Das sollte Sie interessieren ...

Das neue Datenschutzrecht – Datenschutz-Grundverordnung (DSGVO)

Richtig reagieren und Sanktionen vermeiden

Hand aufs Herz: welchen Stellenwert hat das Datenschutzrecht in Ihrem Unternehmen in der täglichen Praxis? Oder bleibt es gar gänzlich unberücksichtigt?

Diese Fragen sollten Sie nicht abtun, denn jede einzelne Datenschutzlücke stellt ein nicht (mehr) vernachlässigbares Geschäftsrisiko dar: Die Prüfungsdichte und Sanktionshäufigkeit von Seiten der Aufsichtsbehörden nimmt stark zu, ebenso steigt mit zunehmender Verbreitung moderner Datenverarbeitungs- und Informationstechnik auch deren Verletzlichkeit. Dazu kommt eine neue Rechtslage.

Neue Bestimmungen, denen Ihr Unternehmen bezüglich Datenschutz genügen muss, hat der europäische Verordnungsgeber mit der **Datenschutz-Grundverordnung** (DSGVO) formuliert. Sie ist seit dem 24.05.2016 in Kraft und soll in allen Staaten der Europäischen Union (EU) für grundsätzlich gleiche Standards sorgen, um so zu gleichen Wettbewerbsbedingungen für alle Unternehmen auf dem europäischen Markt beizutragen.

Unabhängig davon, ob Sie sich bereits mit der DSGVO befasst haben, steht nun ein sehr wichtiges Datum an: Nach einer zweijährigen Übergangsfrist müssen ab dem **25.05.2018** alle Dokumente und Prozesse der Neuregelung angepasst sein. Besondere Brisanz ergibt sich daraus, dass die DSGVO im Vergleich zum Bundesdatenschutzgesetz (BDSG) einige Änderungen vorsieht. Allerdings gilt das (novellierte) BDSG auch mit Inkrafttreten der DSGVO weiter - es sind also beide Regelwerke zu beachten! Dabei hat die DSGVO das letzte Wort: Sofern sie keine ausdrücklichen Möglichkeiten für einzelstaatliche Regelungen vorsieht, verdrängt sie die Vorschriften der einzelnen EU-Mitgliedstaaten zur Datenverarbeitung, also insbesondere die des BDSG.

Auf den folgenden Seiten geben wir Ihnen einen Überblick über das ab dem 25.05.2018 verbindlich geltende Datenschutzrecht für private Unternehmen: Was sind Ihre Pflichten, was sind die Rechte Ihrer Kunden?

1 Grundlagen und Begrifflichkeiten

1.1 Personenbezogene Daten

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

1.2 Anwendungsbereich

Allgemein unterliegen Unternehmen dem Datenschutzrecht nur dann, wenn sie personenbezogene Daten

- unter Einsatz von Datenverarbeitungsanlagen oder
- in bzw. aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben.

Hinweis:

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

1.3 Verbot mit Erlaubnisvorbehalt

Für die Verarbeitung personenbezogener Daten gilt der allgemeine Grundsatz des Verbots mit Erlaubnisvorbehalt: Es ist grundsätzlich verboten, was nicht ausdrücklich erlaubt ist. In diesem Fall bedeutet das konkret, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten verboten sind, es sei denn,

- sie sind 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, ist zu beachten, dass:

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

Erhebung, Verarbeitung und Nutzung personenbezogener Daten unterliegen einer Vielzahl von Einschränkungen. Bereits bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen. Diese Festlegung ist grundsätzlich bindend: Änderungen oder Erweiterungen des Verarbeitungszwecks sind grundsätzlich nur erlaubt, wenn sie mit dem ursprünglichen Erhebungszweck vereinbar sind. Als Kriterien zur Beurteilung der Vereinbarkeit einer Zweckänderung gelten etwa:

- die Verbindung zwischen den Zwecken,
- der Gesamtkontext der Datenerhebung,
- die Art der personenbezogenen Daten,
- mögliche Konsequenzen der zweckändernden Verarbeitung für den Betroffenen und
- das Vorhandensein von angemessenen Sicherheitsmaßnahmen (z.B. eine Verschlüsselung).

Hinweis:

Eine strikte Zweckbindung besteht für Daten, die ausschließlich zur Datenschutzkontrolle, Datensicherung, Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage oder zur wissenschaftlichen Forschung gespeichert werden.

Eine Verwendung für andere als die zuvor festgelegten Zwecke kommt als Ausnahme unter anderem in Betracht

- zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten, oder
- wenn die Daten allgemein zugänglich sind oder veröffentlicht werden dürften.

Hinweis:

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Auf der anderen Seite liegt keine Zweckänderung vor, soweit die Daten verwendet werden für:

- die Rechnungsprüfung,
- die Nutzung von Aufsichts- und Kontrollbefugnissen,
- Organisationsuntersuchungen sowie
- Ausbildungs- und Prüfzwecke der speichernden Stelle.

