Thum GmbH Steuerberatungsgesellschaft
Kirchberg 57
56626 Andernach
Telefon: 02632/493504
Fax: 02632/492238
Email: andernach@thum-gmbh.de

DW Steuerberatungsgesellschaft Thum GmbH
Weißeritzstr. 15d
01744 Dippoldiswalde
Telefon: 03504/64310
Fax: 03504/643123
Email: dippoldiswalde@thum-gmbh.de

THUM Steuerberatungsgesellschaft mbH
Bahnhofstr. 29a
56745 Weibern
Telefon: 02655/1500
Fax: 02655/4242
Email: weibern@thum-gmbh.de

Steuerberatungsgesellschaft Sächsische Schweiz Thum-Schröder mbH
Königstraße 10
01816 Bad Gottleuba
Telefon: 035023/526-0
Fax: 035023/526-11
Email: gottleuba@thum-gmbh.de

Petra Uhl Steuerberaterin
Amselweg 26
69190 Walldorf
Telefon: 06227/3098764
Email: p.uhl@gmx.de

Mandanten-Information: Praxishinweise zur DSGVO - Erste Hilfe in sechs Schritten

Sehr geehrte Mandantin,
sehr geehrter Mandant,

nun bleibt nicht mehr viel Zeit, sich mit den zahlreichen Neuerungen rund um den Datenschutz zu beschäftigen: Zum 25.05.2018 tritt die neue EU-Datenschutz-Grundverordnung (DSGVO) in Kraft. Und beschäftigen sollten Sie sich damit auf jeden Fall, denn bei Nichtbeachtung drohen hohe Bußgelder für Ihr Unternehmen. Es ist zu erwarten, dass sowohl die Prüfungsdichte als auch die Sanktionshäufigkeit von Seiten der Aufsichtsbehörden stark zunehmen.

Sehr wichtig in diesem Zusammenhang: Es gibt keine Übergangsfrist. Ab dem 25.05.2018 müssen alle Dokumente und Prozesse der Neuregelung angepasst sein.

Inhaltsverzeichnis

Ebenfalls zum 25.05.2018 tritt das geänderte Bundesdatenschutzgesetz (BDSG) in Kraft, das im Vergleich zur DSGVO einige Unterschiede aufweist. So wird etwa der Datenschutzbeauftragte (DSB; vgl. Punkt 2.1) bestellt und nicht benannt (wie in der DSGVO vorgesehen), und es besteht nicht die Möglichkeit, einen Konzerndatenschutzbeauftragten zu benennen. Ab dem 25.05.2018 müssen also beide Regelwerke beachtet werden! Dabei hat die DSGVO das letzte Wort: Sofern sie nicht ausdrücklich Möglichkeiten für einzelstaatliche Regelungen vorsieht, verdrängt sie entsprechende Vorschriften der einzelnen EU-Mitgliedstaaten, also auch die des BDSG.

Auf den folgenden Seiten geben wir Ihnen einen kurzen Überblick über das ab dem 25.05.2018 verbindlich geltende Datenschutzrecht für Ihr Unternehmen. In Anbetracht der Kürze der verbleibenden Zeit noch wertvoller: Unter Punkt 2 zeigen wir Ihnen außerdem, welche praktischen Schritte am wichtigsten sind, um nicht gleich von den Aufsichtsbehörden sanktioniert zu werden.

1 Für wen gilt die DSGVO?

Die DSGVO gilt für alle natürlichen Personen, öffentlichen Institutionen sowie für alle Privatunternehmen mit Sitz in der EU, die im Rahmen ihrer betrieblichen Tätigkeit personenbezogene Daten verarbeiten.

Das klingt erst einmal abstrakt, jedoch betrifft Sie das neue Datenschutzrecht schneller, als Sie vielleicht glauben: Es gilt grundsätzlich auch für Vereine und Verbände, die personenbezogene Daten speichern. Handwerksbetriebe sind ebenso betroffen wie Arztpraxen oder Rechtsanwaltskanzleien. Auch Vermieter können betroffen sein. Möglicherweise ein kleiner Trost: Die neuen Datenschutzregelungen gelten gleichermaßen für alle Behörden, insbesondere Finanzbehörden.

Hinweis:

Wenn Ihr Unternehmen keinen Sitz in der EU hat, unterliegt es dennoch der DSGVO, sofern Sie Ihre Waren oder Dienstleistungen in der EU anbieten.

