IHK Magdeburg

Die EU - Datenschutz-Grundverordnung in der praktischen Umsetzung

Stand Dezember 2017

Inhaltsverzeichnis

A) Einführung in die DS-GVO

Vorbemerkungen

Datenschutz ist nichts Neues. In Deutschland gibt es ihn schon seit Jahrzehnten, und auch auf EU-Ebene war er bereits seit 1995 geregelt. Die neue gesetzliche Vorschrift, die EU-Datenschutz-Grundverordnung (DS-GVO), schafft aber ein neues und weit umfangreicheres Rechtsregime. Daran müssen sich alle Unternehmen halten. Um Ihnen die umfassenden Regelungen etwas näher zu bringen, wollen wir Ihnen mit dem Newsletter verständliche Informationen vermitteln, damit Sie sich mit den neuen Vorschriften vertraut machen können. Die IHK hilft Ihnen ebenfalls mit ihrer Beratungskompetenz.

Was ändert sich im Datenschutz?

Am 14. April 2016 verabschiedete das Europäische Parlament die EU-Datenschutz-Grundverordnung. Sie ist am 25.05.2016 in Kraft getreten, gilt aber erst nach einer zweijährigen Übergangsfrist. Dieser Zeitraum dient den nationalen Gesetzgebern, die bisher geltenden Gesetze wie das Bundesdatenschutzgesetz (BDSG) anzupassen. Unternehmen sind angehalten, die Übergangszeit bis zum Gültigwerden der Verordnung zu nutzen, um die internen Datenverarbeitungsprozesse auf Anpassungsbedarf zu überprüfen. Außerdem sollte bei Neuanschaffungen von Datensystemen darauf geachtet werden, dass diese, soweit zum jetzigen Zeitpunkt möglich, die neuen Datenschutzregelungen bereits berücksichtigen.

Jedenfalls ab dem 25. Mai 2018 wird die DS-GVO die bisherige EG-Datenschutzrichtlinie 95/46 und die nationalen Vorschriften wie das BDSG in weiten Teilen ablösen bzw. ersetzen. Sie gilt direkt, d. h. Unternehmen müssen sowohl den Text der VO als auch das Nachfolgegesetz zum BDSG als Rechtsgrundlagen für den Datenschutz verwenden.

Was regelt die DS-GVO?

Beim Datenschutz geht es um den Schutz personenbezogener Daten. Davon sind alle Informationen umfasst, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, wie Name, Geburtsdatum oder IP-Adresse. Der Anwendungsbereich der DS-GVO ist sehr weit gefasst. Es geht um den Schutz dieser Daten als Ausfluss des Persönlichkeitsrechts einer jeden Person.

Was sind die Grundsätze der DS-GVO?

Art. 5 beinhaltet die Grundsätze, die bei einer automatisierten Verarbeitung personenbezogener Daten zu beachten sind:

- *Verbot mit Erlaubnisvorbehalt*

  Da die Verarbeitung personenbezogener Daten in das verfassungsrechtlich geschützte Persönlichkeitsrecht eingreift, ist eine Datenverarbeitung grundsätzlich verboten. Nur, wenn sie z. B. gesetzlich erlaubt oder auf der Einwilligung der betroffenen Person beruht, ist sie erlaubt.

- *Rechtmäßigkeit*

  Die Verarbeitung ist dann rechtmäßig, wenn sie auf einer entsprechenden Grundlage beruht (Rechtsgrundlage, Einwilligung usw.) und der Zwecke der Verarbeitung von der Rechtsgrundlage bzw. der Einwilligung umfasst ist.

- *Transparenz*

  Die betroffene Person muss wissen, wer welche Daten für welchen Zweck verarbeitet. Daher gibt es umfangreiche Betroffenenrechte (z. B. Informationspflichten, Auskunftsrechte, recht auf Berichtigung der Daten, Widerspruchsrecht)

- *Zweckbindung*

  Die Daten dürfen nur für die genannten Zwecke verarbeitet werden. Ausnahmen sind vorgesehen für sog. kompatible Zwecke, also Zweckänderungen, die aber mit dem ursprünglichen Zweck eng zusammenhängen.

- *Datenminimierung*

  Es dürfen nur die personenbezogenen Daten verarbeitet werden, die für die Zweckerreichung notwendig sind.

- *Richtigkeit*

  Die Daten müssen richtig sein, anderenfalls müssen sie berichtigt oder gelöscht werden.

- *Speicherbegrenzung*

  Die Datensparsamkeit ist hierbei zu beachten, also die Frage, wann Daten nicht mehr benötigt und daher gelöscht werden können. Zudem sind alle Möglichkeiten zur Anonymisierung von Daten zu nutzen.

- *Integrität und Vertraulichkeit*

  Die DS-GVO verknüpft sehr stark den Datenschutz mit der Technik. Die IT-Verfahren müssen somit schon von Anfang an darauf ausgerichtet sein, möglichst wenig personenbezogene Daten verarbeiten zu können (privacy by design).

- *Rechenschaftspflicht*

  Das ist der wichtigste Aspekt der Grundsätze! Die verantwortliche Stelle, also das Unternehmen oder die Institution sind verantwortlich für den Datenschutz und seine Beachtung. Dazu ist ein Datenschutzmanagement notwendig – natürlich abhängig von der Größe des Unternehmens, der personenbezogenen Daten, die verarbeitet werden und der Menge und der Qualität der Daten.

  Zumindest muss aber auch in kleineren und mittleren Unternehmen ein Mindestmaß an Dokumentation vorhanden sein, um die Einhaltung des Datenschutzes nachweisen zu können. Denn die Verletzung der Datenschutzpflichten zieht empfindliche Bußgelder nach sich: Bis zu 20 Mio. Euro oder 4 % des weltweiten Umsatzes können von den Aufsichtsbehörden verhängt werden.

B) Zulässigkeit der Datenverarbeitung

Vorbemerkungen

Der Grundsatz lautet schlicht: Jegliche Verarbeitung personenbezogener Daten ist verboten, es sei denn, es gibt eine Erlaubnis dafür. Dieser Satz scheint angesichts einer fortschreitenden Digitalisierung befremdlich, aber er ist Konsequenz des Grundrechtschutzes der personenbezogenen Daten wie er vom Bundesverfassungsgericht festgeschrieben wurde („informationelle Selbstbestimmung“) und er ist Inhalt der Europäischen Menschenrechtskonvention.

Was regelt die EU-Datenschutz-Grundverordnung?

In Artikel 6 sind die verschiedenen Zulässigkeitsgründe für eine Verarbeitung aufgelistet:

1. Die betroffene Person muss über den Umfang der Daten, die verarbeitet werden sollen, sowie den Zweck, zu dem sie verarbeitet werden, ausreichend informiert werden.

Die Einwilligung muss nicht mehr schriftlich erteilt werden. Ihre Erteilung muss aber nachweisbar sein. Insofern ist eine Protokollierung elektronischer Einwilligungen sinnvoll.

Die Einwilligungserklärung muss in leicht zugänglicher und verständlicher Form und in einer klaren und einfachen Sprache vorhanden sein.

Bei der Einholung einer Einwilligung muss die betroffene Person darauf hingewiesen werden, dass sie ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

Die Gegenleistung darf nicht an die Einwilligung in die Verarbeitung von Daten gekoppelt werden, die für die Vertragsausführung nicht erforderlich sind.

Eine auf der Website voreingestellte Einwilligung in Form eines Häkchens („Ich willige in die Verarbeitung meiner Daten ein“) ist keine Einwilligung. Die betroffene Person muss handeln und aktiv ihr Einverständnis ausdrücken.

Wenn die Einwilligung zusammen mit anderen Erklärungen verlangt, muss sie besonders hervorgehoben sein (z. B. drucktechnisch oder als Kasten).

Achtung: Bei Kindern, die das 16. Lebensjahr noch nicht vollendet haben, müssen die Erziehungsberechtigten einwilligen, Art. 8.

Müssen bereits vorliegende Einwilligungen erneut eingeholt werden?

Die Aufsichtsbehörden in Deutschland haben sich darauf verständigt, dass Einwilligungen grundsätzlich nicht erneuert werden müssen, wenn sie nach der bisherigen Rechtslage rechtmäßig eingeholt wurden. Dafür erforderlich ist, dass

- das Kopplungsverbot berücksichtigt wurde,
- der Grundsatz der Freiwilligkeit beachtet wurde und

- der Hinweis auf den jederzeitigen Widerruf erfolgte.

2. Daten, die zur Erfüllung eines Vertrags oder einer vorvertraglichen Maßnahme benötigt werden, dürfen zulässig erhoben werden.