2 Ihre Pflichten im Umgang mit Daten

2.1 Datensparsamkeit

Die Erhebung und Verarbeitung personenbezogener Daten muss auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein (Prinzip der Datensparsamkeit). Die Daten sind grundsätzlich beim Betroffenen - also insbesondere beim Kunden - zu erheben. Es ist ihm mitzuteilen, zu welchem Zweck dies geschieht. Er hat Anspruch darauf zu erfahren,

- welche verantwortliche Stelle die Daten erhoben hat und
- welche Zweckbestimmung der Datenerhebung zugrunde liegt.

- Ohne Mitwirkung des Betroffenen dürfen Daten nur erhoben werden, wenn
- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
- die Erhebung beim Betroffenen einen unverhältnismäßig hohen Aufwand zur Folge hätte und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

2.2 Vorabkontrolle

Für automatisierte Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, sieht das BDSG eine Prüfung vor Beginn der Verarbeitung vor. Beispielhaft genannt werden zwei Fallgestaltungen, in denen die Vorabkontrolle notwendig ist:

1. Bei der Verarbeitung von personenbezogenen Daten besonderer Art.
2. Bei Verfahren zur Bewertung von Persönlichkeit, Fähigkeit, Leistung oder Verhalten des Betroffenen.

Eine Vorabkontrolle entfällt, wenn

- eine gesetzliche Verpflichtung zur Durchführung der Datenverarbeitung besteht,
- die Einwilligung des Betroffenen vorliegt,
- die Erhebung, Verarbeitung oder Nutzung im Rahmen der Zweckbestimmung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erfolgt.

2.3 Datensicherheit

Datenschutz-Folgenabschätzung

Der Vorabkontrolle (siehe Punkt 2.2) eng verwandt ist die mit der DSGVO neu eingeführte Datenschutz-Folgenabschätzung. Sie sieht vor, dass Risiken und deren mögliche Folgen für die persönlichen Rechte und Freiheiten der Betroffenen vorab bewertet werden - vor allem Eintrittswahrscheinlichkeit und Schwere eines möglichen Risikos.

Überdies müssen Unternehmen auch systematisch die verfolgten Zwecke der Datenverarbeitung beschreiben. Ebenso müssen Maßnahmen, Garantien und Verfahren formuliert bzw. geprüft werden, mit denen bestehende Risiken eingedämmt und die sonstigen Vorgaben der Verordnung eingehalten werden können.

Ergibt die Datenschutz-Folgenabschätzung, dass die geplante Datenverarbeitung tatsächlich ein hohes Risiko zur Folge hätte, muss die verantwortliche Stelle die zuständige Aufsichtsbehörde konsultieren, sofern sie keine Maßnahmen zur Eindämmung des Risikos trifft.

Hinweis:

Die Datenschutz-Folgenabschätzung ist ein wichtiges Mittel für Ihr Unternehmen, um die Dokumentationspflichten zu erfüllen. Allein aus diesem Grund sollten Sie zeitnah Strukturen und Prozesse schaffen, um die detaillierten Anforderungen an den Datenschutz zu erfüllen.

Maßnahmen zur Datensicherheit

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 die verantwortliche Stelle und der Auftragsverarbeiter hierfür geeignete technische und organisatorische Maßnahmen umzusetzen. Dabei muss das Sicherheitslevel im Verhältnis zum Risiko angemessen sein.

Hinweis:

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

Beachten Sie auch die Pflicht zur Information bei Datenschutzpannen! Wenn Ihr Unternehmen, Verein oder Verband personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen Sie ebenso wie jedes gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen bei Verlust von als besonders gefährdet eingestuften Daten die Betroffenen sowie die Aufsichtsbehörde informieren. Unterbleibt diese Information oder ist sie nicht richtig, nicht vollständig oder nicht rechtzeitig, droht ein Bußgeld!

Sie sollten folgende Prozesse und Dokumente in Ihrem Unternehmen prüfen bzw. vorhalten, um die deutlich erweiterten Nachweispflichten der DSGVO zu erfüllen:

- Dokumentation der Datenverarbeitungsprozesse im Unternehmen,
- Datenschutzerklärungen, insbesondere im Online-Handel (erweiterte Informationspflichten durch die DSGVO),
- Einwilligungserklärungen (verschärfte formale Vorgaben durch die DSGVO),
- Prozess für den Widerruf der Einwilligung,
- an die DSGVO angepasste Version der Betriebsvereinbarungen,
- Prozesse zur Umsetzung von Widersprüchen,
- Vereinbarungen zur Auftragsverarbeitung (Haftungsregelung, Dokumentation),
- Prozess bei Datenpannen (neue Vorgaben),
- Verfahren, um Daten in gängigem elektronischen Format übertragen zu können,
- zielgruppengerechte Schulungen (Neuerungen der DSGVO und eigener Prozesse),
- Risk Assessment (Festlegung geeigneter technisch-organisatorischer Maßnahmen),
- Privacy Impact Assessment (als Methode der Datenschutz-Folgenabschätzung; siehe oben),
- Monitoring nationaler Gesetzgebung,
- Fortbildungen.

