Die Datenschutzgrundverordnung

(DSGVO)

Ein Leitfaden

von

Thomas Messingschlager

Rechtsanwalt

In den Büngerten 7

56182 Urbar

In Kooperation und Bürogemeinschaft mit

Dr. Zweipfennig & Partner mbB

Steuerberatungsgesellschaft

Inhaltsverzeichnis

Datenschutzgrundverordnung

(DSGVO)

Vorwort und Gebrauchsanleitung

Am 25.05.2018 tritt die DSGVO in Kraft. Parallel dazu gilt ab diesem Datum das neugefasste Bundesdatenschutzgesetz (BDSG). Dieser Leitfaden soll aufzeigen, ob und inwiefern Handlungsbedarf bei der Verarbeitung von Daten besteht und eine erste Hilfe zur Erfüllung der gesetzlichen Anforderungen bieten.

Der Text der DSGVO ist im Internet z.B. unter www.dsgvo-gesetz.de zu finden. Der Text des BDSG ist z.B. unter https://dsgvo-gesetz.de/bdsg-neu/ veröffentlicht.

Ziel und Zweck der Verordnung

Die Datenschutzverordnung hat in erster Linie zum Ziel, dass Daten nur im notwendigen Maß verarbeitet werden und dass die Verarbeitung möglichst sicher erfolgt, so dass Missbrauch, Verlust oder ungewollte Veränderungen ausgeschlossen sind. Sie hat aber auch ein „pädagogisches" Ziel: Durch verschiedene Dokumentationspflichten sollen Datenverarbeiter dazu angehalten werden, sich selbst bewusst zu machen, welche Verantwortung mit der Datenverarbeitung einhergeht und wo eventuell Schwachstellen im System lauern.

Alle im Text angegebenen Artikel beziehen sich auf die DSGVO.

Unterstrichene Begriffe sind am Ende des Textes erläutert.

Teil I

Erster Überblick

1. Für wen gilt die DSGVO?

Die DSGVO ist von den meisten Unternehmen, Vereinen und ähnlichen Organisationen zu beachten, die regelmäßig personenbezogene Daten speichern (Art. 2 DSGVO).

2. Welche Anforderungen müssen in jedem Falle erfüllt werden?

a) **Technische und organisatorische Maßnahmen** zur Sicherstellung, dass die Datenverarbeitung rechtmäßig, inhaltlich richtig, sicher, nur für den vorgesehenen Zweck, und nur bei Erforderlichkeit erfolgt (Art. 5, 25 DSGVO).

b) **Dokumentation** der wesentlichen Datenverarbeitungsvorgänge (Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DSGVO)

c) Transparente **Information und Auskunft** gegenüber den Betroffenen (d.h. denjenigen Personen, deren Daten verarbeitet werden), u.U. Löschung der Daten und Zurverfügungstellung der Daten an die Betroffenen auf Antrag (Art. 12 ff., 20 DSGVO).

3. Welche weitergehenden Anforderungen sind im Einzelfall maßgeblich?

a) **Risiko – und Folgeabschätzung** (Datenschutzfolgeabschätzung) für den Fall einer Datenschutzverletzung (Art. 35 DSGVO).

b) **Datenschutzbeauftragter**
Benennung einer Person, die die Einhaltung der gesetzlichen Datenschutzbestimmungen überwacht (Art. 37 ff. DSGVO und § 38 Bundesdatenschutzgesetz).

c) **Besonderes Pflichten bei Auftragsdatenverarbeitung**
Falls Dritte eingeschaltet werden, um die erhobenen Daten zu verarbeiten, müssen besondere Sicherheitsvorkehrungen getroffen werden (Art. 28 DSGVO).

4. Konsequenzen im Fall von Verlust und Missbrauch von Daten

Pflicht zur Meldung an die Aufsichtsbehörde bzw. an die betroffene Person (Art. 33, 34 DSGVO).

5. Konsequenzen bei Nichtbeachtung der DSGVO

Anspruch betroffener Personen auf Unterlassung, Schadenersatz, Schmerzensgeld und Bußgelder (z.B. §§ 823 ff, 249 ff, 1004 BGB, Art. 82 u. 83 DSGVO),

Teil II

Die DSGVO im Einzelnen

Zu 1) Für wen gilt die DSGVO?

Unternehmen

Frage	Ja	Nein
Bietet mein Unternehmen Dienstleistungen oder Waren in Deutschland oder in der EU an?		
Habe ich mindestens einen Mitarbeiter in meinem Unternehmen?		

Falls auch nur eine der Fragen mit „Ja“ beantwortet wird, ist die DSGVO zu beachten. Jegliche Verarbeitung, (d.h. insbesondere Erhebung, Speicherung und Weiterleitung) personenbezogener Daten muss dann den Anforderungen der Verordnung genügen (Art. 2 DSGVO).

Vereine, Stiftungen o.ä.

Für Vereine, Stiftungen o.ä. Organisationen, die ihren Sitz in Deutschland oder einem Mitgliedsland der EU haben und personenbezogene Daten verarbeiten (z.B. Führung eines Mitgliederverzeichnisses) gilt die DSGVO ebenfalls.