3. Der Verantwortliche muss eine rechtliche Verpflichtung erfüllen und benötigt dafür Daten (z. B. Erhebung der Religionszugehörigkeit im Beschäftigungsverhältnis wegen der Kirchensteuer).

4. Die Verarbeitung ist für die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich, und die Interessen der betroffenen Person überwiegen diese Interessen nicht.

Hierunter kann z. B. die Verarbeitung personenbezogener Daten für die Direktwerbung fallen (s. Erwägungsgrund 47).

5. Unter bestimmten Voraussetzungen können personenbezogene Daten auch weiterverarbeitet werden, wenn die Verarbeitung nicht mehr dem ursprünglichen Zweck entspricht. Hierfür muss der neue Zweck mit dem alten kompatibel, darf also für die betroffene Person nicht überraschend sein. Hierfür muss aber der Verantwortliche eine genaue – dokumentierte – Prüfung anhand der in Art. 6 Abs. 4 festgelegten Kriterien durchführen:

- jede Verbindung zwischen den Zwecken
- der Zusammenhang der Erhebung der Daten, insbesondere hinsichtlich des Verhältnisses zwischen der betroffenen Person und dem Verantwortlichen
- die Art der personenbezogenen Daten (z. B. besonders sensible Daten)
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen
- vorhandene Verschlüsselungen oder Pseudonymisierungen der Daten.

Ergibt die Prüfung, dass der Zweck nicht kompatibel ist, ist eine darauf gestützte Verarbeitung unzulässig, es sei denn, der Verantwortliche holt für den neuen Zweck wiederum eine Einwilligung ein.

6. Rechtsgrundlagen

Die DS-GVO, aber auch das Bundesdatenschutzgesetz (BDSG), das angepasst wird, enthalten selbst Erlaubnistatbestände, nach denen Datenverarbeitung zulässig ist. Hierzu gehören insbesondere Regelungen zur Videoüberwachung und zum Beschäftigtendatenschutz. Die bisherige Vorschrift des § 32 BDSG wird zwar geändert, soll aber im Wesentlichen erhalten bleiben. Sie macht noch einmal deutlich, dass Tarifverträge bzw. Betriebs- und

Dienstvereinbarungen verbindlich datenschutzrechtliche Regelungen für das Beschäftigungsverhältnis treffen können.

C) Datenschutzmanagement

Vorbemerkungen

Die EU-Datenschutz-Grundverordnung (DS-GVO) verlangt von den Unternehmen die Erfüllung der Rechenschaftspflicht. Damit ist die verantwortliche Stelle, also das Unternehmen oder die Institution, verantwortlich für den Datenschutz und seine Beachtung. Dazu ist ein Datenschutzmanagement notwendig – natürlich abhängig von der Größe des Unternehmens, der personenbezogenen Daten, die verarbeitet werden, und der Menge und der Qualität der Daten. Zumindest muss aber auch in kleineren und mittleren Unternehmen ein Mindestmaß an Dokumentation vorhanden sein, um die Einhaltung des Datenschutzes nachweisen zu können. Denn die Verletzung der Datenschutzpflichten zieht empfindliche Bußgelder nach sich: bis zu 20 Mio. Euro oder 4 % des weltweiten Umsatzes können von den Aufsichtsbehörden verhängt werden.

Was verlangt ein Datenschutzmanagement?

1. Planung und Konzeption

Die Risiken, die sich aus der Datenverarbeitung in dem Unternehmen ergeben, müssen hinsichtlich Art, Umfang, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit von Verletzungen und Schäden beachtet werden. Insbesondere geht es um die Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen.

Das Unternehmen muss zunächst seine „Datenschutzpolitik“ beschreiben, also festlegen:

- *die Zuständigkeiten für den Datenschutz im Unternehmen*
    - hierzu gehört auch die Einbindung und Aufgabenstellung des betrieblichen Datenschutzbeauftragten
- *die Sensibilisierung und Schulung der Mitarbeiter*
- *Verpflichtung auf das Datengeheimnis*
    - das ist zwar gesetzlich nicht mehr vorgeschrieben, aber anzuraten; alternativ muss sichergestellt werden, dass die Mitarbeiter, die personenbezogenen Daten verarbeiten, dies nur entsprechend ihrer Aufgabenerfüllung tun. Für Auftragsverarbeiter ist vorgeschrieben, dass sie ihre Mitarbeiter auf die Vertraulichkeit verpflichten müssen.
- *die Durchführung von Kontrollen, ob die getroffenen Regelungen/Anweisungen auch eingehalten werden*
- *den Einsatz datenschutzfreundlicher Technologien*
- *den Stand der Technik als Anforderung an die IT-Sicherheit*

- *die Führung des Verzeichnisses von Verarbeitungstätigkeiten*
- *den Prozess zum Abschluss von Auftragsverarbeitungen oder – bei gemeinsamer Verantwortlichkeit – zum Abschluss entsprechender Vereinbarungen*
- *den Prozess zur Umsetzung der Betroffenenrechte und der Transparenz der Datenverarbeitung*
- *den Prozess zur Durchführung einer Risikobewertung*
- *den Prozess zur Durchführung von Datenschutz-Folgenabschätzungen und einer eventuellen Meldung an die Aufsichtsbehörde*
- *den Prozess zur Meldung von Verletzungen des Datenschutzes (Datenpannen).*

Es sollte geprüft werden, ob es im Unternehmen Anknüpfungspunkte für ein Datenschutzmanagement gibt. Herfür bieten sich z. B. bereits bestehende Compliance-Richtlinien oder ein Qualitätsmanagement sowie ein IT-Sicherheits- oder ein Risikomanagement an.

2. Umsetzung

Hiervon umfasst ist die Konkretisierung der unter 1. genannten Maßnahmen in der Praxis. Dazu gehört eine ausreichende Dokumentation sowie die geeigneten technisch-organisatorischen Maßnahmen.

3. Erfolgskontrolle und Überwachung

Die Planung und Konzeption sowie ihre Umsetzung müssen stetig auf ihre Wirksamkeit hin kontrolliert werden.

4. Optimierung und Verbesserung

Wird unter 3. festgestellt, dass Anpassungen notwendig sind, müssen sie vorgenommen werden. Hierzu gehört auch die Erfüllung des angemessenen Stands der Technik bei den technischen IT-Sicherheitsmaßnahmen, denn die DS-GVO verlangt die Anpassung an entsprechende technische Entwicklungen.

Ergebnis muss jedenfalls sein, dass die Rechtskonformität der Verarbeitung in rechtlicher, technischer und organisatorischer Hinsicht jederzeit nachweisbar ist.

D) Die Einwilligung nach der EU-Datenschutz-Grundverordnung

Die Europäische Datenschutzgrundverordnung (DS-GVO) führt den bisher geltenden Grundsatz des Verbots mit Erlaubnisvorbehalt fort. Datenverarbeitungen sind demnach generell verboten, es sei denn es liegt ein gesetzlicher Erlaubnistatbestand oder eine Einwilligung der betroffenen Person vor. Versinnbildlicht schließt die DS-GVO zunächst alle

Tore, um dann einzelne wieder zu öffnen. Die Einwilligung wird demnach auch unter der DS-GVO eine wichtige Rolle für die Zulässigkeit der Datenverarbeitung sein.

I. Rechtsgrundlage

Nach Artikel 4 Nr. 11 DS-GVO bezeichnet der Ausdruck „Einwilligung der betroffenen Person“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Formale Anforderungen an die Einwilligung enthält § 7 DS-GVO. Die Einwilligungserklärung muss in verständlicher, leicht zugänglicher Form, in klarer und einfacher Sprache sein. Sie darf nicht in den AGB’s oder in der Datenschutzerklärung „versteckt“ werden, sondern ist getrennt von anderen Inhalten darzustellen.

1. Freiwilligkeit

Die Verarbeitung von personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ist zulässig, wenn die betroffene Person hierin ausdrücklich eingewilligt hat. Grundsätzlich gilt das bisher bekannte Prinzip, dass eine Einwilligung freiwillig und ohne jeden Zwang abgegeben werden muss. Nach den Erwägungsgründen, welche der DS-GVO angehängt sind und ihrer Auslegung dienen, gilt eine Einwilligung dann nicht als freiwillig abgegeben, wenn zwischen den Parteien ein klares Ungleichgewicht besteht und es deshalb unwahrscheinlich ist, dass die Einwilligung ohne Zwang abgegeben wurde.

2. Informiertheit

Für das weitere Erfordernis der Informiertheit greift die DS-GVO auf bisher bekannte Grundsätze zurück. Danach genügen Blankoeinwilligungen nicht den Ansprüchen. Vielmehr muss die betroffene Person deutlich verstehen, welche personenbezogenen Daten zu welchem Zweck und von wem verarbeitet werden. Die verantwortliche Stelle muss ausdrücklich genannt werden. Dient eine Verarbeitung mehreren Zwecken, müssen alle Zwecke ausdrücklich genannt und die Einwilligung für sämtliche Zwecke eingeholt werden.

