

Neue EU-Datenschutzgrundverordnung

Datenschutz wird zur Herkulesaufgabe für Unternehmen

Ab dem 25.05.2018 treten die neue EU-Datenschutzgrundverordnung (EU-DSGVO) und auch das überarbeitete BDSG (Bundesdatenschutzgesetz) in Kraft. Für die Unternehmen bedeutet das weitreichende Änderungen und eine große Herausforderung.

Ein Gastbeitrag von Klaus Eder

Die Datenschutz-Skandale in der jüngsten Vergangenheit haben eines bewiesen – Datenschutz spielt eine wichtige Rolle. Niemand will seine persönlichen Daten im Internet ohne seine Einwilligung veröffentlicht sehen.

In modernen Reinigungen und Wäschereien werden heute eine Vielzahl personenbezogener Daten auf unterschiedlichsten Geräten verarbeitet. Die Textilbestellungen von Kunden werden über Internetseiten oder spezielle Eingabegeräte in die entsprechende Software der Wäscherei übertragen, Leistungsdaten der Mitarbeiter werden durch Maschinen erfasst und der Produktionsleitung zur Auswertung zur Verfügung gestellt und die Standorte der LKW des wäschereieigenen Fuhrparks werden durch Handys oder andere Geräte an den Fuhrparkleiter weitergegeben. Das Kleiderwechselverhalten beispielsweise von Beschäftigten im Gesundheitswesen mit Berufsbekleidung kann ausgewertet werden. Die sozialen Medien werden zur Kundenbindung beziehungsweise Mitarbeitergewinnung eingesetzt. In all den genannten Bereichen werden personenbezogene Daten verarbeitet und der Datenschutz muss durch die Unternehmen gewährleistet werden.

Ab dem 25.05.2018 kommen auf die Unternehmen im Bereich Datenschutz weitreichende Änderungen zu. Die neue EU-Datenschutzgrundverordnung (EU-DSGVO) und auch das überarbeitete BDSG (Bundesdatenschutzgesetz) treten in Kraft. Die genannten Bestimmungen beschäftigen sich mit dem Umgang von Unternehmen mit personenbezogenen Daten, also Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen wie zum Beispiel der Name, die Adresse, die

Kontodaten, das Kfz-Kennzeichen, Standortdaten, IP-Adressen oder Cookies.

Scharfe Kontrollen, drastische Strafen

Die Vorbereitungszeit von fast zwei Jahren auf die gesetzlichen Veränderungen haben viele Unternehmen ungenutzt verstreichen lassen. Großes Schreckgespenst sind die hohen Bußgelder von bis zu 10 Millionen Euro oder zwei Prozent des Weltjahresumsatzes bei formellen und 20 Millionen Euro oder vier Prozent des Weltjahresumsatzes bei materiellen Verstößen sowie die vielen offenen Fragen hinsichtlich der rechtssicheren Umsetzung der Anforderungen im Unternehmen. Der Artikel Art. 83 Abs. 1 DS-GVO klingt hier fast schon wie eine Kriegserklärung an alle Unternehmen, die keine Vorkehrungen getroffen haben: „Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen ... in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.“

Wie kann die Umsetzung noch gelingen ?

Für viele Unternehmen stellt die große Menge an Informationen, die zu dem Thema „Datenschutz“, beispielsweise im Internet vorhanden sind und die vielen gesetzlichen Regelungen im Zusammenhang mit dem Datenschutz eine große Herausforderung dar. Deshalb lohnt sich ein genaues Studium der 99 Artikel der DSGVO, um einen Überblick zu erhalten. Insbesondere die Anforderungen an die Datenverarbeitung wie Rechtmäßigkeit, Transparenz / Informationspflichten, Sicherheit der Verarbeitung und Auftrags(daten)verarbeitung spielen eine große Rolle.



Viele Unternehmen sind schlecht vorbereitet.

In Artikel 5: „Grundsätze für die Verarbeitung personenbezogener Daten“ legt die DSGVO fest, dass personenbezogene Daten auf

