden oder eine Aufbewahrungspflicht (z.B. Steuerrecht) existiert. Eine Alternative zum Löschen könnte auch eine Anonymisierung sein. Sollen beispielsweise längerfristige Auswertungen ermöglicht werden, kann durch die Anonymisierung der Daten der Personenbezug wegfallen und somit eine unbegrenzte Speicherung ermöglicht werden (z.B. für Umsatz- & Auslastungsauswertungen).

Auch Datenweitergaben sollten geprüft werden und geschaut werden, wer auf die Daten Zugriff bekommt. Sind es verschiedene Abteilungen oder gar Externe, an die die Daten weitergegeben werden? Auch hier muss das Vorliegen einer gesetzlichen Legitimation geprüft werden. Empfänger der Daten oder Personen, die unnötiger weise Zugriff auf diese Daten haben könnten, müssen geprüft und dokumentiert werden.

Ferner muss geschaut werden, ob die Betroffenen (Kunden, Interessenten etc.) über die Verarbeitung informiert wurden und, falls eine Einwilligung vorliegt, diese DS-GVO-konform ist und dokumentiert wurde. Ist dies nicht geschehen, muss dies nachgeholt werden.

Wenn besondere technische oder organisatorische Maßnahmen zum Schutz der Daten, speziell zu diesem Prozess vorliegen, sollte dies auch dokumentiert

werden. Es ist zu prüfen, ob die Verarbeitung an sich nach heutigem Stand der Technik ausreichend geschützt ist. Dieser Schutz kann zum Beispiel durch Zugriffsbeschränkungen, Backuplösungen, die verschlüsselte Speicherung und Übertragung und natürlich entsprechende Schutzsoftware umgesetzt werden. Es muss geschaut werden, ob diese Maßnahmen ausreichen, um den Schutz und die Integrität der Daten zu gewährleisten.

Diese Bestandsaufnahme samt Analyse sollte nicht geschönt werden. Es geht um die Aufnahme und Dokumentation des aktuellen und tatsächlich Standes im Unternehmen und das Erkennen von Handlungsbedarf.

Sind Defizite, Schwachstellen oder gar Rechtsverstöße zutage gekommen, geht es im nächsten Schritt darum, diese zu beseitigen.

3.6 Anpassen der Prozesse

Erkannte Schwachstellen und Verstöße in der Verarbeitung müssen in dieser Phase angegangen werden. Rechte in den IT-Systemen müssen geändert werden, nicht notwendige Daten gelöscht und Datenweitergaben unterbunden werden, sofern sie nicht zulässig sind. Ein Heilmittel kann auch eine Einwilligung der Betroffenen sein. Beispielsweise kann es sinnvoll sein, jene anzuschreiben und eine schriftliche Einwilligung in die Verarbeitung einzuholen, wenn die Daten zum Beispiel länger als zulässig oder umfangreicher als notwendig verarbeitet werden.

Denkbare notwendige Maßnahmen könnten zum Beispiel auch die Verschlüsselung der Datenbank, Umstrukturierung des Ablaufes, das Anonymisieren von Daten oder gar die Einstellung des Prozesses sein.

An dieser Stelle einmal eine Darstellung von eine bespielhaft notwendigen Anpassung.

Ergebnis der Bestandsaufnahme

Prozess:	Terminvereinbarung mit Kunden per Whatsapp vom Firmenhandy des Außendienstmitarbeiters
Zweck:	Durchführung von Dienstleistungsverträgen
Rechtsgrundlage:	Vertragserfüllung
Einwilligung:	Nicht vorhanden
Löschung der Daten:	Nicht vorgesehen
Information des Kunden:	Nicht erfolgt
Weitergabe der Daten:	WhatsApp Inc. (Drittland, zertifiziert gem. US-EU-Privacy Shield)
Verarbeitete Daten:	Name, Telefonnummer, Zuletzt online, Onlinestatus, ggf. Foto, Inhaltsdaten

Ermittelte Schwachstellen

Datenminimierung nicht beachtet (Verarbeitung von Foto, Onlinestatus, Zuletzt online nicht für den Zweck erforderlich; zusätzlich bei allgemeiner Nutzung von Whatsapp Datenweitergabe aller Telefonkontakte an den Anbieter)

Fehlende Löschfrist / Routine

Information an den Kunden nicht erfolgt

Weitergabe der Daten an einen Dritten; es ist von einer Auftragsverarbeitung auszugehen; entsprechender Vertrag fehlt

Abgeleitete notwendige Maßnahmen

Umstellung auf telefonische Terminvereinbarung;
Löschen der App auf dem Firmenhandy;
Treffen von Vereinbarung mit den Mitarbeitern, dass die App nicht mehr genutzt werden darf

Die Prüfung dieses Beispiels hat gut gezeigt, dass teilweise ein komplette Neuorganisation notwendig sein kann. Es soll im Folgenden nochmals auf den konkreten Fall eingegangen werden und erläutert werden, warum die Nutzung eingestellt werden sollte.