3. Eindeutigkeit

Das Einverständnis in die Verarbeitung muss außerdem eindeutig zum Ausdruck kommen. Dieser Grundsatz bedeutet das Ende von Opt-Out-Wahlmöglichkeiten – Stillschweigen, Inaktivität oder vorangekreuzte Kästchen gehören damit also der Vergangenheit an und werden von der Opt-In-Lösung abgelöst.

4. Kopplungsverbot

Die DS-GVO führt das sogenannte Kopplungsverbot ein. Danach dürfen Verantwortliche Verträge oder die Erbringung von Dienstleistungen nicht davon abhängig machen, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten, die für die Erfüllung des Vertrages nicht erforderlich sind, einwilligt. Umstritten ist, ob das Kopplungsverbot auch dort Anwendung findet, wo Nutzern entgeltfreie – weil zum Beispiel werbefinanzierte – Inhalte und Dienstleistungen angeboten werden. Wird eine vertragliche Leistung entgeltfrei angeboten unter Bereitstellung personenbezogener Daten als Gegenleistung (= Dienstleistung gegen Daten) und kann der angebotene Dienst nur auf diese Weise wirtschaftlich angeboten werden, wird teilweise die Ansicht vertreten, dass das Kopplungsverbot nicht greift. Die Klärung dieser Streitfrage bleibt abzuwarten. Bis zur rechtsverbindlichen Entscheidung der Frage, ist es jedoch ratsam, sich an dem Wortlaut der DS-GVO zu orientieren.

5. Form

Die DS-GVO sieht keine bestimmte Form für die Erteilung einer Einwilligung vor. Sie kann schriftlich, elektronisch oder mündlich erfolgen. Wichtig ist, dass eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutig bestätigenden Handlung, mit der die betroffene Person ihr sein Einverständnis zur Datenverarbeitung signalisiert, erkennbar ist. Welche Form sich unter der DS-GVO als praktikabel erweisen wird, ist zum heutigen Zeitpunkt noch nicht geklärt. Allerdings – und dies dämpft die Freude über die Lockerung der Formvorschrift erheblich – sollte in jedem Fall berücksichtigt werden, dass Datenverarbeiter zwingend der Nachweispflicht aus Artikel 5 Absatz 2 DS-GVO unterliegen. Danach sind sie verpflichtet, die Einhaltung der Rechtmäßigkeit der Datenverarbeitung nachzuweisen. In der Praxis wird es im Ergebnis daher wohl weiterhin empfehlenswert sein, Einwilligungen in Schriftform oder auf andere bewährte Weisen einzuholen, wie beispielsweise mittels dem Double Opt-in-Verfahren. Nur so kann die Eindeutigkeit der Einwilligung dokumentiert werden.

6. Hinweis auf Widerrufsmöglichkeit

Alt bekannt und keine Überraschung ist das Erfordernis des Hinweises auf die Widerrufsmöglichkeit. Die betroffene Person muss ausdrücklich auf ihr Recht hingewiesen werden, dass sie ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Dieser Hinweis ist ebenso wie die Einwilligungserklärung selbst in einfacher, verständlicher Sprache zu verfassen und leicht zugänglich zu machen. Der Hinweis auf das Widerrufsrecht muss vor Abgabe der Einwilligung erteilt werden.

II. Gelten bisher eingeholte Einwilligungen fort?

Von besonders großer Bedeutung für Unternehmen ist die Frage, ob die bislang nach BDSG und TMG eingeholten Einwilligungen fortgelten. Hierzu bringt Erwägungsgrund 171 Licht ins Dunkel. Danach ist es nicht erforderlich, dass betroffene Personen ihre Einwilligung erneut erteilen, sofern diese ihrer Art nach den Bedingungen der DS-GVO entsprechen. Verstoßen alte Einwilligungen allerdings gegen das Gebot der Freiwilligkeit und insbesondere gegen das

neu verankerte Kopplungsverbot nach Art. 7 Absatz 4 DS-GVO gelten sie nicht fort und müssen erneut eingeholt werden. Es ist daher ratsam, bestehende Einwilligung speziell darauf hin zu prüfen und den Einwilligungsprozess bei Handlungsbedarf kurzfristig anzupassen.

III. Was passiert bei unwirksamen Einwilligungen?

Erweisen sich Einwilligungen nach den oben genannten Kriterien als unwirksam, ist das Vorliegen der Einwilligung nicht durch den Verantwortlichen nachweisbar und liegen auch keine sonstigen gesetzlichen Erlaubnistatbestände vor, ist die Verarbeitung der personenbezogenen Daten unzulässig und kann mit einem Bußgeld belegt werden.

E) Datenschutz und Datensicherheit

Vorbemerkungen

Die EU-Datenschutz-Grundverordnung (DS-GVO) verknüpft Datenschutz und Datensicherheit eng miteinander. Schutz und Technik sind nicht nur bei den technisch-organisatorischen Maßnahmen miteinander verbunden, wie es bisher bei § 9 BDSG und seiner Anlage der Fall war. Die DS-GVO verlangt Datensicherheitsmaßnahmen, die geeignet sind, das Schutzniveau zu gewährleisten, das dem Risiko der Datenverarbeitung für die Rechte und Freiheiten des Betroffenen angemessen ist. Hierbei ist der Stand der Technik angemessen zu berücksichtigen. Es bedarf also einer stetigen Anpassung der Maßnahmen. Zu prüfen ist, ob ein IT-Sicherheitsmanagement notwendig ist.

Welche Schutzziele sind einzuhalten?

(Die Zuordnung erfolgt zur Konkretisierung unter Berücksichtigung der bisher in § 9 BDSG und seiner Anlage vorgenommenen Definitionen)

1. Vertraulichkeit durch

- Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)
- Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle)
- Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle)

- Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungsgebot).

2. Integrität durch

- Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle)
- Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle/Verarbeitungskontrolle)
- Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können (Dokumentationskontrolle)
- Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

3. Verfügbarkeit und Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten) durch

- Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).
- Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO).

Wie ist der Schutzbedarf festzustellen?

Hierfür werden üblicherweise die drei Schutzklassen „normal“, „hoch“ und „sehr hoch“ verwendet. Diese Zuweisung zu den Schutzklassen muss nicht nur für personenbezogene Daten gelten, sondern kann für alle unternehmensrelevanten Informationen verwendet werden.

Die Klassifizierung „normal“ gilt z. B. für alle internen Datenverarbeitungen bzw. für Daten, die aus allgemein zugänglichen Quellen stammen. Das Risiko für den Betroffenen ist tolerabel.

„Hoch“ ist ein Schutzbedarf für Daten, die einen gewissen Vertraulichkeitsgrad erfüllen müssen, weil eine – erhebliche - Beeinträchtigung der Rechte des Betroffenen möglich ist.

Ein „sehr hohes“ Schutzniveau ist zu gewährleisten, wenn eine besonders bedeutende Beeinträchtigung zu befürchten ist.

Die **Risikobewertung** muss also abwägen, wie wahrscheinlich ein Schadenseintritt ist und welchen Schaden er mit welchen Auswirkungen beim Betroffenen anrichten könnte.

Welche Maßnahmen müssen ergriffen werden?

Die technischen und organisatorischen Maßnahmen müssen im Verhältnis zum Risiko stehen. Hierbei sind folgende Punkte zu berücksichtigen:

- Geeignetheit der Maßnahmen
- Stand der Technik
- Kosten der Implementierung
- Aufwand

Nach der DS-GVO gibt es einige Maßnahmen wie:

- Pseudonymisierung
- Verschlüsselung
- Die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherzustellen
- Die Verfügbarkeit und den Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall schnell wiederherzustellen
- Ein Verfahren einzurichten, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technisch-organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gewährleistet
- Sicherstellung, dass die Mitarbeiter, die personenbezogenen Daten verarbeiten, dies nur entsprechend ihrer Aufgabenerfüllung auf Anweisung des Verantwortlichen tun.

Im Rahmen der Rechenschaftspflicht nach Art 5 DS-GVO müssen die Risikobewertung und die daraufhin passend ergriffenen Maßnahmen dokumentiert werden.

Weitere technische Maßnahmen

Bereits im Vorfeld von Anwendungen zur Verarbeitung personenbezogener Daten müssen die Aspekte eines Datenschutzes durch Technikgestaltung (privacy by design) oder durch datenschutzfreundliche Voreinstellungen (privacy by default) berücksichtigt werden. Damit ist dem Grundsatz der Datenminimierung (Art. 5 DS-GVO) zu entsprechen. Schon bei der Beschaffung von IT-Lösungen muss geprüft werden, wie diese Anforderungen umgesetzt

werden können. Anonymisierung, Pseudonymisierung, Einschränkung der Verarbeitung (Sperrung) oder Löschung von Daten können hier Maßnahmen sein.