- rechtmäßige Weise („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“),
- für festgelegte, eindeutige und legitime Zwecke ... („Zweckbindung“),
- auf das notwendige Maß beschränkt ... („Datenminimierung“),
- sachlich richtig („Richtigkeit“), erforderlich ... („Speicherbegrenzung“) und mit
- angemessener Sicherheit ... („Integrität und Vertraulichkeit“)

verarbeitet werden. Besonders kritisch ist hier die sogenannte Rechenschaftspflicht des Artikel 5 zu sehen, welche von den Unternehmen verlangt, dass die Einhaltung der oben genannten Grundsätze schriftlich nachweisbar sein muss. Dieser Verpflichtung können Unternehmen nachkommen, indem eine schriftliche Dokumentation beispielsweise in Form einer Tabelle angelegt wird. Diese Tabelle enthält die Anforderungen von Art. 5 DSGVO und deren betriebsspezifische Umsetzung und Kontrolle. Ein Unternehmen kann zusätzlich nachweisen, dass es beispielsweise den Grundsatz der Rechtmäßigkeit der Verarbeitung einhält, indem es eine Betriebsvereinbarung/ Leitlinie für die Mitarbeiter erstellt, welche regelt, dass nur Daten verarbeitet werden dürfen, bei denen eine Rechtsgrundlage für die Datenverarbeitung und gegebenenfalls eine Einwilligung der betroffenen Person vorliegt. Die Dokumentation der Prüfung der Rechtmäßigkeit erfolgt im Verarbeitungsverzeichnis und wird im Rahmen von Begehungen und Datenschutzaudits geprüft.

Allein schon aus dieser Anforderung geht hervor, dass die Unternehmen nun Dokumente benötigen, welche die Erfüllung der rechtlichen Vorgaben belegen.

Achtung bei Auskunftsanfragen

Wie schon das BDSG in seiner alten Fassung, sieht auch die Datenschutz-Grundverordnung (DSGVO) ein Auskunftsrecht für von der Datenverarbeitung betroffenen Personen vor (Art. 15 DSGVO). Nach Art. 15 Abs. 1 DSGVO haben betroffene Personen das Recht, von Unternehmen eine Bestätigung darüber zu erhalten, ob diese sie betreffende personenbezogene Daten verarbeiten. Ist das der Fall, haben die betroffenen Personen ein Recht auf Auskunft über diese Daten und darüber hinausgehende Informationen zu deren Verarbeitung.

Nach Art. 12 Abs. 1 der Datenschutz-Grundverordnung können die Informationen schriftlich, auf

elektronischem Wege (in einem gängigen elektronischen Format z.B. PDF) oder, auf Verlangen der betroffenen Person, mündlich erteilt werden. Wichtig ist im Rahmen der Auskunftserteilung die Feststellung der Identität des Auskunftssuchenden, zum Beispiel durch seinen Personalausweis. Auch sind hier die Fristen zu beachten. Die Auskunft ist unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen. Die Erstauskunft ist für die betroffene Person kostenlos, für weitere Auskünfte können Unternehmen ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen. Jedoch gibt die DSGVO weiterhin vor, dass betroffene Personen ihr Recht auf Auskunftserteilung in angemessenen Abständen kostenlos wahrnehmen können sollten.

Unternehmen sollten rechtzeitig dokumentierte, organisatorische Vorkehrungen treffen, um die Forderung der DSGVO nach schneller und vollständiger Beantwortung von Auskunftersuchen erfüllen zu können. Ein schriftliches Verfahren mit einer Festlegung der einzelnen Bearbeitungsschritte sowie den Verantwortlichkeiten ist hier dringend notwendig.

Verzeichnis von Verarbeitungstätigkeiten

Vielen Unternehmen fehlt der Überblick, welche personenbezogenen Daten in ihrer Verantwortung „verarbeitet“ werden. Gemäß den Vorgaben der DSGVO werden die meisten Unternehmen ein Verzeichnis von Verarbeitungstätigkeiten erstellen und führen müssen, da regelmäßige Kunden- und/oder Beschäftigtendaten verarbeitet werden.

Unter Verarbeitung versteht man dabei jeden mit oder ohne Hilfe automatisierter Verfahren ➔



Besonders kritisch ist die sogenannte Rechenschaftspflicht.

Zum Autor



Dipl. Betriebswirt (FH) Klaus Eder ist seit 20 Jahren geschäftsführender Gesellschafter der Intrasys-Beratungsgesellschaft. Sein Hauptaufgabengebiet ist die Einführung und Optimierung von Managementsystemen (ISO 9001, ISO 14001, usw.) und der Datenschutz. Seit fast zehn Jahren beschäftigt er sich mit dem Thema „Datenschutz in Unternehmen“. Eder ist Lehrbeauftragter an der Hochschule Landshut zu den Themen „Integration von Managementsystemen“, „Projektmanagement“ und „Betriebswirtschaftslehre“.

ausgeführten Vorgang, wie erheben, erfassen, organisieren, ordnen, speichern, anpassen oder verändern, auslesen, abfragen, verwenden, offenlegen durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, abgleichen oder verknüpfen, einschränken, löschen oder vernichten von Daten, also eigentlich allen Tätigkeiten im Zusammenhang mit personenbezogenen Daten.