Allgemein unterliegt Ihr Unternehmen nur dann dem Datenschutzrecht, wenn die Verarbeitung, Nutzung oder Erhebung personenbezogener Daten dort

- in bzw. aus nicht automatisierten Dateien oder
- mit Hilfe von Datenverarbeitungsanlagen erfolgt.

Hinweis:

Ausgenommen sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für ausschließlich persönliche/familiäre Zwecke und Tätigkeiten.

Mit der DSGVO wird ein weitestgehend einheitliches Datenschutzrecht innerhalb der EU eingeführt. Dabei sollen insbesondere die Rechte und Kontrollmöglichkeiten derjenigen gestärkt werden, deren personenbezogene Daten verarbeitet werden („Betroffene“). Dadurch steigen die Anforderungen sowohl an „Verantwortliche“ als auch an „Auftragsverarbeiter“.

1.1 Wer ist Verantwortlicher und wer Auftragsverarbeiter?

Verantwortlicher im Sinne der DSGVO ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die (zulässigen) Zwecke und Mittel dieser Verarbeitung sind durch die DSGVO bzw. das BDSG vorgegeben.

Auftragsverarbeiter im Sinne der DSGVO ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.

1.2 Was sind personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener): Alter, Geschlecht, Anschrift, Religion, sexuelle Orientierung, Vermögen, Äußerungen, politische und weltanschauliche Überzeugungen usw.

1.3 Wann ist die Datenverarbeitung erlaubt?

Für die Verarbeitung personenbezogener Daten gilt der allgemeine Grundsatz: Es ist grundsätzlich verboten, was nicht ausdrücklich erlaubt ist. Das bedeutet, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten verboten ist, es sei denn,

- dies ist durch eine Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder
- der Betroffene hat seine Einwilligung dazu erklärt.

Soll eine Einwilligung des Betroffenen Grundlage für eine Erhebung, Verarbeitung oder Nutzung sein, so

- muss sie freiwillig erfolgen,
- bedarf sie grundsätzlich der Schriftform (es sei denn, wegen besonderer Umstände ist eine andere Form angemessen),
- muss der Betroffene vorher über die Tragweite seiner Einwilligung aufgeklärt werden und
- ist der Betroffene auch darüber zu informieren, was geschieht, wenn er nicht einwilligt.

Ausdrücklich auf diese Daten beziehen muss sich die Einwilligung bei der Verarbeitung besonderer Arten personenbezogener Daten. Darunter fallen Angaben über ethnische Herkunft, politische Meinungen, religiöse oder politische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

2 Ihre ersten Schritte zur Umsetzung der DSGVO

2.1 Schritt 1: Brauchen Sie einen Datenschutzbeauftragten?

Hier hat sich nichts verändert. Es gilt wie bislang auch schon, dass Unternehmen nur dann einen DSB benötigen, wenn mehr als neun Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind („Zehn-Personen-Regel“). Die entscheidende Neuerung ist jedoch, dass nun erhebliche Sanktionen drohen.

Hinweis:

Bei der Zählweise für die Zehn-Personen-Regel ist zu beachten, dass allein die Anzahl der Personen, die sich mit Datenverarbeitung befassen, gilt. Es kommt nicht darauf an, ob es Mitarbeiter, Studenten, freie Mitarbeiter, Voll- oder Teilzeitkräfte usw. sind.

Falls Sie noch keinen DSB bestellt haben sollten, ist das Ihr erster Schritt, denn die Aufsichtsbehörden können nichts leichter überprüfen. Der DSB ist in allen Datenschutzinformationen zu nennen. Darüber hinaus müssen Verantwortliche und Auftragsverarbeiter die Kontaktdaten des DSB veröffentlichen und den Aufsichtsbehörden mitteilen. Sollten Sie also einen DSB benötigen, so sollten Sie den Posten spätestens am 25.05.2018 besetzt haben.

Hinweis:

Auskunfteien, Adresshändler sowie Markt- und Meinungsforschungsinstitute müssen in jedem Fall einen DSB bestellen.

Stellung des DSB

Der DSB ist unmittelbar dem Geschäftsführer unterstellt und in der Ausübung seiner Aufgaben weisungsfrei. Zudem genießt er einen besonderen Kündigungsschutz: Während seiner Bestellung bzw. bis ein Jahr nach seiner Abberufung darf ihm nur aus wichtigem Grund (z.B. Arbeitsverweigerung) gekündigt werden. Dieser Kündigungsschutz gilt jedoch nicht für freiwillig bestellte DSB.