Auch diese Überlegungen bzw. Maßnahmen sind zu dokumentieren.

F) Bestellung einer/s betrieblichen Datenschutzbeauftragten

I. Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB) nach der DS-GVO

Die **Anwendbarkeit der DS-GVO ab 25. Mai 2018** bringt eine europaweite Verpflichtung zur Bestellung eines bDSB mit sich. Der bDSB ist **zwingend zu bestellen**, wenn die Kerntätigkeit des Verantwortlichen in Verarbeitungsvorgängen besteht, welche aufgrund Art, Umfang und/oder Zweck eine umfangreiche regelmäßige und systematische Beobachtung personenbezogener Daten erforderlich machen. Unter **„Kerntätigkeit“** fallen hierbei Geschäftsbereiche, die für die Umsetzung der Unternehmensstrategie erforderlich sind (insbesondere, aber nicht abschließend: Kundenservice, Marketing, Produktdesign Auskunfteien oder Adresshandel). **“Art, Umfang und Zweck“** ist anhand objektiver Merkmale zu beurteilen (insb. die Anzahl der Betroffenen, die Menge der betroffenen Daten und/oder Vielzahl der verschiedenen Datensätze, die Dauer oder geographische Reichweite der Datenverarbeitung).

Die DS-GVO lässt den Mitgliedstaaten die Befugnis, weitere Bestellpflichten zu regeln, solange der nationale Gesetzgeber nicht von den oben beschriebenen Rechten und Aufgaben abweicht. Hiervon hat der deutsche Gesetzgeber im Rahmen der Änderung des Bundesdatenschutzgesetzes (BDSG) Gebrauch gemacht.

Die Bestellpflicht des bDSB wird abweichend zur DS-GVO erweitert und **behält die Regelungen des bisherigen BDSG weitgehend bei**: das heißt, ein bDSB muss bestellt werden, wenn **mindestens zehn Personen** ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind.

Eine freiwillige Bestellung von Datenschutzbeauftragten ist möglich.

Die Position des bDSB kann innerhalb des Betriebs durch einen eigenen Mitarbeiter besetzt werden (auch als „Teilzeit“-Tätigkeit neben seinen eigentlichen Aufgaben), wenn er die persönlichen und fachlichen Voraussetzungen dafür besitzt. Es kann auch ein externer Datenschutzbeauftragter bestellt werden. Für eine Unternehmensgruppe kann ein gemeinsamer Datenschutzbeauftragte benannt werden. Dieser muss jedoch von jeder Niederlassung aus leicht erreichbar sein.

Im Folgenden werden die Pflicht zur Bestellung eines bDSB, die persönlichen und sachlichen Anforderungen sowie seine Rechte und Pflichten beschrieben.

II. Anforderungen an die Bestellung, Stellung und Aufgaben des bDSB

1. Bestellpflicht

a. Nicht bestellt werden darf eine Person, die in einen Interessenkonflikt geraten könnte oder für die eine Gefahr der Selbstkontrolle besteht (insb. Mitglieder der Unternehmensleitung, IT- und Personalleiter sowie IT- Administratoren).

b. Der bDSB muss aufgrund der beruflichen Qualifikation und des Fachwissens benannt werden, um die Aufgaben aus Art. 39 DS-GVO übernehmen zu können. Zu den Fachkundevoraussetzungen gehört ein Verständnis der allgemein datenschutzrechtlichen und spezialgesetzlichen datenschutzrechtlichen Vorschriften, die für das eigene Unternehmen relevant sind, sowie

c. technisch-organisatorische Kenntnisse, insbesondere Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit. Diese Mindestkenntnisse müssen bereits zum Zeitpunkt der Bestellung zum bDSB vorliegen.

d. Eine Form und bestimmte Dauer für die Bestellung besteht nicht; die Bestellung sollte aus Nachweisgründen in Textform erfolgen (s. unten stehendes Muster).

e. Die Kontaktdaten des dDSB sind zu veröffentlichen (z.B. auf der Unternehmenshomepage) und sind der jeweiligen Landesdatenschutzbehörde zu melden (Hierfür soll es ein elektronisches Formular bei den Aufsichtsbehörden geben).

2. Stellung

a. Der bDSB ist **weisungsunabhängig** bzgl. seiner Aufgabenerfüllung,und er berichtet unmittelbar der höchsten Managementebene des Verantwortlichen.

b. Er darf wegen der Erfüllung seiner Aufgaben **weder abberufen noch benachteiligt** werden.

c. Es besteht ein Anspruch auf ordnungsgemäße und frühzeitige Einbindung in alle datenschutzrechtlichen Fragen. Dem bDSB sind zur Aufgabenerfüllung das notwendige Zeitbudget sowie die nötige Unterstützung (Fortbildung, finanzielle, materielle und personelle Ausstattung) zu gewähren.

d. Dem bDSG ist Zugang zu allen personenbezogenen Daten und damit zusammenhängenden Verarbeitungsvorgängen zu geben.

e. Der bDSB ist zur Wahrung der Geheimhaltung und Vertraulichkeit bei der Erfüllung seiner Aufgaben verpflichtet. Dies gilt insbesondere in Bezug auf die Identität von betroffenen Personen, die sich an den bDSB gewandt haben. Ein gesetzliches Zeugnisverweigerungsrecht steht ihm zu, soweit der Leitung oder einer bestimmten Person des Verantwortlichen ein solches Recht zusteht. Akten oder Schriftstücke des bDSB unterliegen soweit einem Beschlagnahmeverbot.

Nach der geplanten Änderung des BDSG besteht – wie bereits nach der bisherigen Fassung des BDSG – ein **besonderer Kündigungsschutz** für den bDSB. Das Arbeitsverhältnis darf während der Tätigkeit als Datenschutzbeauftragter und nach deren Beendigung für ein Jahr nicht gekündigt werden, es sei denn die Kündigung erfolgt aus wichtigem Grund.

3. Aufgaben

Der bDSB hat schwerpunktmäßig die Einhaltung der datenschutzrechtlichen Vorschriften und den datenschutzkonformen Umgang mit personenbezogenen Daten im Betrieb zu überwachen.

In diesem Zusammenhang hat er gem. Art. 39 DS-GVO die folgenden Aufgaben zu erfüllen:

a. Unterrichtung über die bestehenden datenschutzrechtlichen Pflichten und Beratung bei der Lösung datenschutzrechtlicher Fragen.
b. Überwachung und Einhaltung der datenschutzrechtlichen Vorschriften (DS-GVO, BDSG sowie weitere Rechtsvorschriften) sowie der unternehmenseigenen Datenschutzbestimmungen inkl. Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung von Mitarbeitern.
c. Auf Anfrage Beratung bei der Datenschutz-Folgenabschätzung (Art. 35 Abs. DS-GVO) und Überwachung ihrer Durchführung.
d. Zusammenarbeit mit der Aufsichtsbehörde und Zuständigkeit für die vorherige Konsultation datenschutzrechtlicher Fragen an die Aufsichtsbehörde.
e. Ansprechpartner für betroffene Personen und Mitarbeiter zu allen mit der Verarbeitung ihrer Daten und mit der Wahrnehmung ihrer Rechte zusammenhängenden Vorgänge.

Über diese Mindestaufgaben hinaus nimmt der bDSB eine beratende und unterstützende Funktion ein. Insbesondere sind hier zu nennen: Unterstützung des Verantwortlichen bei der Etablierung von Prozessen bzw. Dokumentationen zur Erfüllung der umfassenden Nachweispflicht, Unterstützung bei der Melde- und Benachrichtigungspflicht bei Datenschutzverletzungen sowie die Erfüllung der Betroffenenrechte (Recht aus Auskunft, Berichtigung, Einschränkung oder Löschen von Daten).

Die Pflicht, ein Verzeichnis der Verarbeitungstätigkeiten zu führen, liegt grundsätzlich beim Verantwortlichen, kann aber - unter der Verantwortung des Verantwortlichen – auf den bDSB übertragen werden.

Bei der Erfüllung seiner Aufgaben hat der bDSB die **Pflicht zur risikoorientierten Tätigkeit**, d. h., er entscheidet selbst, welche Verarbeitungsvorgänge er aufgrund des damit verbundenen Risikos vorranging prüft.

III. Haftung

Nach den Leitlinien der sogenannten Artikel-29-Datenschutzgruppe (unabhängiges Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes) vom Dezember 2016 trägt der bDSB im Falle der Nichteinhaltung der DS-GVO keine persönliche Verantwortung. Aus der DS-GVO gehe klar hervor, dass es Sache des Verantwortlichen sei, sicherzustellen und nachweisen zu können, dass die Verarbeitung im Einklang mit der DS-GVO erfolge.