Das Verzeichnis von Verarbeitungstätigkeiten dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Unternehmen dabei, gemäß Art. 5 Abs. 2 DSGVO nachzuweisen, dass die Vorgaben aus der DSGVO eingehalten werden (Rechenschaftspflicht). Muster für die genannten Verzeichnisse sind bei den jeweiligen Landesbeauftragten für den Datenschutz online erhältlich.

Folgende Verarbeitungstätigkeiten sind häufig in Unternehmen anzutreffen: Personalaktenführung/Stammdaten, Lohn-, Gehalts- und Bezügeabrechnung, Urlaubsdatei, Bewerbungsverfahren, Videoüberwachung an Arbeitsplätzen usw.

Ein großes Augenmerk sollte auf den Zweck der Verarbeitung gelegt werden. Warum verarbeitet unser Unternehmen diese Daten eigentlich? Gibt es dafür eine Rechtsgrundlage? Gibt es Einwilligungen? Diese Verzeichnisse sollten so klar formuliert sein, dass die Aufsichtsbehörde die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung einschätzen kann.

Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind jedoch keinesfalls alle von der DSGVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur ein Baustein.

In engem Zusammenhang mit den Verzeichnissen von Verarbeitungstätigkeiten steht die Datenschutz-Folgenabschätzung (DSFA). Diese ist im Grunde nichts anderes, als die bisher im deutschen Datenschutzrecht schon bekannte Vorabkontrolle (§ 4d Abs. 5 BDSG). Immer dann, wenn in den Verarbeitungsverzeichnissen besonders sensible Daten verarbeitet werden oder die Datenverarbeitung dazu bestimmt war, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten, muss der Datenschutzbeauftragte, die dem Verfahren innewohnenden besonderen Risiken für die Rechte und Freiheiten des Betroffenen prüfen und gibt am Ende dieser Prüfung eine Stellungnahme zur Rechtmäßigkeit der Datenverarbeitung ab. Genau wie die Vorabkontrolle dient die Datenschutz-Folgenabschätzung also der



In modernen Textilpflegebetrieben werden heute eine Vielzahl personenbezogener Daten verarbeitet. Zum Beispiel werden die Leistungsdaten der Mitarbeiter an den Maschinen erfasst.

Bewertung von Risiken und deren mögliche Folgen für die persönlichen Rechte und Freiheiten der Betroffenen.

In der Wäscherei oder Reinigung sind beispielsweise die Videoüberwachung von Verkaufsräumen oder Arbeitsplätzen oder die geographische Ortung von Mitarbeitern kritisch zu betrachten. Liegt der Zweck der Verarbeitung dieser Daten im Bereich der Arbeitssicherheit oder der Durchsetzung des Hausrechts, könnte eine Verarbeitung erlaubt sein.

Einwilligungen einholen

Im Datenschutzrecht gilt das Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass eine Datenverarbeitung verboten ist, wenn sie nicht durch ein Gesetz ausdrücklich erlaubt ist oder der Betroffene in die Verarbeitung eingewilligt hat.

Die Einwilligung des Betroffenen muss freiwillig sein und auf einer ausführlichen, erkennbaren und bestimmten Information des Betroffenen basieren. Der Betroffene ist über den Zweck der Verarbeitung seiner Daten zu informieren. Einwilligungen sollten aus Nachweisgründen wenn möglich schriftlich eingeholt werden. Die Möglichkeit der einfachen elektronischen Einwilligung im Internet, zum Beispiel in Online-Shops, wird derzeit nur durch das Telemediengesetz (§ 13 Abs. 2 TMG) geschaffen. Die Einwilligungserklärung kann durch den Betroffenen jederzeit widerrufen werden.

Insbesondere im Vertrieb und Marketing sowie im Vertragswesen ist hier durch die Unternehmen zu prüfen, ob die notwendigen Kundeneinwilligungen beispielsweise für Werbesendungen, Newsletter oder Außendienstbesuche vorliegen. Die Einwilligungen von Mitarbeitern sollten auch im Rahmen der Veröffentlichung von Fotos der Mitarbeiter beispielsweise



Im Datenschutz gilt das Verbot mit Erlaubnisvorbehalt.

auf Facebook oder auf der Firmenhomepage, eingeholt werden.