Rein private Datenverarbeitung wie z.B. die Archivierung von Adressen aus dem Bekanntenkreis ist nicht von der DSGVO erfasst.

Zu 2) Welche Anforderungen müssen in jedem Falle erfüllt werden?

a) **Technische und organisatorische Maßnahmen** zur Sicherstellung, dass die Datenverarbeitung rechtmäßig, inhaltlich richtig, sicher, nur für den vorgesehenen Zweck, vertraulich und nur bei Erforderlichkeit erfolgt (Art. 25 DSGVO).

aa) **Rechtmäßigkeit** der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist gem. Art. 6 Abs. 1 DSGVO nur dann rechtmäßig, wenn

- die betroffene Person zuvor eine **Einwilligung** erteilt hat oder
- die Verarbeitung **zur Erfüllung eines Vertrages** oder einer sonstigen Verpflichtung erforderlich ist oder
- sie zur Wahrung **berechtigter Interessen** des Verantwortlichen oder eines Dritten erforderlich ist.

Die **Einwilligung** zur Verarbeitung personenbezogener Daten setzt keine bestimmte Form voraus. Sie kann schriftlich, aber auch in elektronischer Form abgegeben werden. Sie muss aber nachweislich

- freiwillig
- für einen bestimmten definierten Fall (also z.B. nicht „für alle heute und in Zukunft relevante Zwecke“)
- nach klarer und verständlicher Information darüber, wer die Daten verarbeitet und zu welchem Zweck
- durch eine eindeutige bestätigende Handlung
  also z.B. durch Ankreuzen einer Erklärung – sog. „opt-in“ (das bloße Stehenlassen eines bereits vorangekreuzten Kästchens reicht nicht)

abgegeben worden sein.

Einwilligungen können allerdings jederzeit ohne Angabe von Gründen widerrufen werden (Art. 7 Abs. 3 DSGVO). Die Ausübung

des Widerrufs muss so einfach wie die Erteilung der Einwilligung sein.

Die Berufung auf die Erforderlichkeit der Datenverarbeitung zur **Erfüllung eines Vertrages** setzt voraus, dass die fraglichen Daten tatsächlich benötigt werden. Dies ist z.B. für den Namen und die Adresse des Käufers eines Kühlschranks unproblematisch der Fall. Bereits das Geburtsdatum wird aber weder für die Lieferung der Ware, noch für die Erfüllung eventueller Gewährleistungsansprüche relevant sein. Bestehen Zweifel an der Volljährigkeit, reicht eine einmalige Prüfung beim Kauf aus. Eine Speicherung des Geburtsdatums ist nicht erforderlich. Erst recht sind in diesem Zusammenhang die Speicherung bestimmter Vorlieben oder politischer/religiöser Überzeugungen des Kunden nicht vom Vertragszweck abgedeckt. Diese Daten dürfen daher nur im Falle einer Einwilligung oder bei Vorliegen sonstiger „berechtigter Interessen" des Verantwortlichen verarbeitet werden.

Als **„sonstige Verpflichtung"**, zu deren Erfüllung personenbezogene Daten verarbeitet werden dürfen, kommt insbesondere die steuerrechtliche Verpflichtung in Betracht, Belege 10 Jahre aufzubewahren.

„**Berechtigte Interessen"** des Verantwortlichen sind nur dann eine Rechtsgrundlage zur Datenverarbeitung, **sofern nicht** die Interessen der betroffenen Person überwiegen.

Ein berechtigtes Interesse liegt schon dann vor, wenn ein Zweck verfolgt wird, der gesetzlich nicht untersagt ist - z.B. wenn der Verantwortliche Marktforschung betreiben will und hierzu Kundendaten und Angaben zur gekauften Ware speichert. Ein berechtigtes Interesse kann auch dann bestehen, wenn der Verantwortliche Kundendaten speichert, um ihm später passende zusätzliche Angebote unterbreiten zu können (z.B. zum Kauf von Winterreifen nach Kauf eines PKW). In diesem Zusammenhang ist allerdings zu beachten, dass die Zusendung unbestellter Werbung gegen das Gesetz gegen den unlauteren Wettbewerb (UWG)verstoßen kann.

Wann allerdings die Interessen der betroffenen Person einer Verarbeitung entgegenstehen und überwiegen, ist vom

Gesetzgeber nicht näher definiert und wird daher in der Praxis vermutlich zu Streitigkeiten führen. Bis sich hier ein klareres Bild abzeichnet, empfiehlt sich Zurückhaltung bei der Verarbeitung von personenbezogenen Daten, die nicht zur Erfüllung von vertraglichen oder sonstiger Verpflichtungen dienen und zu deren Verarbeitung keine Einwilligung erteilt wurde.