IV. Folgen bei Nichtbestellung

Die vorsätzliche oder fahrlässige Versäumnis einen betrieblichen Datenschutzbeauftragten nicht oder nicht rechtezeitig zu bestellen, kann nach bisherigem BDSG mit einem **Bußgeld** in Höhe von bis zu 50.000 € belegt werden. Die DS-GVO sieht hier höhere Bußgelder von bis zu **10 Millionen EURO oder 2 % des weltweiten Jahresumsatzes** vor, je nachdem, welcher Betrag höher ist.

G) Fragebogen zur Umsetzung der DS-GVO

Mit Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) zum 25. Mai 2018 wird sich der Datenschutz in Unternehmen verändern. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat einen Fragebogen zum neuen Datenschutz (sog. „DS-GVO-Prüffragebogen“) formuliert. Damit möchte es Unternehmen eine Checkliste an die Hand geben. Wer sich auf die DS-GVO vorbereiten möchte, kann diesen Fragenbogen verwenden und in seinem Betrieb einen Datenschutz-Check durchführen.

(Link: https://www.lda.bayern.de/de/index.html)

Gleichzeitig können sich Unternehmen mit dem Fragebogen auf eine eventuelle Prüfung durch die Datenschutzaufsichtsbehörde vorbereiten. Unternehmen können über diese Datenschutz-Checkliste ermitteln, was bereits umgesetzt worden ist und an welchen Stellen nachgebessert werden sollte. Dazu gehören:

- Struktur und Verantwortlichkeit im Unternehmen: Gibt es eine Datenschutzleitlinie? Wie sind die Verantwortlichkeiten für den Datenschutz geregelt?
- Gibt es im Unternehmen einen Datenschutzbeauftragten?
- Gibt es eine Übersicht über die Verarbeitung personenbezogener Daten in Ihrem Unternehmen?
- Haben Sie Externe zur Verarbeitung (Auftragsverarbeiter) solcher Daten eingebunden und ist dies ordentlich dokumentiert? Sind Vereinbarungen mit Dienstleistern abgeschlossen und dokumentiert?
- Ist die Verarbeitung personenbezogener Daten transparent? Sind die Informationspflichten erfüllt und die Texte an die neuen Vorgaben der DS-GVO angepasst?
- Für den Umgang mit Risiken: Haben Sie die Rechtmäßigkeit Ihrer Verarbeitung niedergelegt und liegen alle erforderlichen Einwilligungen vor?
- Datenschutz-Folgenabschätzung: Haben Sie in Ihrem Unternehmen geklärt, ob eine Datenschutz-Folgenabschätzung notwendig ist? Wenn ja, haben Sie bereits eine Methode dafür festgelegt?
- Ist bei Datenschutzverletzungen in Ihrem Unternehmen sichergestellt, dass die Aufsichtsbehörde innerhalb von 72 Stunden darüber informiert wird?

Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018

I.	Struktur und Verantwortlichkeiten im Unternehmen
1.	Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist, beispielsweise durch • Vorhandensein einer Datenschutzleitlinie • Beschreibung der Datenschutzziele • Regelung der Verantwortlichkeiten • Bewusstsein über Datenschutzrisiken • Transparenz über Zielkonflikte (z.B. zwischen Marketing- und Rechtsabteilung)
2.	Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten? • Wenn nein, warum nicht? • Wenn ja, ist geklärt, wann er von wem einzubeziehen ist? • Wenn ja, ist er schon gem. Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde gemeldet?
II.	Übersicht über Verarbeitungen
1.	Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO? • Wenn nein, warum nicht? Ist das dokumentiert? Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen Berücksichtigung finden (Privacy by Design –Art. 25 DS-GVO)?
III.	Einbindung Externer
1.	Haben Sie Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden? • Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter? • Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?
IV.	Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte
1.	Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst? • Wenn nein, warum nicht?
2.	Haben Sie insbes. folgende Informationen neu aufgenommen, sofern nicht bereits vorher enthalten: • Kontaktdaten des Datenschutzbeauftragten

	• Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten • Falls Sie die Verarbeitung mit ihren berechtigten Interessen oder berechtigten Interessen eines Drittenbegründen: die berechtigten Interessen • Falls Sie Daten in Drittländer übermitteln: die von Ihnen zum Einsatz gebrachten geeigneten Garantien zum Schutz der Daten (z.B. Standarddatenschutzklauseln) • Dauer der Speicherung; sofern nicht möglich, die Kriterien für die Festlegung dieser Dauer • Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen Person sowie auf Datenportabilität • Sofern Verarbeitung auf Einwilligung beruht: das Recht zum jederzeitigen Widerruf der Einwilligung • Recht auf Beschwerde bei der Aufsichtsbehörde • Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist • Sofern einschlägig: die Vornahme einer automatisierten Entscheidungsfindung einschließlich Profiling sowie – in diesem Fall – Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person • Sofern Sie die Daten nicht bei der betroffenen Person erhoben haben: aus welcher Quelle die personenbezogenen Daten stammen und ggf. ob sie aus öffentlich zugänglichen Quellen stammen • Haben Sie Ihre Werbe-Einwilligungserklärungen für Kunden, Interessenten usw., an die Anforderungen von Art. 7 und 13 DS-GVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?
3.	Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DS-GVO zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 DS-GVO)?
4.	Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art. 20 DS-GVO)?
V.	Verantwortlichkeit, Umgang mit Risiken
1.	Gibt es für jede Verarbeitungstätigkeit Angaben, mit der Sie die Rechtmäßigkeit Ihrer Verarbeitung nachweisen können, z. B. bezüglich Zwecken, Kategorien personenbezogener Daten, Empfängern und/oder Löschfristen (Art. 5 Abs. 2 DS-GVO)? • Haben Sie geprüft, ob die Einwilligungen, auf die Sie eine Verarbeitung stützen, noch den Voraussetzungen der Art. 7 und/oder 8 DS-GVO entsprechen? • Können Sie das Vorliegen der Einwilligung nachweisen?

2.	Haben Sie ein Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der DS-GVO erfolgt (Art 24 Abs. 1 DS-GVO)?
3.	Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 DS-GVO angepasst? • Haben Sie insbesondere bestehende Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen durch eine risikoorientierte Betrachtungsweise auf Basis von Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten ersetzt? • Wurde ein geeignetes Managementsystem zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen umgesetzt? • Wurden Schutzmaßnahmen wie Pseudonymisierung und der Einsatz von kryptographischen Verfahren zum Schutz vor unbefugten oder unrechtmäßigen Verarbeitungen sowohl bezüglich externer als auch interner „Angreifer“ umgesetzt?
4.	Haben Sie sich auf die evtl. Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung vorbereitet? • Haben Sie eine geeignete Methode zur Bestimmung der Frage, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, in Ihrem Unternehmen eingeführt? • Haben Sie eine geeignete Risikomethode zur Durchführung einer Datenschutz-Folgenabschätzung in Ihrem Unternehmen eingeführt? Haben Sie sich für einen Prozess der Datenschutz-Folgenabschätzung entschieden; haben Sie diesen schon einmal getestet?
VI.	Datenschutzverletzungen
1.	• Haben Sie gem. Art. 33 DS-GVO sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde möglich ist? • Haben Sie insbesondere sichergestellt, dass Datenschutzverletzungen in Ihrem Unternehmen erkannt werden können. Haben Sie dazu eine geeignete Methode zur Ermittlung eines Risikos bzw. eines hohen Risikos in Ihrem Unternehmen eingeführt? • Haben Sie einen Prozess aufgesetzt, wie mit potentiellen Verletzungen intern umzugehen ist • Haben Sie festgelegt, wer, wann und wie mit der Datenschutzaufsichtsbehörde kommuniziert?
Die Richtigkeit der Angaben wird bestätigt:	

Datum	Unternehmensleitung	ggf. Datenschutzbeauftragter

H) Betroffenenrechte

Vorbemerkungen

Die EU-Datenschutz-Grundverordnung (DS-GVO) stärkt spürbar die Rechte der betroffenen Personen, also derjenigen, deren personenbezogene Daten verarbeitet werden. Die DS-GVO enthält umfangreiche Informationspflichten bei der Datenerhebung, Auskunftsrechte, Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit, Widerspruchsrechte sowie das Recht, nicht einer automatisierten Einzelentscheidung unterworfen zu sein. Der Anspruch richtet sich in der Regel gegen den Verantwortlichen. Er ist verpflichtet, der betroffenen Personen die Ausübung ihrer Rechte (Art. 12 Abs. 2 DS-GVO) zu erleichtern. Das verantwortliche Unternehmen muss auf Anträge des Betroffenen nach den Art. 15 bis 22 innerhalb eines Monats antworten. Zwar gibt es Möglichkeiten der Fristverlängerung, allerdings müssen die Gründe dafür ebenfalls in der Monatsfrist mitgeteilt werden, so dass in jedem Fall schnell reagiert werden muss. Kommt das Unternehmen einem Antrag der betroffenen Person nicht nach, droht ein Bußgeld. Der Verantwortliche im Unternehmen muss also Prozesse implementieren, die eine fristgerechte und korrekte Bearbeitung der Anträge der betroffenen Personen gewährleisten.