Ein weiteres schriftliches Verfahren fordert die DSGVO für das Vorgehen im Rahmen von Verletzungen des Schutzes personenbezogener Daten. Damit sind die umgangssprachlich als „Datenpannen“ bezeichneten Vorfälle gemeint, die laut DSGVO „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.“

Innerhalb von 72 Stunden nach Bekanntwerden der Datenschutzverletzung hat eine Meldung an die zuständige Aufsichtsbehörde und ohne unangemessene Verzögerung die Benachrichtigung der betroffenen Person zu erfolgen. Eine Ausnahme von der Meldepflicht liegt nur vor, wenn die Verletzung nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt.

Datenschutzorganisation festlegen

Zur Datenschutzorganisation zählen neben den oben erwähnten Verfahren (Leitlinien bzw. Betriebsvereinbarungen) zum Umgang mit Datenschutzverstößen oder Auskunftersuchen auch noch weitere Verfahren wie zum Beispiel der Umgang mit E-Mails oder der privaten Internetnutzung im Unternehmen. Hierzu sind Verantwortlichkeiten schriftlich festzulegen. Unternehmen mit einem Managementsystem gemäß DIN EN ISO 9001 können diese Sachverhalte auch im Managementsystem regeln.

Auftragsverarbeitung

Ob Cloud-Computing, die extern erstellte Lohnabrechnung oder die technische Wartung durch IT-Dienstleister – sobald personenbezogene Daten im Auftrag weisungsabhängig verarbeitet werden, liegt eine Auftragsverarbeitung (AV) vor. Unternehmen sind durch die datenschutzrechtlichen Regelungen gezwungen, die Auftragsverarbeiter sorgfältig und unter besonderer Berücksichtigung der technischen und organisatorischen Maßnahmen die der Verarbeiter getroffen hat, auszuwählen. Der Auftragsverarbeiter darf die Daten nur auf Weisung verarbeiten. Unternehmen sollten die bestehenden Prozesse und Verträge zur Datenverarbeitung im Auftrag überprüfen beziehungsweise bei neuen Verträgen die künftige Rechtslage berücksichtigen. Entsprechende Verträge mit dem externen

Lohnbüro, dem Steuerberater oder dem IT-Dienstleister sollten vorliegen.

Datenschutzbeauftragter ab zehn Personen

Bei der Beantwortung und Bearbeitung all dieser Themen ist ein betrieblicher Datenschutzbeauftragter hilfreich. Dieser muss nach § 4f BDSG bestellt werden, wenn im Unternehmen mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden.

Datenschutzbeauftragter kann jede natürliche Person sein, die beispielsweise nicht der Geschäftsführung angehört oder der Verantwortliche für die IT ist, da hier Interessenkollisionen mit Sicherheit nicht zu vermeiden sind. Der schriftlich bestellte Datenschutzbeauftragte muss über eine entsprechende Fachkunde verfügen, die im Rahmen von Schulungen erworben werden kann. Die Aufgabe des Datenschutzbeauftragten besteht darin, zur Einhaltung der Vorschriften zum Datenschutz in seiner Organisation beizutragen. Dies realisiert er beispielsweise durch eine datenschutzrechtliche Schulung seiner Mitarbeiter und die Kontrolle der datenverarbeitenden Prozesse. Unternehmen die nicht über ausreichende personelle Ressourcen verfügen, können auch mit sogenannten externen Datenschutzbeauftragten zusammenarbeiten.

Weitere Informationen einholen

Inzwischen ist das Internet eine Fundgrube von Musterdokumenten und weiteren Informationen zum Thema DSGVO geworden. Erste Anlaufstelle für Unternehmen sollte die Datenschutzaufsicht des jeweiligen Bundeslandes sein. Auf den Webseiten dieser Behörden finden Unternehmen eine Vielzahl von Vorlagen, Muster und Informationen, die kostenlos heruntergeladen werden können. In schwierigen Fällen kann die Behörde auch direkt angesprochen werden, da es wie bisher zum Selbstverständnis und Aufgabenspektrum dieser Behörden gehört, Unternehmen informierend und gegebenenfalls beratend bei der Umsetzung des Datenschutzes behilflich zu sein.

Umgehend handeln

Zum 25.05.2018 treten die DSGVO sowie das neue Bundesdatenschutzgesetz in Kraft, die wie oben beschrieben eine Vielzahl von Maßnahmen von Unternehmen fordert. Im Rahmen eines gut strukturierten Projekts gilt es die Maßnahmen umzusetzen und somit Rechtssicherheit im Unternehmen zu schaffen. 



Datenschutzbeauftragter muss Fachkunde nachweisen.