Die Unternehmensleitung ist nicht an das Votum des DSB gebunden. Die Letztverantwortung für die Datenverarbeitung verbleibt damit bei ihr.

Der DSB muss die erforderliche „Fachkunde und Zuverlässigkeit“ besitzen. Der Verantwortliche ist verpflichtet, dem DSB zum Erhalt seiner Fachkunde die Teilnahme an Schulungs- und Fortbildungsveranstaltungen zu ermöglichen und hierfür die Kosten zu übernehmen.

Hinweis:

Um Interessenkonflikte zu vermeiden, sollten IT- und Personalverantwortliche sowie Systemadministratoren nicht als DSB bestellt werden.

Wie bisher haben Sie die Möglichkeit, einen externen DSB zu bestellen. Es steht Ihnen frei zu entscheiden, ob ein unternehmenseigener Mitarbeiter oder ein externer Dienstleister zum DSB bestellt wird. Natürlich müssen die Verträge mit einem externen DSB an die neue Rechtslage angepasst werden.

Aufgaben des DSB

Die Aufgaben des DSB umfassen

- die Durchführung der Vorabkontrolle (die verantwortliche Stelle für die Datenverarbeitung muss ihm dafür Informationen zur Verfügung stellen),
- auf Anfrage die Beratung hinsichtlich der Datenschutzfolgenabschätzung und die Überwachung ihrer Durchführung,
- die datenschutzrechtliche Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten,
- die Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters zum Schutz personenbezogener Daten,
- die Zusammenarbeit mit der Aufsichtsbehörde,
- Tätigkeiten als Anlaufstelle für die Aufsichtsbehörde in Fragen der Datenverarbeitung und gegebenenfalls Beratung zu allen sonstigen Fragen.

Betroffene können den DSB bei allen Fragen bezüglich der Verarbeitung ihrer personenbezogenen Daten und der Wahrnehmung ihrer Rechte zu Rate ziehen. Dabei ist der DSB an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden.

2.2 Schritt 2: Bestandsaufnahme

An zweiter Stelle sollten Sie sich einen Überblick darüber verschaffen, ob bzw. wie der Datenschutz in Ihrem Unternehmen organisiert ist. Dazu sollten Sie sich unter anderem folgende Fragen stellen:

- Welche Daten verarbeiten wir?
- Wer sind die von der Datenverarbeitung Betroffenen?
- Wie und in welchen Prozessen werden die Daten verarbeitet?
- Wie wird der Datenschutz momentan umgesetzt?
- Werden Auftragsverarbeiter eingesetzt bzw. wohin werden die Daten übermittelt?

2.3 Schritt 3: Verzeichnisse erstellen

Als weiteren wichtigen Bestandteil schreibt die DSGVO vor, dass sowohl jeder Verantwortliche als auch jeder Auftragsverarbeiter ein Verzeichnis aller Verarbeitungstätigkeiten zu erstellen und zu führen hat - elektronisch oder schriftlich. Auf Anfrage ist es einer Aufsichtsbehörde bereitzustellen.

Als Verarbeitungstätigkeiten gelten zum Beispiel:

- Aktenführung,
- Buchhaltungssoftware,
- elektronische Zeiterfassung,
- Führung von Adressdatenbanken,
- Personalakten,
- Profile in sozialen Netzwerken (z.B. Twitter, Xing),
- Rückrufservice,
- Software zur Verarbeitung und Verwaltung von E-Mails,
- Urlaubslisten,
- Websites sowie
- Webtracking.