Transparenzvorgaben

Art. 12 DS-GVO – Transparente Information, Kommunikation und Modalitäten für die Ausübung der Betroffenenrechte

Bereits zu Beginn der Verarbeitung besteht nach dem Grundsatz der Transparenz eine Pflicht zur umfassenden Information gegenüber der betroffenen Person. Nach Art. 12 hat der Verantwortliche geeignete Maßnahmen zu treffen, um der betroffenen Person alle die Datenverarbeitung betreffenden Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Informationen werden schriftlich oder in anderer Form, insbesondere auch elektronisch, übermittelt; ausnahmsweise auch mündlich, sofern die betroffene Person dies verlangt und die Identität der betroffenen Person nachgewiesen wurde.

Geht ein Antrag (beispielsweise auf Auskunft) einer betroffenen Person bei dem Verantwortlichen ein, kann dieser entweder tätig werden und Maßnahmen ergreifen z. B. eine Auskunft erteilen (Art. 12 Abs. 3) oder davon absehen. Wird der Verantwortliche aber nicht tätig (Art. 12 Abs. 4), hat er neben den Gründen hierfür die betroffene Person auch über die Möglichkeit zu unterrichten, bei einer Aufsichtsbehörde Beschwerde oder bei Gericht einen entsprechenden Rechtsbehelf einzulegen. Wird der Verantwortliche tätig, muss er auf den Antrag der betroffenen Person grundsätzlich unverzüglich reagieren (Art. 12 Abs. 3), in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Allerdings muss dann die betroffene Person innerhalb eines Monats über die Fristverlängerung unter Nennung der Gründe für die Verzögerung unterrichtet

werden (Art. 12 Abs. 3). Die Auskunftserteilung erfolgt unentgeltlich. Bei offenkundig unbegründeten oder - insbesondere im Fall von häufiger Wiederholung - exzessiven Anträgen einer betroffenen Person kann ein angemessenes Entgelt verlangt werden oder eine Weigerung erfolgen, aufgrund des Antrags tätig zu werden; der Verantwortliche hat hierfür aber die Nachweispflicht (Art. 12 Abs. 5).

Art. 13 DS-GVO – Informationspflicht bei Datenerhebung beim Betroffenen

Grundsätzlich können personenbezogene Daten entweder direkt bei der betroffenen Person (Art. 13) oder bei einer dritten (Art. 14) erhoben werden. „Direkterhebung“ meint jede Erhebung personenbezogener Daten mit Kenntnis oder unter Mitwirkung der betroffenen Person. Werden die Daten bei der betroffenen Person erhoben, so muss der Verantwortliche zum **Zeitpunkt der Datenerhebung** (Art. 13 Abs. 1) die betroffene Person umfassend über die Verarbeitung informieren und Folgendes mitzuteilen:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters,
- Kontaktdaten des Datenschutzbeauftragten,
- Zwecke der Verarbeitung und Rechtsgrundlage,
- wenn die Verarbeitung auf Art. 6 Abs. 1 f beruht: berechtigtes Interesse des Verantwortlichen,
- ggf. Empfänger oder Kategorien von Empfängern,
- Absicht der Übermittlung in ein Drittland/internationale Organisation sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission,
- Dauer der Datenspeicherung,
- Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und Recht auf Datenübertragbarkeit,
- Recht auf Widerruf einer Einwilligung (bei Verarbeitung mit Art. 6 Abs. 1 a o. Art. 9 Abs. 2 a),
- Bestehen eines Beschwerderechts gegenüber einer Aufsichtsbehörde,
- Information, ob die Bereitstellung der personenbezogenen Daten gesetzlich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und welche möglichen Folgen die Nichtbereitstellung hätte,
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (Art. 22).

Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiter zu verarbeiten, als zu dem für den die personenbezogenen Daten erhoben wurden, so erfordert dies vorab eine erneute Information des Betroffenen. Über diesen anderen Zweck und alle anderen maßgeblichen Informationen nach Art. 13 Abs. 2 (Prüfung, ob eine solche Zweckänderung im Rahmen von Art. 6 Abs. 4 überhaupt zulässig ist).

Ausnahmen: Nach Art. 13 Abs. 4 entfällt die Information bei Direkterhebung, wenn und soweit die betroffene Person bereits über die Information verfügt. Weitere geringfügige Ausnahmen hierzu enthält auch § 32 des neuen BDSG-neu, welches am 25. Mai 2018 in Kraft tritt. Hier hat

der Gesetzgeber von den Öffnungsklauseln Gebrauch gemacht und weitere Eingrenzungen aufgenommen.

Art. 14 DS-GVO – Informationspflicht, wenn Datenerhebung nicht beim Betroffenen erfolgt

Erfolgt die Datenerhebung nicht beim Betroffenen, sind die Informationspflichten weitgehend parallel zu Art. 13 Abs. 1 und 2 geregelt. Abweichungen sind folgende:

- Es müssen die Kategorien personenbezogener Daten, die verarbeitet werden, genannt werden, zum Beispiel Kundendaten, Mitarbeiterdaten.
- Es muss genannt werden, aus welcher Quelle die personenbezogenen Daten stammen und ggf. ob sie aus öffentlich zugänglichen Quellen stammen.
- Außerdem muss **nicht** über die Pflicht zur Bereitstellung der Daten informiert werden, also ob es sich um eine freiwillige Angabe handelt oder nicht.

Des Weiteren gibt es im Unterschied zu Art. 13 detailliertere Regelungen zum Zeitpunkt der Informationserteilung (Art. 14 Abs. 3) und zu den Ausschlusstatbeständen nach Art. 14 Abs. 5, wenn die Informationspflicht entfällt.

Auch hier sind weitere Ausnahmen in den §§ 29, 33 des BDSG-neu zu finden. Auch zur Videoüberwachung gibt es in § 4 Abs. 2 des BDSG-neu Ausnahmen.

Grundsätzlich sollte das verantwortliche Unternehmen sicherstellen können, dass diese Datenschutzinformationen den oben genannten Anforderungen entsprechen und insbesondere ein Nachweis über die Mitteilung der Informationen geführt werden kann.

Art. 15 DS-GVO – Auskunftsrecht

Das Auskunftsrecht der betroffenen Person über beim Verantwortlichen gespeicherte personenbezogene Daten ist das zentrale Recht, um bei Bedarf gezielt weitere Rechte, z. B. Recht auf Berichtigung, Löschung etc. geltend zu machen. Die betroffene Person kann von dem Verantwortlichen eine **Bestätigung** darüber verlangen, ob dort sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat die betroffene Person bezüglich dieser personenbezogenen Daten ein Recht auf Auskunft über:

- Verarbeitungszwecke,
- Kategorien personenbezogener Daten, die verarbeitet werden,
- Empfänger oder Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden, insbesondere Drittländer,
- soweit möglich über die geplante Speicherdauer, ansonsten Kriterien für die Festlegung der Dauer,

- Informationen über die Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie über ein Widerspruchsrecht gegen die Verarbeitung,
- über das Beschwerderecht bei der Aufsichtsbehörde,
- über die Herkunft der Daten, soweit diese nicht von der betroffenen Person selbst erhoben wurden,
- soweit zutreffend über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling,
- wenn Übermittlung an Drittländer/internationale Organisation, dann Unterrichtung über die geeigneten Garantien gemäß Art. 46

Form der Auskunftserteilung: je nach Sachverhalt schriftlich, elektronisch oder mündlich, möglichst in Form einer Kopie der personenbezogenen Daten (Art. 15 Abs. 3). Der Verantwortliche hat sicherzustellen, dass die Auskunft nur der betroffenen Person oder einer von ihr bevollmächtigten Person erteilt wird und die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden. Als datenschutzfreundlichste Variante wird in Erwägungsgrund Nr. 63 Satz 4 ein Fernzugriff der betroffenen Person auf ihre eigenen Daten über ein sicheres System bezeichnet. Auch hier sieht das BDSG-neu Erleichterungen bzw. Modifizierungen vor (§§ 29, 30, 34).