Gegen jede Datenverarbeitung die aufgrund eines „berechtigten Interesses" des Verantwortlichen erfolgt, hat der Betroffene gem. Art. 21 Abs. 1 DSGVO ein **Widerspruchsrecht**. Der Datenverarbeiter darf dann nur weiterverarbeiten, wenn er „zwingende Gründe" für die Verarbeitung nachweisen kann, was selten der Fall sein dürfte. Dafür trägt er zudem die Darlegungs- und Beweislast.

Ohne jede Begründung können Betroffene gemäß Art. 21 Abs. 2 DSGVO widersprechen, wenn die Verarbeitung ihrer Daten zum Zwecke des Direktmarketings erfolgt.

bb) Inhaltliche **Richtigkeit** der verarbeiteten Daten

Verantwortliche müssen entsprechende organisatorische Vorkehrungen treffen, dass die Daten ihrer Mitarbeiter, Kunden und sonstigen Betroffenen stets auf dem aktuellen Stand sind.

cc) **Sicherheit** der Datenverarbeitung

Der Verantwortliche hat geeignete organisatorische und technische Maßnahmen zu treffen, dass Daten nicht in die Hände Unbefugter geraten oder in sonstiger Weise missbraucht werden. Es sind daher die *marktüblichen Programme zum Schutz vor Cyberattacken* jeder Art zu installieren und regelmäßig durch Updates auf dem aktuellen Stand zu halten – und zwar auch für mobile Geräte wie Notebooks oder Mobiltelefone. Insbesondere ist auch auf *ständige Aktualisierung* der verwendeten Systeme zu achten *(Patch-Management)*, damit Sicherheitslücken immer möglichst zeitnah geschlossen werden können.

Darüber hinaus ist, je nach Sensibilität der Daten und Schadensrisko eine *Pseudonymisierung und Verschlüsselung* der Daten vorzunehmen. Der Gesetzgeber hat leider auch hier keine präzisen Ausführungen dazu gemacht, unter welchen

Voraussetzungen Daten zu pseudonymisieren bzw. zu verschlüsseln sind und welche Standards hier maßgeblich sein sollen. Vielmehr soll, je nach Art und Inhalt der Datenverarbeitung eine Abwägung maßgeblich sein: je nach Art, Umfang, Umständen und Zweck der Datenverarbeitung sollen nach dem Stand der Technik geeignete Maßnahmen getroffen werden, um den Datenschutz zu gewährleisten. Bei der Auswahl der Maßnahmen sollen auch die Höhe des Schadensrisikos einerseits und die entstehenden Kosten berücksichtigt werden.

Leider lassen sich angesichts dieser vagen Formulierung des Gesetzgebers noch keine verbindlichen Angaben dazu machen, welche Maßnahmen von den Aufsichtsbehörden als ausreichend bzw. nicht ausreichend eingestuft werden. Im Zweifel wird man daher dazu raten müssen, maximale Sicherungsvorkehrungen zu treffen, die mit den handelsüblichen Systemen mit vertretbarem finanziellem Aufwand zu erreichen sind.

Bei sensiblen Daten empfiehlt sich daher z.B. eine Zip-Verschlüsselung bzw. eine Verschlüsselung mit AES-256. Auch eine zusätzliche Firewall wie z.B. „Sonicwall" kann sinnvoll sein, um unbefugte Zugriffe auszuschließen.

Beim Versand von Mails ist die Gefahr des Missbrauchs höher als beim Speichern auf dem eigenen PC, da die Daten sowohl beim Transport als auch beim Empfänger von Unbefugten abgefangen werden könnten.

Von den meisten Mailservern bereits heute zwar eine Transportverschlüsselung vorgenommen. In Betracht kommt auch der *Versand Zip-verschlüsselter Nachrichten*. Zusätzliche Sicherheit kann aber durch Lösungen wie z.B. *PGP oder S/MIME* gewonnen werden, bei denen Mails nur bei Eingabe eines Passwortes gelesen werden können. Eine praktischere Lösung kann es darstellen, wenn der Verwender seine Mails durch einen speziellen Provider verschlüsselt verwendet. Hier muss nicht mit umständlichen Passwörtern hantiert werden; vielmehr ist es ausreichend, wenn der Empfänger der Mails sich einmal bei dem Provider anmeldet. Die Verschlüsselung ist dann bei jeder folgenden Mail zwischen dem Versender und dem Empfänger gewährleistet. Der Service ist kostenpflichtig. Zusätzlich bieten diese Provider jedoch meist Dienste wie die Protokollierung des Empfangs an (ohne Absendung einer Empfangsbestätigung

durch den Empfänger). Angeboten wird das Verfahren z.B. von „regify".

Soweit personenbezogene Daten auf einer Webseite z.B. eines Onlineshops eingegeben werden, ist *HTTPS als Transportverschlüsselung* eine geeignete Sicherheitsmaßnahme. Hierfür wird ein entsprechendes SSL- Zertifikat benötigt.

Beim Betrieb eines *WLAN-Netzes* ist dieses mit *WPA2 und einem 20-stelligen Passwort* zu betreiben. Der Zugang zum Router ist ebenfalls durch entsprechende Passwörter zu verhindern. Auch hier kann eine zusätzliche Firewall sinnvoll sein.