Bei Installation und Nutzung der App Whatsapp werden alle Telefonkontakte an den Betreiber der App weitergegeben. Damit dies rechtskonform geschieht, ist ein Erlaubnistatbestand notwendig, der erfüllt wird und zwar bei allen Telefonkontakten auf dem Mobiltelefonen. Vielleicht kann man die Erlaubnis durch die Vertragserfüllung bei dem Betroffenen herleiten, zumindest was die Kunden anbelangt. Vermutlich werden auf dem Telefon aber auch andere Kontakte von Mitarbeitern und Co. gespeichert, auf die dies nicht zutrifft. Die Erfüllung von rechtlichen Pflichten, lebenswichtige Interessen, Wahrnehmung einer Aufgabe im öffentlichen Interesse und ähnliches sind hier ebenso nicht zu sehen. Ein Mittel, dass noch zur Verfügung stehen würde, wäre die Einwilligung der Betroffenen. Diese müsste allerdings von allen Kontakten vorliegen und stellt sich als impraktikabel dar. Denn was wäre, wenn ein einziger Kunde nicht einwilligt (Wir erinnern uns, dass ein Kopplungsverbot besteht und eine Leistung darf nicht von einer Einwilligung abhängig gemacht werden)? Nunmehr würde noch der Tatbestand eines berechtigten Interesses im Raume stehen. Dies könnte begründet werden mit der Einfachheit der Kommunikation, der hohen Verbreitung der App und dem Servicegedanken des Unternehmens. Nunmehr gibt uns die DS-GVO aber gleichzeitig den Grundsatz der Verhältnismäßigkeit an die Hand. Der uns vermittelt, dass Art und Form der Verarbeitung das mildeste aller gleich effektiven Mittel zur Erreichung des Zweckes sein muss. Dies ist bei der App nicht der Fall. Die Kontaktaufnahme per Telefon oder SMS sind in diesem Zusammenhang mildere Mittel.

Ungeachtet weiterer Gründe, die dafür sorgen, dass die Nutzung der App zumindest als bedenklich angesehen werden muss, bleibt dem Unternehmen derzeit nichts anderes übrig, als diesen Prozess komplett umzustellen, auf zum Beispiel eine telefonische Terminvereinbarung.

Da die Verarbeitung bisher unrechtmäßig erfolgte, sind natürlich auch die unrechtmäßig verarbeiteten Daten und somit die App, in der sie gespeichert sind, zu löschen. Und um den Pflichten genügend gerecht zu werden, sollte eine Vereinbarung mit den Mitarbeitern getroffen oder zumindest eine Richtlinie ausformuliert werden, die es künftig Mitarbeitern verbietet die App auf dem Firmenhandy oder im betrieblichen Zusammenhang zu nutzen.

3.7 Dokumentationspflicht & Anlegen des Verzeichnisses der Verarbeitungstätigkeiten

Sind alle betreffenden Prozesse im Unternehmen aufgenommen, analysiert und ggf. angepasst, geht es an die Anlage des Verzeichnisses der Verarbeitungstätigkeiten.

Dieses beginnt mit einem Deckblatt, auf dem die Angaben zum Unternehmen (Firmierung, Anschrift, Inhaber / Geschäftsführer) und dem Datenschutzbeauftragten gemacht werden und der Gegenstand des Unternehmen in kurzer Form beschrieben wird.

Im Anschluss müssen die einzelnen Verarbeitungstätigkeiten beschrieben werden. Enthalten sein sollten eine allgemeine Beschreibung der Tätigkeit, der Zweck der Verarbeitung, die Rechtsgrundlage, Angaben zur ggf. vorhandenen Einwilligung, die Speicherdauer der Daten, die Datenherkunft, Angaben, ob es sich um eine automatische Entscheidungsfindung handelt, die Art der Verarbeitung, Angaben ob die Betroffenen über die Verarbeitung informiert wurden, Kategorien der Betroffenen, die verarbeiteten Datenkategorien und die Empfänger der Daten. Zusätzlich sind Datenübermittlungen in Drittländer aufzunehmen, spezielle technische und organisatorische Maßnahmen zum Schutz der Daten darzulegen, der für den Prozess Verantwortliche zu benennen und die Erforderlichkeit einer Datenschutz-Folgenabschätzung zu prüfen.

Diese Prozessbeschreibung sollte durch geschultes und entsprechend qualifiziertes Personal erfolgen. Da der jeweilige Verantwortliche sicher ausreichend Kenntnis über den Prozess an sich hat, aber der Datenschutzbeauftragte die notwendige Fachkenntnis zur DS-GVO besitzt, sollten beide gemeinsam die einzelnen Prozesse beschreiben.