Art. 16 DS-GVO – Recht auf Berichtigung

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung der sie betreffenden personenbezogenen Daten zu verlangen, wenn sie **unrichtig** sind. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

Art. 17 DS-GVO – Recht auf Löschung, Recht auf Vergessenwerden

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende Daten unverzüglich gelöscht werden, wenn folgende Gründe vorliegen (Art. 17 Abs. 1):

- Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig,
- die betroffene Person widerruft ihre Einwilligung (Art. 6 Abs. 1 a oder Art. 9 Abs. 2 a), und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung,
- die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen, berechtigten Gründe für die weitere Verarbeitung vor,
- die personenbezogenen Daten wurden unrechtmäßig verarbeitet,
- die Löschung der personenbezogenen Daten ist aufgrund eines spezielleren Gesetzes erforderlich, d. h. zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt,

- die personenbezogenen Daten wurden in Bezug auf direkt gegenüber einem Kind angebotene Dienste der Informationsgesellschaft erhoben.

Hier geht es um die Idee des „digitalen Radiergummis“, wobei dies nicht nur für den Online-Bereich gilt. Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er zur Löschung verpflichtet (Art. 17 Abs. 1), muss er nach Art. 17 Abs. 2 unter Berücksichtigung der verfügbaren Technologien und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, treffen, um andere für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihm die Löschung aller Links zu diesen personenbezogene Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat. Ein Verantwortlicher muss also andere Verantwortliche darüber informieren, dass der Betroffenen die Löschung etwa aller Links oder Kopien verlangt.

Ausnahmen (Art. 17 Abs. 3): Es besteht für den Verantwortlichen keine Pflicht zur Löschung, wenn die weitere Speicherung der personenbezogenen Daten aus einem der folgenden Gründe erforderlich ist:

- Ausübung des Rechts auf freie Meinungsäußerung und Information,
- Erfüllung einer rechtlichen Verpflichtung (z. B. gesetzliche Aufbewahrungspflichten), die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten erfordert oder zur Wahrung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die den Verantwortlichen übertragen wurde,
- Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit,
- im öffentliche Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke,
- Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Weitere Ausnahmen etwa für in Papierform gespeicherte Daten sieht § 35 BDSG-neu vor.

Art. 18 DS-GVO – Recht auf Einschränkung der Verarbeitung

Unter „Einschränkung der Verarbeitung“ sind nach den Erwägungsgründen Methoden zur Beschränkung der Verarbeitung personenbezogener Daten zu verstehen, z. B. dass ausgewählte personenbezogene Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, dass sie für Nutzer gesperrt werden oder dass veröffentlichte Daten vorübergehend von einer Webseite entfernt werden. Die betroffene Person hat das Recht, von dem Verantwortlichen diese Einschränkung der Verarbeitung zu verlangen, wenn die nachfolgend aufgezählten Voraussetzungen vorliegen:

- Die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der Daten zu überprüfen,
- die Verarbeitung ist unrechtmäßig und die betroffene Person lehnt die Löschung der Daten ab und verlangt stattdessen eine Einschränkung der Verarbeitung,
- der Verantwortliche benötigt die personenbezogenen Daten nicht länger für die Zwecke der Verarbeitung, die betroffene Person benötigt diese jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen,
- die betroffene Person hat Widerspruch gegen eine auf berechtigte Interessen des Verantwortlichen gestützte Verarbeitung eingelegt, und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Wurde die Verarbeitung auf Antrag des Betroffenen eingeschränkt, so dürfen diese personenbezogenen Daten – mit Ausnahme ihrer Speicherung – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaates verarbeitet werden. Außerdem muss der Verantwortliche die betroffene Person vor Aufhebung der Einschränkung unterrichten (Art. 18 Abs. 3).

Ausnahmen finden sich im BDSG-neu (§ 35).

Art. 20 DS-GVO – Recht auf Datenübertragbarkeit

Eine betroffene Person, die einem Verantwortlichen sie betreffende personenbezogene Daten bereitgestellt hat, hat das Recht, diese Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Darüber hinaus ist die betroffene Person berechtigt, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten ursprünglich bereitgestellt wurden, zu übermitteln. Dies gilt allerdings nur, sofern die Verarbeitung

- auf einer Einwilligung oder einem Vertrag beruht und
- mit Hilfe automatisierter Verfahren erfolgt.

Der Betroffene kann also erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen übermittelt werden, soweit dies technisch möglich ist.

Ausnahmen gelten, wenn die Verarbeitung zur Wahrnehmung einer Aufgabe erfolgt, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Ferner dürfen die Rechte und Freiheiten anderer Personen durch die Ausübung nicht beeinträchtigt werden.

Art. 21 DS-GVO – Recht auf Widerspruch

Die betroffene Person kann einer Verarbeitung durch den Verantwortlichen jederzeit widersprechen, wenn die Verarbeitung auf Art. 6 Abs. 1 e oder f (Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, oder zur Wahrung berechtigter Interessen des Verantwortlichen) erfolgt ist. Dies gilt auch für ein darauf gestütztes Profiling. Eine fortdauernde Verarbeitung durch den Verantwortlichen ist nicht zulässig, außer er kann

- zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder
- die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Im Fall der **Direktwerbung** findet keine Interessenabwägung statt. Ein Widerspruch führt zu einem sofortigen Verarbeitungsstopp. Bei einer Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken führt der Widerspruch ebenfalls zu einem Verarbeitungsstopp, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich (Art. 21 Abs. 6).

Auf sein Widerspruchsrecht muss der Betroffene spätestens zum Zeitpunkt der ersten Kommunikation ausdrücklich sowie in einer verständlichen und von anderen Informationen getrennter Form hingewiesen werden.

§ 36 BDSG-neu schränkt das Widerspruchsrecht gegenüber öffentlichen Stellen ein, bei einem zwingenden öffentlichen Interesse oder einer zur Verarbeitung verpflichtenden Rechtsvorschrift ein.

Art. 22 DS-GVO – Automatisierte Entscheidung im Einzelfall

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dabei hat die betroffene Person insbesondere das Recht auf Eingreifen einer Person aufseiten des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auch auf Anfechtung der Entscheidung. Das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, gilt nicht, wenn die Entscheidung

- für den Abschluss oder die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
- aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Geringfügige Ausnahmen finden sich in § 37 BDSG-neu.

I) Dokumentationspflichten

Vorbemerkungen

Die Datenschutz-Grundverordnung (DS-GVO) betont die Verantwortlichkeit, die Unternehmen (auch „verantwortliche Stellen“ oder „Verantwortliche“ genannt) für die Einhaltung des Datenschutzes haben. Sie müssen nachweisen können, dass ihre Datenverarbeitung datenschutzkonform ist. Umfangreiche Pflichten zur Dokumentation sollen dies sicherstellen. Die Aufzeichnungen dienen als Nachweis gegenüber der Datenschutzaufsicht, bei gerichtlichen Kontrollverfahren sowie für eine nachträgliche Information Betroffener. Eine erfolgreiche Umsetzung dieser Verpflichtung setzt die Entwicklung, Implementierung und Anwendung eines Datenschutz-Managementsystems voraus. Dabei müssen Verantwortliche eruieren, welche Dokumentationspflichten sie zu beachten haben, Umfang und Grenzen dieser Pflichten kennen und Prozesse einführen, die deren Einhaltung sicherstellen.

Die DS-GVO kennt im Wesentlichen folgende Dokumentationspflichten:

Art. 5 Abs. 2, 24 Abs. 1 DS-GVO - Rechenschaftspflicht

Wer personenbezogene Daten verarbeitet, ist verantwortlich für die Einhaltung aller in der DS-GVO aufgeführten Rechtsgrundsätze. Hierbei handelt es sich um folgende: Rechtmäßigkeit der Verarbeitung, Verarbeitung nach Treu und Glauben, Transparenz, Zweckmäßigkeit, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Ein Verantwortlicher muss deren Einhaltung nachweisen können (sog. „Rechenschaftspflicht“). Ferner haben verantwortliche Stellen geeignete technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen und den Nachweis erbringen zu können, dass sie bei ihrer Datenverarbeitung vollumfänglich die DS-GVO beachten. Zudem haben sie ergriffene Maßnahmen zu überprüfen und zu aktualisieren.

In der Praxis setzt man diese Pflicht über die Beschreibung einer Verarbeitung im sog. „Verzeichnis für Verarbeitungstätigkeiten“ um und ergänzt diese idealerweise um die Rechtsgrundlage, auf die die jeweilige Datenverarbeitung gestützt wird.

Art. 6 - Interessenabwägung, Zweckänderung

Wer eine Datenverarbeitung auf die Rechtsgrundlage „Wahrung der berechtigten Interessen des Verantwortlichen oder Dritten“ stützt, muss den hiervon betroffenen Personen die Gründe

mitteilen, die er oder ein Dritter in Abwägung zu den Interessen der Betroffenen als überwiegend ansieht (z. B. Werbung an Kunden per Brief, Fälle des Datenflusses im Konzern, vgl. Erwägungsgründe 47 und 48). Außerdem muss er Betroffene vorab auf ihr jederzeitiges Widerrufsrecht hinweisen.