Hinweis:

Ihr Unternehmen sollte ein effektives Datenschutzmanagementsystem mit diesen Prozessen integrieren - und dabei die einzelnen Schritte dokumentieren. So kann auch gegenüber einer Aufsichtsbehörde nachgewiesen werden, dass geeignete Strategien erarbeitet und Maßnahmen ergriffen wurden.

3 Datenschutzbeauftragter

3.1 Notwendigkeit einer Bestellung

Da der Bundesgesetzgeber von einer entsprechenden Öffnungsklausel in der DSGVO Gebrauch gemacht hat, bleibt es diesbezüglich bei der bisher geltenden Rechtslage: Unternehmen müssen einen Datenschutzbeauftragten bestellen, wenn mehr als neun Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Auskunfteien, Adresshändler sowie Markt- und Meinungsforschungsinstitute müssen in jedem Fall einen Datenschutzbeauftragten bestellen.

3.2 Stellung im Unternehmen

Der Datenschutzbeauftragte ist unmittelbar dem Geschäftsführer unterstellt und in der Ausübung seiner Aufgaben weisungsfrei. Zudem genießt er einen besonderen Kündigungsschutz: Während der Bestellung bzw. bis ein Jahr danach darf ihm nur aus wichtigem Grund (z.B. Arbeitsverweigerung) gekündigt werden.

Hinweis:

Der besondere Kündigungsschutz gilt jedoch nicht für freiwillig bestellte Datenschutzbeauftragte.

Der Geschäftsführer eines Unternehmens ist nicht an das Votum des Datenschutzbeauftragten gebunden. Die Letztverantwortung für die Datenverarbeitung verbleibt damit bei der Unternehmensleitung.

Der Datenschutzbeauftragte muss die erforderliche „Fachkunde und Zuverlässigkeit" besitzen. Die verantwortliche Stelle ist verpflichtet, dem Datenschutzbeauftragten 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 Datenschutzbeauftragte bestellt werden.

3.3 Aufgaben

Die Aufgaben des Datenschutzbeauftragten umfassen

- die Durchführung der Vorabkontrolle; die verantwortliche Stelle für die Datenverarbeitung muss ihm dafür Informationen zur Verfügung stellen,
- auf Anfrage die Beratung hinsichtlich der Daten-schutz-Folgenabschätzung und die Überwachung ihrer Durchführung,
- die datenschutzrechtliche Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten,
- die Überwachung der Einhaltung der datenschutz-rechtlichen 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.

Hinweis:

Anders als das bisherige Recht sieht die DSGVO umfassende Überwachungspflichten für den Datenschutzbeauftragten vor. Es bleibt daher abzuwarten, ob und in welchem Umfang Gerichte und Behörden Datenschutzbeauftragte künftig als „Überwachergaranten" im Rahmen einer straf- und ordnungswidrigkeitenrechtlichen Verantwortlichkeit einordnen.

4 Sonderfälle der Datenverarbeitung

4.1 Datenverarbeitung im Auftrag

Entschließt sich Ihr Unternehmen zum Outsourcing einzelner Tätigkeiten (z.B. der Personalbuchhaltung), müssen dabei verschiedene rechtliche, technische und organisatorische Voraussetzungen erfüllt werden.

Werden dem Auftragnehmer zu einem solchen Zweck personenbezogene Daten überlassen, findet daten-schutzrechtlich 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.

4.2 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 müssen von Werbung Betroffene auf Ihr Recht, der Zusendung der Werbung zu widersprechen, hingewiesen werden.

4.3 Auskunfteien

Unternehmen dürfen unter bestimmten Voraussetzungen geschäftsmäßig personenbezogene Daten erheben und verarbeiten, um diese Dritten zu übermitteln. So geschieht dies 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.

4.4 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 Kreditinstituten 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).

Hinweis:
Der Begriff „öffentlich zugänglich" charakterisiert hier einen Raum, in dem sich jedermann berechtigt aufhalten kann, ohne in irgendwelche Rechtsbeziehungen zum Inhaber des Hausrechts dieses Raums treten zu müssen.

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

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 (BAG) 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.

Handelt es sich um einen nicht öffentlichen Raum, etwa einen Arbeitsplatz, so richtet sich die Zulässigkeit der Videoüberwachung nach den strengeren Vorgaben des Beschäftigtendatenschutzes im BDSG. Bei der Bewertung der Zulässigkeit ist danach eine umfassende Verhältnismäßigkeitsprüfung durchzuführen.