Eine musterhafte Beschreibung des Prozesses „Betreiben der Website“ folgt hier:

Betreiben der Website

Kurzbeschreibung:	Es wird die Website www.muster.de potentiellen Kunden und Interessenten zur Verfügung gestellt, auf der wir unser Unternehmen und

	Leistungsangebot darstellen. Kunden haben die Möglichkeit über das Kontaktformular Kontakt mit uns aufzunehmen. Die Eingaben gelangen dann per E-Mail zu uns.
Zweck der Verarbeitung:	Marketing & Werbezwecke Zurverfügungstellung Onlineangebot Kontaktaufnahme von Kunden
Rechtsgrundlage:	Beantwortung von Anfragen (bei Nutzung Kontaktformular) Berechtigte Interessen (Marketing)
Einwilligung:	Liegt nicht vor / nicht notwendig
Speicherdauer:	Löschung von Dateneingaben mit Ende der Erforderlichkeit (Prüfung erfolgt jährlich)
Datenherkunft:	Freiwillige Selbstangaben im Online-Formular Serverlogfiles
Art der Verarbeitung:	elektronische Verarbeitung
Autom. Entscheidungsfindung:	nein
Information Betroffener:	Datenschutzerklärung auf Website
Kategorien Betroffener:	Websitebesucher
Datenkategorien:	Name, Kontaktdaten, Texteingaben, Meta- & Kommunikationsdaten
Empfänger intern:	Sekretariat
Empfänger extern:	keine
Übermittlung in Drittland:	keine
TOMs:	allgemeine TOMs + SSL-verschlüsselte Übertragung + Abschluss AV-Vertrag mit Webhoster
Fachverantwortlicher:	Max Mustermann

DS-FA notwendig: nein

An dieser Stelle bleibt zu erwähnen, dass gleiche und sehr ähnliche Verarbeitungen in einer Beschreibung zusammengefasst werden können.

Auch die Inhalte der folgenden drei Kapitel, beziehungsweise die Ergebnisse der beschriebenen Vorgänge, gehören zum Verzeichnis der Verarbeitungstätigkeiten und werden jenem beigefügt.

3.8 Datenschutz-Folgenabschätzung

Birgt eine Verarbeitung voraussichtlich hohe Risiken für die Reche und Freiheiten von natürlichen Personen, muss für jene Verarbeitungstätigkeit eine Datenschutzfolgenabschätzung durchgeführt werden (Näheres hierzu in Kapitel 2.10).

Grundsätzlich ist die DS-FA immer vor Beginn der Verarbeitungstätigkeit durchzuführen und der DSB zu beteiligen. Auch bei der DS-FA können mehrere ähnliche Verarbeitungsvorgänge zusammengefasst werden.

Als praktisches Beispiel nehmen wir uns an dieser Stelle die systematische Videoüberwachung der Verkaufsräume in einem Unternehmen und machen uns den Ablauf und den Inhalt der DS-FA an diesem deutlich.

Zunächst geht es an die systematische Beschreibung der geplanten Verarbeitungstätigkeit, also der Videoüberwachung. Es wird beschrieben, wie genau diese umgesetzt wird, wir geben den Zweck an und die vom Unternehmen verfolgten Interessen. Bei der Videoüberwachung ist also anzugeben, wie viele Kameras wo aufgehängt werden, wo und wie die Bilddaten zusammenlaufen, ob und wie sie gespeichert werden, wer Zugriff auf die Daten hat usw.. Der Zweck und das verfolgte Interesse des Verantwortlichen könnte beispielsweise das Aufdecken von Diebstählen, das Vereiteln von Diebstählen durch Abschreckung und der Schutz der Angestellten und des Unternehmens vor Überfällen sein.

Im Anschluss geht es an die Verhältnismäßigkeitsprüfung. Es muss bewertet werden ob und inwieweit eine Notwendigkeit und Verhältnismäßigkeit in Bezug auf den verfolgten Zweck bei der geplanten Verarbeitung gegeben ist. Die Notwendigkeit der Videoüberwachung könnte sich zum Beispiel aus einer hohen Zahl von Diebstählen oder Überfällen ergeben. Dem gegenüber steht dann die Frage der Verhältnismäßigkeit und die Frage, ob die Videoüberwachung in der geplanten Form das mildeste aller gleich effektiven zur Verfügung stehenden Mittel ist. Beispielsweise könnten auch Ladendetektive eine Alternative sein. Auch der Umfang der Videoüberwachung muss auf den Prüfstand. Geht es darum die Waren vor Diebstahl zu schützen, so sollte die Überwachung auch nur in dem Bereich des Unternehmens erfolgen, in dem sich auch entsprechende Waren befinden. Diese Prüfung muss zum Ergebnis kommen, dass die geplante Tätigkeit sowohl notwendig, als auch verhältnismäßig ist. Anderenfalls muss die geplante Tätigkeit umstrukturiert oder ganz verworfen werden.