Verzeichnis des Verantwortlichen

Das von Verantwortlichen zu erstellende Verzeichnis muss folgende Angaben enthalten:

- Name und Kontaktdaten des Unternehmens,
- gegebenenfalls Name und Kontaktdaten des DSB,
- Zweck der Datenverarbeitung,
- die Art der Personen, deren Daten verarbeitet werden, wie Kunden, Beschäftigte oder Lieferanten,
- die Art der verarbeiteten Daten,
- die möglichen Empfänger der Daten,
- gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
- die Rechtsgrundlage der Verarbeitung,
- die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Verzeichnis des Auftragsverarbeiters

Das Verzeichnis eines Auftragsverarbeiters über alle Kategorien von Verarbeitungen, die er im Auftrag von Verantwortlichen durchführt, muss Folgendes enthalten:

- den Namen und die Kontaktdaten des Auftragsverarbeiters und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des DSB,
- gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation unter Angabe des Staates bzw. der Organisation und
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Hinweis:

Aufgrund des Umfangs solcher Verzeichnisse wird es für Unternehmen vermutlich schwierig sein, ein solches erst bei Anfrage der Aufsichtsbehörde zu erstellen. Es gilt also, vorbereitet zu sein!

Wenn Sie das Verzeichnis noch um weitere Angaben ergänzen wie zum Beispiel die Rechtsgrundlage, Anwendungen, Berechtigungen, Risikoanalyse oder die Umsetzung von Betroffenenrechten, so haben Sie alle benötigten Unterlagen zur Hand.

2.4 Schritt 4: Ihr Umgang mit Daten

Besonders wichtig ist die Gewährleistung der Datensicherheit. Die jeweiligen Maßnahmen dafür sind im Verarbeitungsverzeichnis zu definieren. Da es hierbei im Kern um IT-Fachfragen geht, kann es ratsam sein, entsprechende Fachleute hinzuzuziehen. Insbesondere folgende Fragen sollten Sie sich stellen:

- Wie funktioniert die Datensicherheit in Ihrem Unternehmen?
- Wie sind die Zugriffsrechte auf Daten organisiert?
- Wer hat Zugriff auf die Daten und von wo (Homeoffice etc.)?
- Welche Maßnahmen gegen Hackerangriffe oder Viren setzen Sie um?

Zur Beantwortung dieser Fragen sollten Sie folgende Punkte beim Umgang mit Daten beachten:

- Die Erhebung und Verarbeitung personenbezogener Daten muss auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein. Es gilt das Prinzip der Datensparsamkeit. Die Daten sind grundsätzlich beim Betroffenen - also insbesondere beim Kunden - zu erheben. Unter bestimmten Voraussetzungen dürfen sie auch ohne Mitwirkung des Betroffenen erhoben werden.
- Für automatisierte Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, sieht das BDSG eine „Vorabprüfung“ vor Beginn der Verarbeitung vor. Eine solche ist nicht notwendig, wenn eine gesetzliche Verpflichtung zur Durchführung der Datenverarbeitung besteht oder die Einwilligung des Betroffenen vorliegt.
- Als zentrales Prinzip des Datenschutzes wurde in der DSGVO auch die Gewährleistung von Datensicherheit verankert. Unter Berücksichtigung vor allem der Schwere und Eintrittswahrscheinlichkeit des Risikos für die persönlichen Rechte und Freiheiten der Betroffenen haben der Verantwortliche und der Auftragsverarbeiter hierfür geeignete technische und organisatorische Maßnahmen umzusetzen. Dabei muss das Sicherheitslevel im Verhältnis zum Risiko angemessen sein. Achtung: Bei Datenschutzpannen haben Sie eine Informationspflicht und müssen die Aufsichtsbehörde informieren.

Hinweis:

Mit einem „Datenschutzaudit“ können Sie sowohl als Anbieter von Datenverarbeitungssystemen und -programmen als auch als Verantwortlicher Ihre Datenschutzkonzepte und technischen Einrichtungen mit einem datenschutzrechtlichen Gütesiegel versehen lassen sowie damit werben. Die Prüfung sollte durch unabhängige und zugelassene Gutachter erfolgen.

Jedenfalls müssen Ihre Datenschutzmaßnahmen folgende Voraussetzungen erfüllen:

- Verschlüsselung - personenbezogene Daten sollten soweit möglich verschlüsselt werden (genauso wie E-Mails) -,

- Stabilität - die IT-Systeme müssen auf Dauer Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sicherstellen -,
- Wiederherstellbarkeit - die Verarbeitungsprozesse müssen gegen Ausfall bzw. Beschädigung geschützt werden - und
- regelmäßige Kontrollen der Datensicherheit.

Datenverarbeitung im Auftrag

Entschließt sich Ihr Unternehmen zum Outsourcing einzelner Tätigkeiten, müssen dabei verschiedene rechtliche, technische und organisatorische Voraussetzungen erfüllt werden.