Mobile Geräte wie Laptops, Mobiltelefone, USB-Sticks etc. sollten mit einem Kennwort zum Entsperren des Nutzer-Accounts ausgestattet werden. Eine Datenträgerverschlüsselung bringt zusätzliche Sicherheit und wird vom Bundesamt für Sicherheit empfohlen. Eine kostenfreie Lösung ist z.B. das Produkt VeraCrypt (https://veracrypt.codeplex.dom

Gefahren drohen aber nicht nur durch vorsätzlichen Missbrauch: auch *Fahrlässigkeit der eigenen Mitarbeiter* stellt eine erhebliche Gefahrenquelle dar. Mitarbeiter sollten daher über den sicheren und vertraulichen Umgang mit Daten instruiert und stichprobenartig überprüft werden. Regelmäßige Information der Mitarbeiter durch Rundmails oder Aushänge sind geeignete flankierende Maßnahmen.

Zur Sicherheit der Datenverarbeitung gehört auch die regelmäßige **Datensicherung** zum Schutz vor Verlust. Bei Nutzung von Cloudlösungen sollten die Daten verschlüsselt in die Cloud gesendet werden, damit der Provider keinen Zugriff erhält.

Bei Ausgabe von Mobiltelefonen an Mitarbeiter sollte sichergestellt sein, dass die GPS-Funktion deaktiviert ist.

dd) nur für den vorgesehenen Zweck

Daten sind lediglich für festgelegte, eindeutige Zwecke zu erheben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

ee) Vertraulichkeit der Datenverarbeitung

Es ist sicherzustellen, dass lediglich die Berechtigten Zugriff zu den Daten haben. Bei der Beschäftigung von Mitarbeitern sollte ein Berechtigungsmanagement eingeführt werden, durch welches sichergestellt ist, dass nur die jeweils zuständigen Mitarbeiter Zugriff auf personenbezogene Daten haben. Hierzu gehören auch physische Sicherheitssysteme wie abschließbare Aktenschränke und abschließbare Arbeitsräume.

Beim Versand von E-Mails an mehrere Empfänger sollte gegebenenfalls von der Möglichkeit der „Blindkopie" (BCC) Gebrauch gemacht werden, damit die Empfänger nicht die E-Mailadresse der jeweils anderen Empfänger sehen können.

Beim Einsatz mobiler Geräte z.B. in öffentlichen Verkehrsmitteln muss sichergestellt sein, dass Dritte nicht mitlesen können. Gegebenenfalls kann eine Sichtschutzfolie hilfreich sein.

ff) Erforderlichkeit der Datenverarbeitung/**Aufbewahrungsdauer**

Daten sollen nur dann verarbeitet werden, wenn diese tatsächlich benötigt werden. Der Verantwortliche hat die Daten dann wieder zu löschen, wenn sie für den ursprünglichen Zweck nicht mehr benötigt werden und eine Aufbewahrungspflicht nicht aus anderen (z.B. steuerrechtlichen) Gründen besteht. Die Daten sind auch dann zu löschen, wenn der ursprünglich bestehende Rechtsgrund für die Verarbeitung wegfällt (z.B. Widerruf der Einwilligung).

b) Dokumentation der wesentlichen Grundzüge der im Unternehmen / im Verein o.ä. erfolgenden Datenverarbeitung (Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DSGVO)

Der Verantwortliche hat künftig die Pflicht, die Einhaltung der Vorschriften gegenüber der Aufsichtsbehörde auf Verlangen nachzuweisen. Er hat hierzu eine entsprechende Dokumentation anzufertigen.

Grundsätzlich hat das Verzeichnis folgende Angaben zu enthalten:

- Angabe von Namen, Kontaktdaten des Verantwortlichen,
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern von Daten

Es empfiehlt sich jedoch, ein um folgende Inhalte erweitertes Verzeichnis anzufertigen:

- Konkrete Beschreibung der Verarbeitungstätigkeiten im Sinne der Definition in Art. 4 Nr. 2 DSGVO (erheben, speichern, abfragen, offenlegen usw.)
- Nennung der Rechtsgrundlagen (z.B. Art. 6 DSGVO, Dienstleistungsvertrag, Arbeitsvertrag, Betriebsvereinbarung, Einwilligung etc.

Der Grund hierfür besteht darin, dass die Aufsichtsbehörde auch über diese Aspekte Rechenschaft vom Verantwortlichen verlangen kann. Im Bedarfsfall lässt sich mit dem erweiterten Verzeichnis hierüber schnell Klarheit verschaffen.

Ein vom Bayerischen Landesamt für Datenschutzaufsicht erstelltes Muster des Verzeichnisses findet sich in der Anlage.
Zu beachten ist, dass Auftragsdatenverarbeiter zusätzliche Dokumentationspflichten haben.

c) Transparente **Information und Auskunft** gegenüber den Betroffenen (d.h. denjenigen Personen, deren Daten verarbeitet werden), u.U. Löschung der Daten und Zurverfügungstellung der Daten an die Betroffenen auf Antrag (Art. 12 ff. DSGVO).