Nunmehr geht es an die Prüfung möglicher Risiken für die Betroffenen und die Eintrittswahrscheinlichkeit. Betroffene können bei der Videoüberwachung Kunden, Mitarbeiter, aber auch Lieferanten sein. Es muss dargelegt werden welche Risiken sich für die Einzelnen ergeben, welche Folgen ein Missbrauch hätte und wie hoch die jeweilige Eintrittswahrscheinlichkeit ist. Beispielweise könnte durch unzureichende Sicherungsmaßnahmen ein Fernzugriff für Jedermann auf die Kameras möglich sein und so Bewegungsprofile von Kunden erstellt werden, bzw. deren Standort unberechtigterweise ermittelt werden. Oder aber die Verkäufer erhalten Zugriff auf die Daten und schikanieren ihre Kollegen mit Bildern von unvorteilhaften Situationen, die von einer Kamera aufgezeichnet wurden.

Es muss im Anschluss geprüft und dargelegt werden, wie diesen Risiken durch geeignete technische und organisatorische Maßnahmen begegnet wird. Dies kann zum Beispiel durch die verschlüsselte Übertragung der Kameras, Passwortschutz, Positionierung des digitalen Videorekorders in einem abgeschlossenen Raum, auf den nur die Geschäftsleitung Zugriff hat und ähnlichem erfolgen. Auch Löschfristen sind darzulegen.

Zusätzlich sollte eine Abstimmung und Information der Betroffenen über die geplanten Maßnahmen erfolgen. In unserem Beispiel zum Beispiel mit den Betroffenen Mitarbeitern und dem Betriebsrat. Vorhandene Standpunkte Betroffener sind einzuholen und zu dokumentieren.

Es folgt die abschließende Risikobewertung. Die Risiken auf der einen Seite und die Schutzmaßnahmen auf der anderen Seite. Diese werden gegenübergestellt und bewertet, ob den Risiken ausreichend begegnet wird und somit die Wahrscheinlichkeit und den möglichen Folgen einer Datenpanne ausreichend begegnet wird.

Stellt sich dabei heraus, dass die geplante Verarbeitung immer noch hohe Risiken zur Folge hätte, muss das Unternehmen das nach Artikel 36 DS-GVO vorgeschriebene Konsultationsverfahren mit der Aufsichtsbehörde einleiten, oder aber die geplante Verarbeitungstätigkeit einstellen.

Der gesamte Prozess der Datenschutzfolgenabschätzung muss dokumentiert werden und sollte dem Verzeichnis der Verarbeitungstätigkeiten angehängt werden.

3.9 Auftragsverarbeitung

In allen Fällen, in denen eine Auftragsverarbeitung vorliegt, ist ein Auftragsverarbeitungsvertrag zu schließen und ggf. geeignete Garantien zu dokumentieren (vgl. Kapitel 2.5).

Im Verzeichnis der Verarbeitungstätigkeiten muss ein Verzeichnis der Auftragsverarbeitungsverhältnisse erstellt werden. In jenem sind die einzelnen Auftragsverarbeiter, das Datum des Auftragsverarbeitungsvertrages und der Zweck der Auftragsverarbeitung zu benennen. Ferner, falls die Verarbeitung in einem Drittland erfolgt, ist der Verweis auf geeignete Garantien bzw. Angemessenheitsbeschlüsse zu geben. Empfehlenswert ist ebenso eine Kopie des jeweiligen Vertrages beizufügen.

3.10 Technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten

Der letzte Teil des Verarbeitungsverzeichnisses ist die Darlegung geeigneter technischer und organisatorischer Maßnahmen zum Schutz der personenbezogenen Daten, die das Unternehmen getroffen hat. Der Gesetzgeber gibt dazu keine konkreten Vorgaben, was wie zu tun ist. Er schreibt aber die Integrität und den Schutz der Daten vor.

Das Unternehmen muss eigenständig an Standards im Unternehmen arbeiten, diese umsetzen und dokumentieren. Je größer das Unternehmen, je umfangreicher die Verarbeitung von personenbezogenen Daten und umso sensibler die Daten, umso höhere Anforderungen sind an Sicherheitskonzept zu stellen. Hier sind IT-Dienstleister gewiss gute Hilfen.

Man unterteilt die Maßnahmen gängiger weise wie folgt:

Vertraulichkeit

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Pseudonymisierung
- Trennungskontrolle

Integrität

- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle

Verfügbarkeit & Belastbarkeit

- Storagesysteme
- Patchmanagement
- räumlich getrennt redundante Speicherung

Verfahren zur regelmäßigen Überprüfung

Bei einem sehr kleinen Unternehmen können folgende Mindestmaßnahmen empfohlen werden:

- Bürogebäude mit Sicherheitsschlössern
- Einzelne Räume immer abgeschlossen, wenn niemand darin
- Abschließbare Aktenschränke
- Mindestlängen für Passwörter
- Regelmäßiger Passwortwechsel
- Verschlüsselte Arbeitsrechner
- Aktueller Virenschutz & Firewall
- Anwendungsbezogene Authentifikation mit Benutzername & Passwort
- Protokollierung von Anwenderzugriffen in der Software
- Verschlüsselung mobiler Datenträger
- Geschützte Aufbewahrung von Datenträgern
- Protokollierung der Akten- & Datenvernichtung
- Nutzen von SSL-Verschlüsselungen & VPN-Technologie
- Verbot von Nutzung privater Endgeräte und Datenträger
- Nachvollziehbarkeit von Änderungen, Eingaben und Löschungen
- Sorgfältige Auswahl & Überprüfung von Auftragsverarbeitern
- Updates pflegen
- Regelmäßige Schulung der Mitarbeiter zum Datenschutz
- Regelmäßige Prüfung & Auditierung der Datenschutzstandards

3.11 Mitarbeitersensibilisierung & -verpflichtung

Wichtiger Baustein des Datenschutzes in Unternehmen ist die Mitarbeitersensibilisierung und -verpflichtung. Wenn noch nicht geschehen, sollten Mitarbeiter zur Vertraulichkeit und zum gesetzeskonformen Umgang mit personenbezogenen Daten verpflichtet werden. Dies erfolgt regelmäßig durch eine individuelle, schriftliche Vereinbarung.

Der Gesetzgeber sieht aber auch eine regelmäßige Schulung und Sensibilisierung der Mitarbeiter vor. Für diese hat der ggf. vorhandene Datenschutzbeauftragte zu sorgen. Dies kann zum Beispiel durch Inhouse-Datenschutzschulungen erfolgen, aber auch durch Web-Based-Trainings. Diese Maßnahme sollte einmal im Jahr wiederholt werden.

Wichtig ist ferner die Dokumentation dieser Maßnahmen, sodass im Zweifelsfall nachgewiesen werden kann, dass sich das Unternehmen um die Sensibilisierung und Schulung seiner Mitarbeiter gekümmert hat.

3.12 Kontinuierliche Kontrolle & Anpassung

Wir befinden uns nunmehr in der Phase des Refreezings. Die eigentlichen Veränderungen im Unternehmen sowie die Schaffung der Complience sollte erledigt sein. Nunmehr geht es daran die neuen Prozesse und Strukturen im Unternehmensalltag zu festigen und die Einhaltung der neuen Richtlinien zu prüfen. Es kommt auch häufiger vor, dass etwas nicht so läuft, wie es gewünscht war und weitere Anpassungen notwendig sind.

Es sollte ein betriebliches Meldesystem geschaffen werden, mit dem etwaige Probleme oder Anregungen von Mitarbeitern ermöglicht werden und jene geprüft werden können. Auch sollte immer ein zentraler Ansprechpartner im Unternehmen vorhanden sein, der bei Fragen zur Verfügung steht (z.B. der Datenschutzbeauftragte).

Sobald eine Änderung an den bestehenden Prozessen erfolgt, ist dies im Verarbeitungsverzeichnis entsprechend anzupassen und auf die rechtliche Zulässigkeit zu prüfen.

Routinemäßig, einmal im Jahr, sollte ein Datenschutzaudit durchgeführt werden und die Dokumentation, auch ohne Vorhandensein von Änderungen an den Prozessen, auf den Prüfstand gestellt und dies dokumentiert werden.

Eine Besonderheit gibt es bei Datenschutz-Folgenabschätzungen: Der Gesetzgeber definiert, dass jene häufiger geprüft und aktualisiert werden müssen, als das Verzeichnis der Verarbeitungstätigkeiten, verzichtet dabei aber auch auf eine konkrete Benennung des Zeitraums. Daher gilt es mit viel Augenmaß zu entscheiden. Tendenziell sollten Verarbeitungen mit einem höheren Risiko auch öfter auf den Prüfstand (z.B. alle 3 Monate), als weniger Risikobehaftete.

Dieses Vorgehen, der immer wiederkehrenden Kontrolle, ist als sehr sinnvoll zu betrachten. Denn ständig neue Entwicklungen in der Informationstechnologie

kommen auf uns zu und bringen u.a. auch neue Sicherheitsstandards mit sich, die in die Strukturen der Unternehmen implementiert werden sollten.

Kapitel 4: Wo Unternehmen an ihre Grenzen stoßen

Die Schaffung der Datenschutz-Konformität im Unternehmen ist ein sehr aufwändiger Prozess, der viel Fach- und Methodenkompetenz und natürlich Ressourcen erfordert. Wodurch die meisten Unternehmen in der Praxis an ihre Grenzen stoßen, soll in diesem Kapitel erläutert werden.