Werden dem Auftragnehmer zu einem solchen Zweck personenbezogene Daten überlassen, findet datenschutzrechtlich gesehen keine Übermittlung statt, da der Auftragnehmer nicht Dritter ist. Der Auftragnehmer darf und muss im Rahmen der Weisungen des Auftraggebers tätig werden. Gegenüber Geschäftspartnern und Kunden bleibt Ihr Unternehmen als Auftraggeber der Datenverarbeitung voll dafür verantwortlich, dass mit den personenbezogenen Daten rechtmäßig umgegangen wird. Als Auftraggeber müssen Sie

- einen schriftlichen Auftrag erteilen und
- die erforderlichen Maßnahmen zur Datensicherheit vorgeben.

Überdies müssen Sie sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen und das Ergebnis dieser Überprüfung dokumentieren.

Hinweis:

Es ist möglich, diese Aufgaben an Dritte (z.B. unabhängige Sachverständige) zu delegieren, die die Einhaltung der Vorgaben mittels Zertifikat bescheinigen.

Werbung und Adresshandel

Personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung des Betroffenen zu Zwecken der Werbung und des Adresshandels weitergegeben werden.

Von diesem Grundsatz gibt es - bezogen auf postalische Direktwerbung - jedoch zahlreiche Ausnahmen. So dürfen personenbezogene Daten zu Zwecken der Werbung oder des Adresshandels ohne Einwilligung verarbeitet oder genutzt werden, wenn

- der Betroffene anhand der Werbung erkennen kann, welches Unternehmen seine Adressdaten hierfür weitergegeben hat, oder
- Unternehmen ihre eigenen Kunden bewerben.

Hinweis:

Beim Versand von Werbung müssen Betroffene auf ihr Recht, der Zusendung der Werbung widersprechen zu können, hingewiesen werden.

Auskunfteien

Unternehmen dürfen unter bestimmten Voraussetzungen geschäftsmäßig personenbezogene Daten erheben und verarbeiten, um diese Dritten zu übermitteln. Dies geschieht insbesondere bei Auskunfteien, die anderen Unternehmen Angaben zur Kreditwürdigkeit von Privatpersonen verkaufen.

Folgende personenbezogene Daten dürfen an eine Auskunftei übermittelt werden:

- Forderungen, die durch rechtskräftige Urteile festgestellt worden sind,
- Forderungen im Rahmen von Insolvenzverfahren,
- ausdrücklich anerkannte Forderungen,
- jede unbestrittene Forderung, wenn sie mindestens zweimal schriftlich angemahnt und auf die Meldung bei einer Auskunftei hingewiesen wurde,
- jede Forderung, die den Vertragspartner zur fristlosen Kündigung berechtigt, wenn vorher über die Meldung bei einer Auskunftei informiert wurde.

Videoüberwachung

Die DSGVO trifft keine explizite Regelung zur Videoüberwachung. In der Praxis müssen Sie sich hier also am BDSG und der Rechtsprechung orientieren.

Wenn Videoüberwachung in Unternehmen eingesetzt wird, soll sie oft dem Schutz von Objekten (unter anderem vor Diebstahl) oder Personen dienen. Auch wenn hierbei in den meisten Fällen keine gezielte Beobachtung und Kontrolle der Mitarbeiter beabsichtigt ist, können deren Datenschutz- und Persönlichkeitsrechte von der Videoüberwachung berührt sein.

Beispiel:

In Banken und Parkhäusern sind ebenso wie in Kassenbereichen von Warenhäusern und Museen häufig Videokameras angebracht, mit denen zwangsläufig auch die dort Beschäftigten überwacht werden.

Die Zulässigkeit einer Videoüberwachung von Beschäftigten richtet sich nach unterschiedlichen Vorschriften - je nachdem, ob der überwachte Bereich öffentlich zugänglich ist (z.B. Straße, Warenhaus) oder nicht (z.B. Räumlichkeiten des Unternehmens). Der Begriff „öffentlich zugänglich“ meint dabei einen Raum, in dem sich jedermann berechtigt aufhalten kann, ohne in irgendwelche Rechtsbeziehungen zum Inhaber des Hausrechts für diesen Raum treten zu müssen.

Videoüberwachung darf grundsätzlich eingesetzt werden zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts und zur Wahrnehmung berechtigter Interessen.