Der Betroffene ist in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ darüber zu informieren, was zu welchem Zweck mit seinen Daten gemacht werden soll – und zwar **bevor** es zur Datenverarbeitung kommt.

Offenzulegen sind:

- Angabe von Namen, Kontaktdaten des Verantwortlichen,
- Kontaktdaten des Datenschutzbeauftragten
- Kategorien von Empfängern von Daten
- Zwecke der Verarbeitung und Rechtsgrundlage
- Interessen des Verantwortlichen, wenn er Daten auf der Basis einer Interessenabwägung verarbeitet
- Empfänger der Daten im Falle einer Weiterleitung

Ferner ist anzugeben:

- Dauer der Speicherung
- Hinweis auf Recht auf Auskunft, Berichtigung und Löschung
- Hinweis, dass eine erteilte Einwilligung jederzeit grundlos widerrufen werden kann und dass bei der Verarbeitung von Daten aufgrund „berechtigten Interesses" ein Widerspruchsrecht besteht
- Hinweis auf Beschwerderecht bei der Aufsichtsbehörde

Diese Informationen sollten in Form einer **Datenschutzerklärung** gegeben werden, und zwar sowohl auf der Homepage des Datenverarbeiters als auch bei der Begründung einer Geschäftsbeziehung.

Über das bloße Informations – und Auskunftsrecht hinaus geht das neugeschaffene Recht auf **Datenübertragbarkeit** (Art. 20 DSGVO)

Betroffene haben künftig das Recht, die sie betreffenden personenbezogenen Daten, die sie einem für die Verarbeitung Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Zudem haben sie das Recht, diese Daten auf einfachem Weg zu neuen Anbietern übermitteln zu lassen. Dies soll dem reibungslosen Anbieterwechsel für Kunden gewährleisten.

Zu 3. Welche weitergehenden Anforderungen sind im Einzelfall maßgeblich?

a) **Risiko – und Folgeabschätzung** (Datenschutzfolgeabschätzung) für den Fall einer Datenschutzverletzung (Art. 35 DSGVO).

Sofern eine Datenverarbeitung voraussichtlich hohe Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, hat der Verantwortliche eine genaue Analyse, insbesondere bezüglich der Eintrittswahrscheinlichkeit und der Schwere der Risiken, durchzuführen. Bei der Bewertung der Risiken sollen nach der Vorstellung des Gesetzgebers „Art, Umfang, Umstände und Zweck" der Datenverarbeitung sowie berücksichtigt werden, wobei der Einsatz „neuer Technologien" sich grundsätzlich risikoerhöhend auswirkt. Diese – gelinde gesagt – vage Formulierung präzisiert der Gesetzgeber immerhin insoweit, als dass er Regelbeispiele gibt, wann eine Datenschutzfolge-abschätzung in jedem Falle durchzuführen ist. Dies soll nach dem Gesetzeswortlaut in folgenden Fällen gegeben sein:

a) **systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen**, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) **umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten** gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO

c) **systematische umfangreiche Überwachung** öffentlich zugänglicher Bereiche;

In der Regel wird Ziff. b) am ehesten zur Anwendung kommen. Dies ist der Fall, wenn **„sensible" Daten**, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschafts - zugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer Person oder Daten über

strafrechtliche Verurteilungen oder Straftaten verarbeitet werden (Art. 9 DSGVO).

Die Verarbeitung sensibler Daten allein begründet jedoch noch nicht automatisch ein hohes Risiko. Vielmehr muss in der Regel hinzukommen, dass die Verarbeitung **„umfangreich“** ist. Wann dies der Fall ist, erläutert der Gesetzgeber nicht. Aus den Protokollen der Verhandlungen über den Gesetzestext lässt sich jedoch entnehmen, dass eine „umfangreiche“ Verarbeitung erst dann gegeben sein sollte, wenn „große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene“ verarbeitet werden, die „eine große Zahl von Personen betreffen könnten“