4.1 Überlastung durch Mehrarbeit

In Zeiten des Fachkräftemangels, einem hohem Grad der Bürokratisierung und zahlreichen Gesetzen und Normen, die ein Unternehmen einhalten muss, liegt es mehr als auf der Hand, dass die Anforderungen des neuen Datenschutzrechts zu einer Überlastung im Unternehmen führen können. Im Beratungsalltag beklagen sich einige Unternehmen, dass der Aufwand für die Datenschutz-Complience sogar höher ist, als für die Aufrechterhaltung eines Qualitätsmanagement-Systems. Nunmehr kann dies zwar nicht auf jedes Unternehmen übertragen werden, aber in Unternehmen, in denen viele oder gar besondere Datenkategorien verarbeitet werden, trifft dies unfraglich zu. Die Ursache hierfür sind die umfangreichen Dokumentations- und Rechenschaftspflichten des Datenschutzrechts und die vorgeschriebene, regelmäßige und dokumentierte erneute Prüfung betroffener Verarbeitungsvorgänge. Zudem müssen zuständige Mitarbeiter zuvor erst mit dem notwendigen Fachwissen ausgestattet werden, was zusätzlichen Aufwand mit sich bringt.

Häufig können Unternehmen diesen Aufwand gar nicht alleine bewerkstelligen und benötigen daher Manpower von außen.

4.2 Erkennen von Schwachstellen & Betriebsblindheit

Mitarbeiter im Unternehmen, die seit langer Zeit geübt sind, immer wieder gleiche oder ähnliche Vorgänge durchzuführen, entwickeln für jene eine

gewisse Routine, Betriebsblindheit und Selbstverständlichkeit. Ein sehr einfaches und anschauliches Beispiel ist die selbstverständliche Niederschrift eines Telefonats in einem CRM-System. Dabei kann es vorkommen, dass der jeweilige Gesprächspartner neu angelegt werden muss. Der betreffende Mitarbeiter ist es gewohnt und darin geübt dies zu tun. In der Beratungspraxis, wird dieser Vorgang aber nicht als Verarbeitung von personenbezogenen Daten erkannt, sondern als eine Selbstverständlichkeit. Häufig fehlen solche Verarbeitungstätigkeiten dann in der Bestandsaufnahme der Prozesse und fallen daher im Verzeichnis der Verarbeitungstätigkeiten unter den Tisch, werden nicht geprüft und auch nicht dokumentiert. Auch die Information des Betroffenen zur Verarbeitung seiner Daten findet meist nicht statt oder erfolgt unzulänglich.

Ein weiteres Beispiel schneidet sich mit der Datenminimierung: Für Vertriebsmitarbeiter ist es häufig selbstverständlich, das Geburtsdatum der Geschäftspartner zu erfassen, die gesammelten Daten zu verwalten und so den Kunden zum Geburtstag eine Karte oder ähnliches zukommen zulassen. Die nett gemeinte Geste, ist jedoch ohne Einwilligung in der Regel nicht zulässig. Die notwendige Sensibilität der betreffenden Mitarbeiter, dies zu erkennen, ist jedoch meist nicht vorhanden. In der Beratungspraxis sitzt man oft tagelang zusammen und arbeitet gemeinsam an notwendigen Dokumenten. Kurz vor Erreichen der Ziellinie jedoch, und meist nur beiläufig, fallen dann solche Verarbeitungen auf. Beispielsweise, indem auffällt, dass im Terminkalender des Mitarbeiters für den nächsten Tag der Geburtstag des Kunden „Max Mustermann“ zu finden ist. Auf die Nachfrage beim Mitarbeiter, warum er dies tut und warum es bisher nicht erwähnt wurde, folgt meist ein Schulterzucken oder ein „Das machen wir immer so!“.

Diese Beispiele zeigen sehr deutlich, dass die betriebliche Übung bei dem Erkennen von Schwachstellen nicht förderlich und so ein unvoreingenommener Blick von außen sinnvoll ist.

4.3 Abwägung berechtigter Interessen

Die DS-GVO sieht regelmäßig das Abwägen der berechtigten Interessen des Unternehmens mit den Interessen der Betroffenen am Schutz ihrer Rechte und Freiheiten vor. Dieses Abwägen muss neutral erfolgen. Jedoch trifft man in der Praxis häufig darauf, dass dies seitens des Unternehmens und deren Mitarbeitern nicht möglich ist, sondern vielmehr die Interessen des Unternehmens unrechtmäßig zu schwer gewogen werden. Hierin ist in der Regel kein böswilliges Handeln zu sehen, sondern vielmehr eine fehlende Unparteilichkeit. Selbstverständlich ist es für das Unternehmen von sehr wichtiger Bedeutung, Daten zu verarbeiten und mit ihnen beispielsweise den Absatz zu fördern. Es ist daher verständlich, dass für die Mitarbeiter das berechtigte Interesse der Verkaufsförderung sehr schwer wiegt, denn es geht um die Existenz und den Erfolg des Unternehmens. Jedoch fallen derartige Abwägungen durch einen objektiven Dritten häufig anders aus, jeweilige Interessen wiegen weniger schwer und einige Entscheidungen hätten anders getroffen werden müssen. Daher ist es sehr wichtig, aufgrund der fehlenden Objektivität, im Zweifel externe Unterstützung zur Umsetzung wirklich objektiver Abwägungen hinzuzuziehen.