Hinweis:
Aus Sicht des BAG ist eine Videoüberwachung von Arbeitsplätzen nur ausnahmsweise durch besondere Sicherheitsinteressen des Arbeitgebers oder zur Aufklärung von Straftaten eines Beschäftigten gerechtfertigt.

Generell ist von den folgenden Grundsätzen auszugehen, die sich in der Rechtsprechung entwickelt haben:

- Es müssen überwiegende schutzwürdige Interessen des Arbeitgebers vorliegen (z.B. Schutz von Firmeneigentum), die vor Beginn der Videoüberwachung durch konkrete Anhaltspunkte und Verdachtsmomente belegt sind (keine vage Vermutung und kein pauschaler Verdacht gegen alle Beschäftigten).
- Die Durchführung der Videoüberwachung erfolgt mittels einer offen sichtbaren Anlage nach vorheriger Information der Belegschaft.
- Der Einsatz von verdeckten Kameras ist nur zulässig, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind sowie die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist.

- Der Betriebsrat oder die Personalvertretung sind involviert worden.
- Es wurde eine strenge, einzelfallbezogene Verhältnismäßigkeitsprüfung durchgeführt.

Die weitere Verarbeitung oder Nutzung von Videoaufnahmen ist nur zulässig, soweit sie erforderlich ist. Kontrollfrage: Genügt nicht die einfache Beobachtung? Werden die durch Videoüberwachung erhobenen Daten einer bestimmten Person zugeordnet, muss sie über die Verarbeitung oder Nutzung benachrichtigt werden. Werden Daten nicht mehr für den angestrebten Zweck der Überwachung benötigt oder stehen schutzwürdige Interessen des Betroffenen der weiteren Speicherung entgegen, müssen sie unverzüglich gelöscht werden.

5 Die Rechte Ihrer 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 in Fällen ablehnen, in denen auch 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 auf die Unvollständigkeit der Auskunft ausdrücklich hinweisen. Überdies müssen Sie dann im Allgemeinen auch begründen, aufgrund welcher gesetzlichen Bestimmung oder Tatsache Sie eine Auskunft verweigern oder beschränken. Eine solche Begründung ist nur entbehrlich, wenn sonst der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

Hinweis:

Bei Zweifeln an der Korrektheit einer Auskunft haben Ihre Kunden die Möglichkeit, sich an die zuständige Datenschutzkontrollinstitution zu wenden oder eine gerichtliche Klage einzureichen.

Das Recht auf Einsicht

Die Übersicht über die unternehmensinterne automatisierte Verarbeitung personenbezogener Daten kann von jedermann unentgeltlich eingesehen werden. Diese Übersicht muss eine Vielzahl von Angaben enthalten.

Es geht dabei vor allem um folgende Angaben:

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift der verantwortlichen Stelle,
- 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:

Für Unternehmen ab 250 Mitarbeitern ist es verbindlich, eine solche Übersicht - also ein Verfahrensverzeichnis, das die Datenverarbeitungsprozesse im Unternehmen katalogisiert - zu führen.

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 seines Datenschutzbeauftragten,
- 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, oder
- für eigene Zwecke verarbeitete Daten für die Erfüllung des Speicherungszwecks nicht mehr erforderlich sind,
- 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. Ebenso ist im Allgemeinen mit nicht mehr erforderlichen Akten zu verfahren.

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 die betroffene Person 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.

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 Beweismittel verloren gingen, 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 dieser Sperrung darf dann ebenfalls nicht übermittelt werden.

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

Das Recht auf Datenübertragbarkeit

Neu eingeführt durch die DSGVO wurde das Recht auf Datenübertragbarkeit: Kunden haben unter bestimmten Voraussetzungen den Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten. Allerdings ist dies auf die Daten beschränkt, die der jeweilige Kunde 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 der verantwortlichen Stelle an der Erhebung, Verarbeitung oder Nutzung der entsprechenden personenbezogenen Daten überwiegt.

Werden die Daten für Direktwerbung verarbeitet, können Betroffene jederzeit Widerspruch gegen die Verarbeitung einlegen.

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 Datenschutz-Folgenabschätzung.

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:

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

6 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.

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.

7 Fazit

Zum 25.05.2018 endet die Übergangsfrist. Nehmen Sie die Hinweise ernst, bereiten Sie sich bzw. Ihr Unternehmen vor und vermeiden Sie so empfindliche Sanktionen!

Weitere Informationen zur Vorbereitung auf die DSGVO finden Sie auch im Internet - auf der Website der Aufsichtsbehörde für Schleswig-Holstein:

ULD – Unabhängiges Landeszentrum für Datenschutz: www.datenschutzzentrum.de