Hinweis:

Solche berechtigten Interessen können zum Beispiel Diebstahlschutz oder die Dokumentierung von Schäden zwecks Nachvollziehbarkeit sein.

Sind aber Beschäftigte von der Überwachung betroffen, so ist die Überwachung nur eingeschränkt zulässig. Etwa rechtfertigt allein das Hausrecht nicht die Videoüberwachung von Beschäftigten, da sie sich der Überwachung nicht durch Verlassen der Räumlichkeiten entziehen können. Wenn Beschäftigte dauerhaft von Überwachungskameras erfasst werden, müssen deshalb zusätzliche Abwägungskriterien herangezogen werden.

In jedem Fall ist eine Videoüberwachung durch geeignete Maßnahmen kenntlich zu machen. Diese Hinweispflicht schließt heimliche Videoüberwachungen grundsätzlich aus. Dazu hat das Bundesarbeitsgericht festgestellt, dass eine verdeckte Videoüberwachung im öffentlichen Bereich nur dann zulässig ist, wenn sie das einzige Mittel zur Überführung eines Beschäftigten ist, gegen den der konkrete Verdacht vorliegt, eine Straftat begangen zu haben.

2.5 Schritt 5: Verträge anpassen

Auch bestehende Verträge mit Servicefirmen, Cloud-Dienstleistern und Dienstleistern für Textverarbeitung, Terminplanung oder andere Formen der Datenverarbeitung müssen bis zum 25.05.2018 an das neue Recht angepasst werden.

2.6 Schritt 6: Datenschutzinformationen anpassen

Die Datenschutzbestimmungen auf Unternehmenswebsites sowie die Hinweise zur Datenverarbeitung müssen angepasst werden. Beide sollten außerdem jedem Auftrag sowie jedem Arbeitsvertrag beigefügt werden. Enthalten sollten sie jeweils insbesondere die nachfolgend aufgeführten Rechte der Betroffenen (z.B. Kunden).

Das Recht auf Auskunft

Jeder Betroffene hat das Recht auf (kostenfreie) Auskunft über die zu seiner Person gespeicherten Daten. Hierzu gehören

- die zur eigenen Person gespeicherten Daten einschließlich der Angabe, woher sie stammen und an wen sie weitergegeben werden, sowie
- die Angabe über den Zweck der Speicherung.

Sie dürfen eine Auskunft nur dann ablehnen, wenn keine Benachrichtigungspflicht besteht. Der Betroffene hat grundsätzlich Anspruch auf eine vollständige Auskunft. Alle Angaben, für die nach dem Gesetz grundsätzlich eine Auskunftsverpflichtung besteht, müssen mitgeteilt werden. Wenn Sie keine oder nur teilweise Auskunft erteilen, müssen Sie im Allgemeinen auch begründen, aufgrund welcher gesetzlichen Bestimmung oder Tatsache Sie die Auskunft verweigern oder beschränken. Eine solche Begründung ist nur entbehrlich, wenn sonst der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Überdies müssen Sie, wenn Sie nur teilweise Auskunft erteilen, auf die Unvollständigkeit der Auskunft ausdrücklich hinweisen.

Hinweis:

Bei Zweifeln an der Korrektheit Ihrer Auskunft haben Ihre Kunden (bzw. alle Betroffenen) die Möglichkeit, sich an die zuständige Datenschutzkontrollinstitution zu wenden oder gerichtliche Klage einzureichen.

Das Recht auf Einsicht

Die Übersicht über die unternehmensinterne automatisierte Verarbeitung personenbezogener Daten kann von jedermann unentgeltlich eingesehen werden. Sie muss vor allem folgende Angaben enthalten:

- Name oder Firma des Verantwortlichen,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift des Verantwortlichen,
- Zwecke der Erhebung, Verarbeitung und Nutzung der Daten,
- Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten,
- Empfänger der Daten,
- Regelfristen für die Löschung der Daten,
- etwaige geplante Datenübermittlung in Drittstaaten.

Hinweis:

Unternehmen mit mehr als 250 Mitarbeitern müssen eine solche Übersicht - also ein Verfahrensverzeichnis, das die Datenverarbeitungsprozesse im Unternehmen katalogisiert - führen. Entscheidend ist nur die Anzahl der Mitarbeiter und nicht, ob diese auch tatsächlich Daten verarbeiten.