4.4 Detailgenauigkeit

Der Aspekt der Detailgenauigkeit geht sehr eng mit der Überlastung durch Mehrarbeit einher. Wenn verantwortliche Mitarbeiter überlastet sind, sind sie in der Regel gezwungen Arbeiten schneller zu erledigen. In dieser Eile ist ein erhebliches Risiko zu sehen, da notwendige Betrachtungen und Einschätzungen sehr wahrscheinlich nicht detailliert genug und zu oberflächlich durchgeführt werden. Wichtig ist es jedoch, sich Zeit zu nehmen und im Zweifel Zweitmeinungen und weitere Informationen einzuholen. Daher sind zur Wahrung einer umfassenden und lückenlosen Prüfung häufig mehr zeitliche Ressourcen als eigentlich vorhanden notwendig.

4.5 Interpretation von Begrifflichkeiten

Die DS-GVO nutzt Formulierungen wie „umfangreich“, „Kerntätigkeit“, „regelmäßig“, „systematisch“ und „in der Regel“, ohne jedoch diese konkret zu beschreiben oder quantitativ messbare Indikatoren zur Bewertung an die Hand zu geben, wie zum Beispiel, dass eine umfangreiche Verarbeitung vorliegt, wenn 100 natürliche Personen betroffen sind. Vielmehr obliegt es häufig den Unternehmen, jene Deutung der Begrifflichkeiten vorzunehmen und diese dann in die Prüfung der Verarbeitungstätigkeiten einzubringen.

Dies erfolgt auf Seiten der Unternehmen zudem meist zum Vorteil des jeweiligen Unternehmens, was mit einem erheblichen Risiko einhergeht, wenn die Datenschutzbehörde beispielsweise einer anderen Meinung ist.

Daher sollten sich die Verantwortlichen regelmäßig auf dem Laufenden bezüglich Informationen der Datenschutzbehörden halten und optimalster weise über umfangreiche Erfahrungen aus der praktischen Anwendung solcher Formulierungen verfügen. Dies ist für Mitarbeiter, die den Datenschutz nebenbei erledigen, meist jedoch gar nicht möglich.

Ansätze für die Deutung der Begrifflichkeiten finden sich zum Beispiel in den Erwägungsgründen der DS-GVO und den Leitlinien der Artikel-29-Datenschutzgruppe. Diese Datenschutzgruppe besteht aus Vertretern der jeweiligen nationalen Datenschutzbehörden und hat vorrangig beratende Funktion, kann aber auch Empfehlungen und Stellungnahmen abgeben.

Dies verdeutlicht, dass es meist nicht ausreicht, sich nur mit den reinen Gesetzen zu beschäftigen und viel Augenmaß nach Treu und Glauben seitens der Verantwortlichen erforderlich ist.

4.6 Steuerung von Prozessen

Gerade in kleinen und jungen Unternehmen, wurden noch keine effektiven Instrumente zur Steuerung und Koordinierung von Prozessen im Unternehmen geschaffen. Dies wird besonders riskant, wenn dieses Fehlen auch im Rahmen der Schaffung der Datenschutz-Complience der Fall ist.

Das gesamte Bereich Datenschutz muss professionell überwacht und gesteuert werden. Entsprechendes Handwerkszeug fehlt einem nicht unbeachtlichem Teil der Unternehmen und muss ggf. durch externe Unterstützung ins Unternehmen geholt werden. Mechanismen müssen, sowohl für Abläufe, regelmäßige Audits und natürlich eine Art Alarmsystem, gefunden und realisiert werden.

4.7 Umgang mit Widerständen

Widerstände im Unternehmen rühren aus mehreren Richtungen. Gründe hierfür können aus der Mehrarbeit und Überlastung, der Ablehnung der Sinnhaftigkeit notwendiger Schritte, aber auch aus dem allgemeinen Abwehrverhalten gegen Veränderungen stammen.

Es gilt Konflikte und Widerstände so früh wie möglich zu erkennen, Ursachen zu suchen und Abhilfemaßnahmen einzuleiten, um Sabotagen, Verweigerungen und die Stimmungsmache zu vermeiden. Grundsätzlich kann man sagen, umso früher eingegriffen wird, umso eher lässt sich mit Widerständen umgehen. Zur Prävention sollten alle Betroffenen umfassend informiert und beteiligt werden.

Mögliche Handlungsalternativen im Umgang mit diesen Widerständen können sein, jeweilige Beteiligte auf fachlicher Ebene zu überzeugen und entsprechende Vorbehalte ernst zu nehmen, den Widerständler zum Beteiligten zu machen, eine aktive Beziehung aufzubauen und Ängste zu nehmen oder die jeweilige Person, als letzte Maßnahme, abzulösen.

Dies erfordert viel Fingerspitzengefühl und Erfahrung im Bereich des Konfliktmanagements, das in diesem Ausmaß, aufgrund der Komplexität des neuen Datenschutzrechts, so nicht alltäglich sein dürfte und auch erfahrene Führungskräfte schnell überfordern könnte. Professioneller Rat ist hier gefragt.

