Ott&Partner

Info-Service

Unser großes Thema: Das neue Datenschutzrecht – Datenschutzgrundverordnung (DSGVO)

April 2018

Nachfolgend geben wir Ihnen einen Überblick über das Datenschutzrecht für private Unternehmen:

1. Grundlagen und Begrifflichkeiten

a) 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.

b) 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.

c) 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.

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.

2. Pflichten im Umgang mit Daten

a) 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.

b) Vorabkontrolle

Für automatisierte Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, sieht das BDSG eine besondere Prüfung vor Beginn der Verarbeitung vor.

c) Datensicherheit

Datenschutz-Folgenabschätzung

Der Vorabkontrolle (siehe Punkt 2.b)) eng verwandt ist die mit der DSGVO neu eingeführte Datenschutz-Folgenabschätzung. Sie sieht vor, dass Risiken und deren mögliche Folgen für die persönli-

chen 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.

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.

Pflicht zur Information bei Datenschutzpannen! Wenn das Unternehmen, Verein oder Verband personenbezogene Daten erhebt, verarbeitet oder nutzt, wird 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.

Folgende Prozesse und Dokumente im Unternehmen sollten geprüft werden bzw. vorgehalten, 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,
- 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),
- Privacy Impact Assessment (als Methode der Datenschutz-Folgenabschätzung; siehe oben),

3. Datenschutzbeauftragter

a) Notwendigkeit einer Bestellung

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.

b) Stellung im Unternehmen

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

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

4. Sonderfälle der Datenverarbeitung

a) 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 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 Datenverar-

beitung 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.

b) 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.

c) 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.

5. Die Rechte Ihrer Kunden

a) 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.

b) 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.

c) 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.

d) 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.

e) 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.

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.

f) 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.

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.

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.

7. Resümee

Das neue komplexe Datenschutzrecht wirft die heutigen Datenschutzregelungen zum großen Teil über den Haufen, betrifft jedes Unternehmen, das personenbezogene Daten nutzt, tritt ab 25.05.2018 in Kraft und sollte deshalb eilig umgesetzt werden.

Weitere Informationen und Handreichungen für Kleinunternehmen und Vereine finden Sie unter https://www.lda.bayern.de/de/kleine-unternehmen.html

Bernhard Ott

Steuerberatung
Ott & Partner

Erhältlich im App Store (iOS)

JETZT BEI Google play (Android)