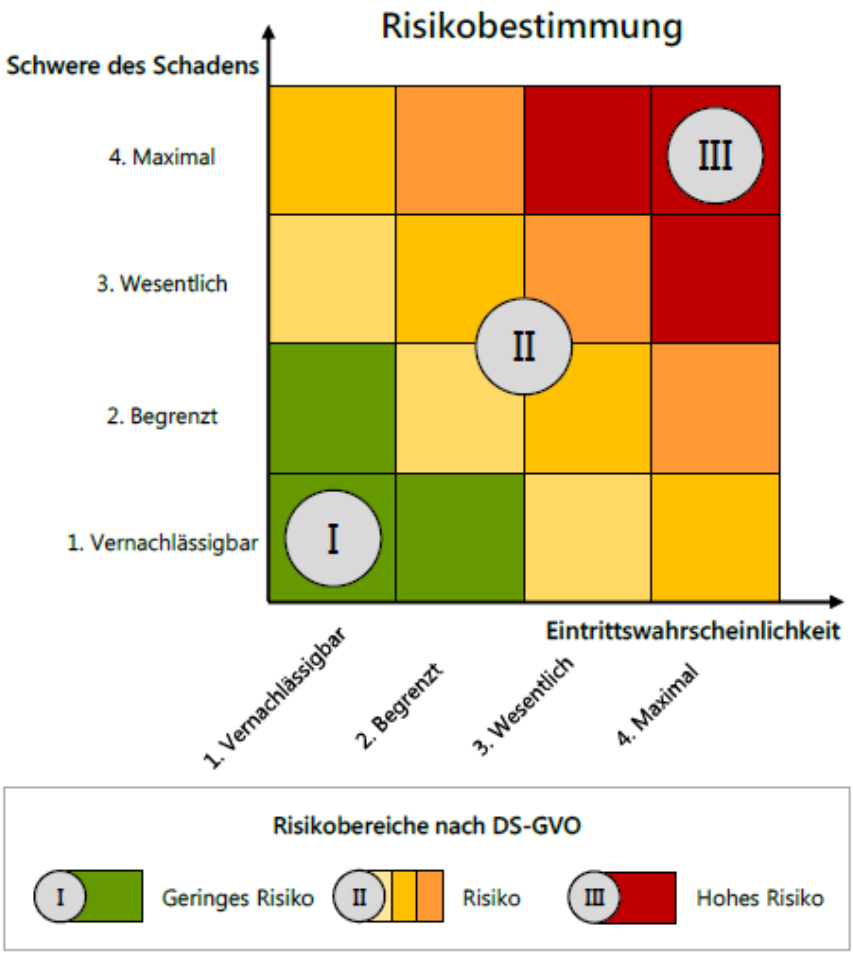
Ferner geht aus der Gesetzesbegründung hervor, dass eine umfangreiche Verarbeitung dann nicht vorliegen soll, wenn ein einzelner Arzt oder Anwalt sensible Daten in seiner Praxis/Kanzlei verarbeitet.

Im Rahmen des Parlamentsentwurfs wurde davon ausgegangen, dass in den anderen Fällen die Schwelle eines „konkreten“ Risikos dann überschritten sei, wenn von der Verarbeitung 5000 Personen innerhalb eines Zeitraums von 12 Monaten betroffen seien (Sydow: Europäische Datenschutzgrundverordnung, Art. 35, Rdnr. 22).

Es ist jedoch zu berücksichtigen, dass der Gesetzgeber die oben genannten Fälle a – c nur als Beispiel formuliert hat. Es ist daher immer zu prüfen, ob ein vergleichbarer Fall vorliegt, der ebenfalls zu hohen Gefahren Rechte und Freiheiten der betroffenen Personen führen könnte.

Die DSGVO sieht vor, dass die zuständigen Aufsichtsbehörden Listen veröffentlichen, in denen Datenverarbeitungen benannt werden, die eine Datenschutzfolgeabschätzung erforderlich machen. Dies ist jedoch bei Herausgabe dieses Leitfadens noch nicht erfolgt.

Immerhin hat das Bayerische Landesamt für Datenschutzaufsicht die nachfolgende graphische Darstellung herausgegeben, die einen Anhaltspunkt für die Bewertung liefert, wann man zu dem gesetzlich genannten „hohen Risiko“ kommt.



Gelangt der Verantwortliche zu der Einschätzung, dass die Datenverarbeitung bei ihm mit hohen Risiken verbunden ist, muss er die Folgenabschätzung durchführen. Diese muss Folgendes enthalten:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Ergibt sich aus der Datenschutz-Folgeabschätzung, dass die Datenverarbeitung mit einem hohen Risiko verbunden wäre, hat der Verantwortliche geeignete Maßnahmen zur Eindämmung des Risikos zu ergreifen. Sollte das Risiko nicht mit hinreichender Sicherheit ausgeschaltet werden können, hat der Verantwortliche vor der Verarbeitung die Aufsichtsbehörde zu konsultieren.

b) Datenschutzbeauftragter

Benennung einer Person, die die Einhaltung der gesetzlichen Datenschutzbestimmungen überwacht (Art. 37 ff. DSGVO und § 38 BDSG = Bundesdatenschutzgesetz).

Ein Datenschutzbeauftragter ist in jedem Falle zu bestellen wenn im Betrieb des Verantwortlichen bzw. im Verein / der Stiftung o.ä. **mindestens 10 Personen damit beschäftigt sind, personenbezogene Daten automatisiert zu verarbeiten** (§ 38 BDSG). Automatisiert ist eine Datenverarbeitung nicht nur dann, wenn z.B. Computer eingesetzt werden, sondern auch dann, wenn z.B. Kopierer oder Kameras verwendet werden.