Kapitel 5: Hilfen bei der Umsetzung

Viele Unternehmen sind vermutlich nicht in der Lage alle notwendigen Maßnahmen allein und in Eigenregie umzusetzen. Aber es gibt auch kompetente Hilfen. Auf die externen Datenschutzbeauftragten und IT-Dienstleister wurde schon eingegangen. Ferner bleibt zu erwähnen, dass auch Rechtsanwälte gute Partner für die Formulierung von Erklärungen, Vereinbarungen etc. sind. Auf Unternehmensberater und die Datenschutzbehörden soll an dieser Stelle aber nochmals gesondert eingegangen werden.

5.1 Unternehmensberater

Neben der fachlichen Kompetenz des Unternehmensberaters, verfügt er in der Regel über umfangreiche Erfahrungen im Bereich der Prozessoptimierung und des Changemanagements. Dies ist der gravierende Vorteil bei einer Beauftragung, denn er weiß in der Regel, wie Veränderungen in Unternehmen unter verschiedensten Voraussetzungen angegangen werden sollten und verfügt, als auf den Datenschutz spezialisierter Experte, über umfangreiches Fachwissen.

Zusätzlich bietet sich bei Unternehmensberatern häufig die Möglichkeit einer Förderung an. Das Bundesamt für Wirtschaft und Ausfuhrkontrolle fördert Unternehmensberatungen zum Thema Complience mit bis zu 80% der förderfähigen Kosten. Dies sind bei Bestandsunternehmen bis zu 3.000 Euro und bei Jungunternehmen bis maximal 2 Jahren bis zu 4.000 Euro.

5.2 Die Datenschutzbehörden

Auch die Datenschutzbehörden sind gute Ansprechpartner, wenn es um Unklarheiten bei der Umsetzung der neuen Rechtslage geht. Zwar werden sie keine umfangreiche Beratung leisten, aber bei einfachen kurzen Fragen, in denen Unsicherheit besteht, gerne zur Seite stehen.

Die Behörden dürfen gemäß Artikel 57 Absatz 3 DS-GVO von betrieblichen Datenschutzbeauftragen und Betroffenen übrigens keine Gebühren für ihre Tätigkeit verlangen.

Bei komplexeren Themen oder Problemen, werden jedoch auch sie auf externe Berater verweisen.

Kapitel 6: Schlussbetrachtungen

Die Intension des Gesetzgebers, die Rechte und Freiheiten natürlicher Personen zu schützen sowie die informationelle Selbstbestimmtheit zu stärken, ist mit der neuen Gesetzgebung gut gelungen.

Auf der Seite der Unternehmen jedoch, führen die neuen Regelungen zu einem erheblichen Mehraufwand im Bereich der Dokumentation und Nachweispflichten, was sich gerade für Kleinstunternehmen als sehr hohe Hürde darstellen dürfte.

Zudem verwendet die DS-GVO und auch das BDSG-neu zum Teil sehr schwammige Formulierungen, wie zum Beispiel „umfangreich“, ohne dabei fest greifbare Zahlen und Indikatoren für die Bewertung einer Verarbeitung zu geben. Dies führt derzeit zu einer nicht unerheblichen Unsicherheit. Auch die Abwägung von berechtigter Interessen kann von Beurteilendem zu Beurteilendem anders ausfallen, um nur ein weiteres Beispiel zu nennen.

Diese Unsicherheiten werden nunmehr Gerichte konkretisieren müssen und es obliegt den Unternehmen selbst, dabei auf dem Laufenden zu bleiben und das eigene Wissen aktuell zu halten. Die Kosten für diese gerichtlichen Konkretisierungen wird leider die Wirtschaft tragen müssen.

Disclaimer

Diese Ausarbeitung ist urheberrechtlich geschützt, jegliche Nutzung oder Veröffentlichung, auch auszugsweise, bedarf einer schriftlichen Zustimmung des Verfassers.

Diese Ausarbeitung wurde nach bestem Wissen und Gewissen verfasst, kann eine Rechtsberatung aber nicht ersetzen und erhebt auch keinen Anspruch darauf. Die Verwendung dieser Ausarbeitung in Ihrem Unternehmen erfolgt auf eigene Gefahr. Im Zweifel sollte eine zusätzliche Beratung in Anspruch genommen werden.

Derzeit gibt es noch fast keine Rechtsprechung zur DSGVO, BDSG-neu und anderen Gesetzen, die den Datenschutz betreffen. Daher bleibt es noch abzuwarten, wie Gerichte die Gesetzestexte interpretieren und welche Maßnahmen als angemessen gesehen werden. Sie sollten kommende Urteile und weitere Gesetzesänderungen im Auge haben und auf diese durch geeignete Maßnahmen im eigenen Unternehmen reagieren.