Das Recht auf Benachrichtigung

Sie sind verpflichtet, alle Betroffenen individuell zu benachrichtigen, über die Sie Daten ohne deren Kenntnis erhoben haben und deren Daten Sie speichern oder verarbeiten möchten - und das bereits bei der ersten Datenspeicherung!

Die Benachrichtigung muss umfassen:

- Kontaktdaten des Verantwortlichen und gegebenenfalls seines DSB,
- Zwecke der Datenverarbeitung, gegebenenfalls berechtigte Interessen des Verantwortlichen oder eines Dritten an der Datenverarbeitung,
- Empfänger oder Kategorien von Empfängern personenbezogener Daten,
- Meldung der Übermittlung von Daten in ein Drittland,
- Speicherdauer,
- Auskunftsrechte, Rechte auf Berichtigung, Löschung, Einschränkung, Widerspruch und Datenübertragbarkeit sowie Beschwerderechte bei Aufsichtsbehörden.

Das Recht auf Berichtigung

Ihr Unternehmen ist verpflichtet, unrichtige Daten zu berichtigen. Es liegt aber auch am Betroffenen selbst, darauf hinzuweisen, wenn Daten unrichtig oder überholt sind. Geschätzte Daten müssen als solche deutlich gekennzeichnet werden.

Das Recht auf Löschung

Sie müssen Daten löschen, wenn

- die Speicherung unzulässig ist,
- die erteilte Einwilligung zur Datenspeicherung widerrufen wurde,
- es sich um Daten bezüglich ethnischer Herkunft, politischer Meinungen, religiöser oder philosophischer Überzeugungen, der Gewerkschaftszugehörigkeit, der Gesundheit, des Sexuallebens, strafbarer Handlungen oder Ordnungswidrigkeiten handelt und Sie deren Richtigkeit nicht beweisen können,
- für eigene Zwecke verarbeitete Daten für die Erfüllung des Speicherungszwecks nicht mehr erforderlich sind oder
- geschäftsmäßig zum Zweck der Übermittlung verarbeitete Daten aufgrund einer am Ende des vierten Kalenderjahres nach der ersten Speicherung vorzunehmenden Prüfung nicht mehr erforderlich sind. Soweit es sich um Daten über erledigte Sachverhalte handelt, muss bereits zum Ende des dritten Kalenderjahres nach der ersten Speicherung die Löschverpflichtung überprüft werden.

Gelöscht werden müssen personenbezogene Daten, die aus automatisierter Datenverarbeitung oder aus einer manuellen, also ohne Automationsunterstützung geführten Datei stammen - nicht aber einzelne Daten, die in nicht dateimäßig strukturierten Akten festgehalten sind.

Hinweis:

Sind allerdings komplette Akten unzulässig angelegt, so sind sie ebenfalls zu vernichten. Dies gilt im Allgemeinen auch für nicht mehr erforderliche Akten.

Als besonderen Löschungsanspruch sieht die DSGVO ein „Recht auf Vergessenwerden“ vor: Wenn Sie die zu löschenden Daten öffentlich gemacht haben (z.B. im Internet), müssen Sie vertretbare Schritte unternehmen, um die Stellen, die diese Daten verarbeiten, darüber zu informieren, dass der Betroffene die Löschung aller Links zu diesen Daten bzw. die Löschung aller Kopien oder Replikationen dieser Daten verlangt.

Hinweis:

Sie sollten die veränderten Anforderungen bei den Löschpflichten präzise in Ihren Löschkonzepten abbilden, um nachweisen zu können, dass Sie die Vorgaben der DSGVO einhalten.

Beachten Sie dabei unbedingt, dass die gesetzlichen Aufbewahrungsfristen für Unternehmen, etwa die steuerliche Aufbewahrungsfrist für Rechnungen und Bücher von zehn Jahren, jedoch zwingend vorgehen.

Das Recht auf Sperrung

Personenbezogene Daten sind immer dann zu sperren, wenn einer fälligen Löschung besondere Gründe entgegenstehen. Derartige besondere Gründe sind etwa

- gesetzlich, satzungsmäßig oder vertraglich festgelegte Aufbewahrungsfristen,
- schutzwürdige Interessen des Betroffenen, etwa wenn ihm sonst Beweismittel verlorengehen, und
- ein unverhältnismäßig hoher Aufwand wegen der besonderen Art der Speicherung.