Falls nicht mindestens 10 Personen damit beschäftigt sind, personenbezogene Daten automatisiert zu verarbeiten, muss dennoch ein Datenschutzbeauftragter insbesondere dann bestellt werden, falls

a) **umfangreich „sensible" Daten**, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer Person, Gesundheitsdaten oder

Daten zum Sexualleben oder der sexuellen Orientierung einer Person oder Daten über strafrechtliche Verurteilungen oder Straftaten verarbeitet werden und die Verarbeitung dieser Daten **zur Kerntätigkeit des Unternehmens / Vereins o.ä. gehört**.

Zur Kerntätigkeit gehört die Verarbeitung der genannten Daten dann, wenn sie wesentlich zur Erreichung des Unternehmenszwecks sind und nicht nur unterstützende Randfunktion haben (wie etwa bei der Lohnbuchhaltung).

Beispiel: Ein Krankenhaus kann ohne die Verarbeitung von Gesundheitsdaten seine Tätigkeit nicht sinnvoll ausüben.

Bezüglich des Merkmals „umfangreich" wird auf die obigen Ausführungen zur Datenschutzfolgeabschätzung Bezug genommen.

b) die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters **in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.**

Ferner bestimmt § 38 Abs. 1 Satz 2 BDSG, dass ein Datenschutzbeauftragter benannt werden muss, wenn

c) **Datenverarbeitungen** vorgenommen werden, die einer **Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen**, oder

d) **personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.**

Nach dem derzeitigen Stand ist somit ein Datenschutzbeauftragter bereits schon dann zu bestellen, wenn die o.g. „sensiblen Daten" von einem Unternehmen/Verein/einer Stiftung verarbeitet werden, ohne dass es auf die Größe des

Unternehmens/der Organisation oder auf den Umfang der Datenverarbeitung ankommt (so z.B. ausdrücklich Bayerisches Landesamt für Datenschutzaufsicht in „Erste Hilfe zur DSGVO“).

Ist ein Datenschutzbeauftragter zu bestellen, kann dieser sowohl ein Angestellter des Verantwortlichen sein als auch ein Außenstehender. Der Datenschutzbeauftragte muss seine Tätigkeit allerdings frei von Weisungen durchführen können und er darf in keinem Interessenkonflikt stehen. Es wird daher überwiegend vertreten, dass der Inhaber des datenverarbeitenden Unternehmens, der Vorstand, Geschäftsführer, Leiter der IT-Abteilung etc. keine geeigneten Personen seien, die zum Datenschutzbeauftragten ernannt werden können.

Die **Aufgaben des Datenschutzbeauftragten** bestehen darin, auf die Einhaltung der Datenschutzgesetze hinzuwirken. Ferner ist er der erste Ansprechpartner im Unternehmen, wenn es um Fragen zur Verarbeitung personenbezogener Daten geht.
Die Aufgaben des Datenschutzbeauftragten sind im Einzelnen in Art. 37 Abs. 1 DSGVO aufgezählt.

c) Besondere Pflichten bei Auftragsdatenverarbeitung

Falls Dritte eingeschaltet werden, um die erhobenen Daten zu verarbeiten, müssen besondere Sicherheitsvorkehrungen getroffen werden (Art. 28 DSGVO).

Dieser Fall kann in der Praxis schnell eintreten: Bereits durch die Weitergabe von personenbezogenen Daten an ein Buchhaltungsunternehmen und sogar gegebenenfalls bei Wartung der IT durch ein externes Unternehmen, bei der Verlagerung von Daten in eine „Cloud“ oder bei der Aktenvernichtung durch ein externes Unternehmen liegt eine „Auftragsdatenverarbeitung“ vor, so dass die besonderen Regelungen der DSGVO zu beachten sind.

Eine Auftragsdatenverarbeitung liegt immer dann vor, wenn eine andere Person oder Organisation personenbezogene Daten im Auftrage des Verantwortlichen verarbeitet.

In diesem Fall sind vom Verantwortlichen folgende Sicherheitsvorkehrungen zu treffen:

- bei der Auswahl des Auftragsdatenverarbeiters ist sicherzustellen, dass dieser hinreichende Garantien (z.B. durch zertifizierte oder bekannte und bewährte Verfahren) dafür bietet, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Bestimmungen erfolgt.

- die vertragliche Beziehung zwischen Verantwortlichem und Auftragsverarbeiter muss so gestaltet sein, dass der Verantwortliche die Kontrolle über den Umgang mit den Daten behält und dass Vertraulichkeit der Datenverarbeitung und die Einhaltung von Sicherheitsstandards gewährleistet ist und zudem geregelt ist, was mit den Daten nach Abschluss der Auftragsverarbeitung geschehen soll.

  Ein vom Bayerischen Landesamt für Datenschutzaufsicht erstelltes Muster finden Sie hier: https://www.lda.bayern.de/media/muster/formulierungshilfe_av.pdf

- Der Auftragsverarbeiter ist verpflichtet, ein Verzeichnis seiner Auftraggeber zu führen (Art. 30 Abs. 2 DSGVO).

Zu 4. Konsequenzen im Fall von Verlust und Missbrauch von Daten

Pflicht zur Meldung an die betroffene Person bzw. an die Aufsichtsbehörde (Art. 33, 34 DSGVO).

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, sind besondere Mitteilungspflichten gegenüber der betroffenen Person bzw. gegenüber der Aufsichtsbehörde zu beachten.

Eine Verletzung liegt insbesondere vor, wenn die betreffenden Daten verlorengehen, aber auch wenn sie unbeabsichtigt oder unrechtmäßig vernichtet, offengelegt oder Dritten zugänglich gemacht werden und eine negative Konsequenz daraus entstehen kann. Dies kann z.B. der Fall sein, wenn ein Einbrecher Computer oder Festplatten stiehlt, ein Laptop verlorengeht oder Daten infolge einer Fehlbedienung gelöscht werden.

Wenn eine solche Schutzverletzung stattfindet, ist die **zuständige Aufsichtsbehörde unverzüglich** (nach dem Gesetzestext „möglichst binnen 72 Stunden“) **zu informieren**. Der Inhalt der Meldung ist in Art. 33 Abs. 2 DSGVO detailliert vorgegeben.

Die Meldepflicht entfällt lediglich, wenn die Verletzung des Schutzes der personenbezogenen Daten „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten“ von Personen führt. Dies kann z.B. dann der Fall sein, wenn entwendete Daten aufgrund ihrer Verschlüsselung nicht von Unbefugten genutzt werden können.

Darüber hinaus hat der Verantwortliche im Falle der o.g. Schutzpflichtverletzungen **den Betroffenen (also die Person, um deren Daten es geht) zu informieren**, wenn „voraussichtlich ein hohes Risiko für dessen persönliche Rechte und Freiheiten entstanden ist. Der Inhalt der Meldung ist in Art. 33 Abs. 2 und Art. 34 Abs. 2 DSGVO detailliert vorgegeben.

Zu 5. Konsequenzen bei Verstößen gegen die DSGVO

Anspruch betroffener Personen auf Unterlassung, Schadenersatz, Schmerzensgeld und Bußgelder (z.B. §§ 823 ff, 249 ff, 1004 BGB, Art. 82 u. 83 DSGVO),

Erfolgt die Datenschutzverletzung infolge Verschuldens des Verantwortlichen (also bei Vorsatz und Fahrlässigkeit), kann der Betroffene Ersatz des ihm durch die Verletzung entstandenen Schadens verlangen. Die Höhe des konkret entstandenen Schadens muss allerdings im Einzelfall genau dargelegt und vor allem – z.B. durch entsprechende Belege - bewiesen werden.

Aber auch für immaterielle Schäden wie z.B. Rufverletzungen bei Bekanntwerden heikler Informationen kann der Betroffene Ausgleich in Form von Schmerzensgeld verlangen. Die jeweilige Höhe ergibt sich aus der einschlägigen Rechtsprechung in vergleichbaren Präzedenzfällen. Sie kann durchaus 4 – oder 5 – stellige Beträge erreichen.

Unabhängig davon, ob ein konkreter Schaden eingetreten ist oder nicht, können die Aufsichtsbehörden Bußgelder in empfindlicher Höhe (bis zu 20 Mio. € bzw. 4 % des Jahresumsatzes) verhängen (Art. 83 DSGVO).

Stand: 17.10.2019

© Rechtsanwalt Thomas Messingschlager

Hinweis: *Das Merkblatt ist eine Zusammenfassung der rechtlichen und technischen Grundlagen des aktuellen Datenschutzrechts und soll einen ersten Einstieg in die Materie ermöglichen. Es erhebt keinen Anspruch auf Vollständigkeit. Obwohl das Merkblatt mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.*

Glossar

Auftragsverarbeiter
eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Betroffener/betroffene Person

jede identifizierte oder identifizierbare Person, auf die sich der Datenverarbeitungsvorgang bezieht.

Datenverarbeitung

Das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Übermitteln, Verknüpfen, Löschen oder ähnliche Tätigkeiten in Bezug auf Daten (weitere Einzelbeispiele in der vollständigen Definition des Art. 4 Nr.2 DSGVO)

personenbezogene Daten

alle Informationen, die sich auf eine identifizierte oder identifizierbare Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Es liegen somit in der Regel auch dann personenbezogene Daten vor, wenn die Informationen unter Zuhilfenahme weiterer verfügbarer Daten und technischer Mittel einer bestimmten Person zugeordnet werden können. Dies ist etwa bei Telefonnummern, KFZ-Kennzeichen, Kundennummern und auch IP-Adressen der Fall. Der Anwendungsbereich der DSGVO und des BDSG-neu endet erst da, wo eine solche Zuordnung auch mit größtmöglichem Aufwand nicht möglich ist.

Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden; (z.B. Führung einer Mitarbeiterakte nicht mit dem vollständigen Namen, sondern mit einer Personalnummer).

Unternehmen

eine Person oder eine Gesellschaft (z.B. GbR, oHG, GmbH, AG) die eine wirtschaftliche Tätigkeit ausübt, oder sonstige Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

Verantwortlicher

Die Person, Behörde, Einrichtung, das Unternehmen oder eine andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;