Außerdem müssen personenbezogene Daten gesperrt werden, wenn der Betroffene ihre Richtigkeit bestreitet und sich weder deren Richtigkeit noch deren Unrichtigkeit feststellen lässt. Die Tatsache der Sperrung darf dann ebenfalls nicht übermittelt werden.

Hinweis:

Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur in Ausnahmefällen übermittelt oder genutzt werden.

Das Recht auf Datenübertragbarkeit

Mit der DSGVO neu eingeführt wurde das Recht auf Datenübertragbarkeit: Betroffene haben unter bestimmten Voraussetzungen Anspruch darauf, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten.

Hinweis:

Dieser Anspruch ist allerdings beschränkt auf die Daten, die der jeweilige Betroffene dem Verarbeiter zur Verfügung gestellt hat.

Das allgemeine Widerspruchsrecht

Betroffene haben das Recht, unter bestimmten Voraussetzungen sogar einer rechtmäßigen Datenverarbeitung zu widersprechen. Begründet ist dies, sofern

- besondere Umstände in der Person des Betroffenen vorliegen und deswegen
- das schutzwürdige Interesse des Betroffenen das Interesse des Verantwortlichen an der Erhebung, Verarbeitung oder Nutzung der entsprechenden personenbezogenen Daten überwiegt.

Werden die Daten zum Zweck der Direktwerbung verarbeitet, können Betroffene jederzeit Widerspruch gegen die Verarbeitung einlegen.

Das Widerspruchsrecht besteht nicht, wenn eine Rechtsvorschrift die Erhebung, Verarbeitung oder Nutzung vorschreibt.

3 Sanktionen bei Verstößen

Verletzungen des Schutzes personenbezogener Daten müssen unverzüglich an die zuständige Aufsichtsbehörde gemeldet werden. Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt (etwa aufgrund einer geeigneten Verschlüsselung).

Stellt die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten dar, muss auch die betroffene Person ohne unangemessene Verzögerung benachrichtigt werden - es sei denn, es kann eine Kenntnisnahme durch Dritte verhindert oder das Risiko reduziert werden.

Hinweis:

Fehler bei der Umsetzung der Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen werden mit Bußgeldern von bis zu 2 % des Umsatzes geahndet. Das Gleiche gilt auch für Fehler bei der Datenschutzfolgenabschätzung.

Wenn Ihr Unternehmen einem Betroffenen durch eine unzulässige oder unrichtige Datenverarbeitung einen Schaden zufügt, besteht eine Schadenersatzpflicht, in schweren Fällen gar ein Anspruch auf Schmerzensgeld.

Für Ihr Unternehmen steigen durch die DSGVO auch die zivilrechtlichen Haftungsrisiken aufgrund von Datenschutzverstößen. So sind nunmehr materielle und immaterielle Schäden zu erstatten, die auf Verstößen gegen die Verordnung beruhen. Die ausdrückliche Nennung immaterieller Schäden wird in der Praxis zu einer erheblichen Veränderung gegenüber der bisherigen Rechtslage führen.

Eine weitere Neuerung ist die ausdrückliche Erweiterung der Haftung auch auf Auftragsverarbeiter.

Hinweis:

Gerade vor dem Hintergrund der erweiterten Haftung ist es umso wichtiger, dass Sie Ihre Datenschutzmaßnahmen umfassend dokumentieren. Nur so können Sie sich angesichts der massiv erweiterten Beweislast nach der DSGVO effektiv gegen Schadenersatzforderungen verteidigen.

Die DSGVO sieht Bußgelder von bis zu 4 % des gesamten weltweiten Jahresumsatzes eines Unternehmens bzw. 20 Mio. € vor, wobei der jeweils höhere Wert gilt.

Hinweis:

Die DSGVO enthält einen Katalog von Kriterien zur Bußgeldbemessung. An diesen Vorgaben können Sie sich orientieren, um Strukturen und Prozesse zu schaffen, die sicherstellen, dass Sie bei Fehlern möglichst geringen Risiken ausgesetzt sind.

4 Fazit

Zum 25.05.2018 gilt das neue Datenschutzrecht. Es gibt keine Übergangsfrist. Nutzen Sie insbesondere die Schritte 1 bis 6 als erste Hilfestellung und bereiten Sie Ihr Unternehmen vor, sonst drohen empfindliche Sanktionen!

Mit freundlichen Grüßen