Ferner haben verantwortliche Stellen Betroffene vorab umfassend (z. B. über die Rechtsgrundlage für die geplante weitere Datenverarbeitung) zu informieren, wenn sie Informationen über diese zu einem anderen Zweck weiterverarbeiten möchten als zu dem ursprünglichen.

Art. 7 - erteilte Einwilligungen

Wird eine Datenverarbeitung auf eine datenschutzrechtliche Einwilligung gestützt, so muss das Unternehmen nachweisen können, dass diese vorliegt, also ein Betroffener diese

- *wirksam erteilt hat*
  - durch eine unmissverständliche Willensbekundung in Form einer Erklärung (Textform z. B. durch E-Mail, Fax, Dokumentenscan ist ausreichend; nicht mehr erforderlich ist die Schriftform, also die Unterschrift im Original. Schriftform wird jedoch durch eine Festlegung im BDSG neu, das am 25.05.2018 in Kraft treten wird, weiterhin erforderlich sein für Einwilligungen im Beschäftigungsverhältnis!)
  - oder durch eine sonstige eindeutige bestätigende Handlung des Einwilligenden wie z. B. einer Einwilligung per Mausklick
- *diese rechtmäßig gestaltet ist*
  - durch eine verständliche und leicht zugängliche Form
  - in einer klaren und einfachen Sprache
  - klar von anderen Sachverhalten zu unterscheiden
  - und ohne Zwang und damit freiwillig abgegeben worden ist, insbesondere – soweit dies angebracht ist – zu verschiedenen Verarbeitungsvorgängen gesondert erteilt werden kann
  - sowie ferner das sog. Koppelungsverbot beachtet ist, d. h. die Erfüllung eines Vertrages wurde nicht von einer Erteilung einer Einwilligung abhängig gemacht, die für deren Erfüllung nicht erforderlich wäre.
- diese für die Zukunft widerruflich gestaltet ist (Hinweis gegenüber Betroffenen!)
- und nicht (zum Teil) unverbindlich ist, weil diese (oder Teile hiervon) gegen die DS-GVO verstoßen.

Die Datenschutzaufsichtsbehörden in Deutschland haben beschlossen, dass bisher rechtswirksame Einwilligungen weiterhin wirksam sind (Beschluss des „Düsseldorfer Kreises“

vom 13./14.09.2016).1 Jedoch müssen Verantwortliche deren Einholung nachweisen können. Dies setzt eine entsprechende Dokumentation voraus (Einwilligungs-Management).

(Näheres zur Einwilligung s. Newsletter Nr. 4)

Art. 8 - Einwilligung bei Kindern – Pflicht zur Altersverifikation

Hat ein Kind das sechzehnte Lebensjahr vollendet, so kann es in Dienste der Informationsgesellschaft (z. B. Online-Informationsangebote, Online-Handel von Waren und Dienstleistungen, Online-Werbung) datenschutzrechtlich wirksam einwilligen. Allerdings muss die Einwilligung rechtskonform (s. o.) gestaltet sein. Kinder unter sechzehn benötigen die Einwilligung der Erziehungsberechtigten oder deren Zustimmung, um wirksam einwilligen zu können. Insoweit ist ein Verantwortlicher verpflichtet, umfassend (auch unter Einsatz technischer Mittel) zu prüfen, ob die Einwilligung eines Erziehungsberechtigten vorliegt. Es besteht nach der DS-GVO die Möglichkeit, dass andere EU-Mitgliedstaaten das Alter auf 13 Jahren festsetzen.

Art. 12 ff. – Betroffenenrechte (Näheres zu den Betroffenenrechten s. Newsletter Nr. 8)

Verantwortliche Stellen müssen die Rechte Betroffener kennen und Prozesse implementieren, um hierauf entsprechend reagieren zu können. So müssen z. B. Geschäftsprozesse geprüft und die Sachverhalte erfasst werden, an die Informationspflichten (z. B. bei einer Einwilligung oder bei einer Datenerhebung über Dritte) geknüpft sind. Ferner sollten Umfang und Grenzen von Betroffenenrechten und die Fristen bekannt sein, in denen verantwortliche Stellen Betroffenenrechte erfüllen müssen und deren Einhaltung sichergestellt sein.

Art. 13, 14 - Erfüllung der Informationspflichten

Verantwortliche Stellen haben nachzuweisen, dass sie die erweiterten Informationspflichten nach der DS-GVO erfüllen. Es empfiehlt sich insoweit, diese Informationen zum Datenschutz (auch Vorversionen mit dem Hinweis „verwendet von… bis…“) aufzubewahren sowie den Zeitpunkt der Übermittlung zu dokumentieren. Ein Verstoß gegen Informationspflichten führt in der Regel nicht dazu, dass die Datenverarbeitung unzulässig wird. Allerdings sind die Verstöße bußgeldbewährt.

Art. 15 - Erfüllung der Auskunftsersuchen

Jede Person, deren Daten verarbeitet werden, hat das Recht, unentgeltlich binnen eines Monats (Fristverlängerung um max. zwei Monate möglich) von der verantwortlichen Stelle Auskunft darüber zu erhalten, welche Daten über sie verarbeitet werden. Wichtig hierbei ist, dass ein Auskunftsanspruch nicht uneingeschränkt besteht. Würde eine Auskunft z. B. Rechte Dritter, ein Geschäftsgeheimnis oder ein Urheberrecht beeinträchtigen, so ist ein Verantwortlicher nicht verpflichtet, die Auskunft insoweit zu erteilen. Generell empfiehlt es sich,

[1] Jetziger Stand. Die Datenschutzkonferenz diskutiert dies aktuell. Sollten sich insoweit Änderungen ergeben, werden wir Sie hierüber informieren.

Umfang und Grenzen von Auskunftsansprüchen zu kennen und intern entsprechende Festlegungen (z. B. wer darf Auskunftsansprüche bearbeiten, Mitarbeiter schulen und festlegen, was als Geschäftsgeheimnis anzusehen ist) zu treffen.

Denn jede Person kann von einer datenverarbeitenden Stelle, wenn diese die Identität eines Antragstellers geprüft hat, in den Varianten „schriftlich“, „Kopie der Daten“ bzw. „elektronisch bei elektronischer Antragstellung“ folgende Auskünfte über sich verlangen:

- ob Daten zu seiner Person verarbeitet werden
- die Verarbeitungszwecke und Datenkategorien
- Empfänger(-kategorien)
- Information über das Beschwerderecht bei der Datenschutzaufsichtsbehörde
- Herkunft der Daten, soweit diese nicht beim Betroffenen selbst, sondern bei Dritten erhoben worden sind
- bei automatisierten Entscheidungen/Profiling: Über die implementierte Logik und die Tragweite/Auswirkungen dieser Verarbeitung für/auf den Betroffenen
- Unterrichtung über geeignete Garantien bei Drittlandtransfers (z. B. Standardvertragsklauseln, gesichertes Drittland)

Art. 16 - Erfüllung des Rechts auf Berichtigung

Verantwortliche haben unrichtige Angaben über eine Person auf deren Verlangen unverzüglich zu berichtigen und unvollständige Angaben zu ergänzen.

Art. 17 - Erfüllung des Rechts auf Löschung

Sind Angaben über eine Person für eine Verarbeitung nicht mehr notwendig, so hat der Verantwortliche diese unverzüglich zu löschen. Dies gilt auch, wenn ein Betroffener aus diesem Grund die Löschung seiner Daten fordert. Betroffene können verlangen, dass Verantwortliche ihnen bestätigen, dass diese die Daten antragsgemäß gelöscht haben. Sie sind jedoch nicht verpflichtet zu dokumentieren, welche Daten wann gelöscht worden sind. Allerdings sollten sie ein Löschkonzept (Dokumentation) haben und darin festlegen, wie lange bestimmte Daten aufgrund gesetzlicher bzw. unternehmensinterner Vorgabe aufbewahrt werden müssen.

Wer Angaben über eine Person (im Internet) veröffentlicht, sollte festhalten, an wen er welche Daten zur Veröffentlichung weitergegeben hat. Denn verantwortliche Stellen müssen angemessene Maßnahmen ergreifen, um zu gewährleisten, dass sie diejenigen, an die sie die Daten über eine Person weitergeben haben, darüber informieren können, dass diese Person eine Löschung aller Links, Kopien oder Replikationen verlangt. Um diesen Anspruch erfüllen zu können, haben sie unter Berücksichtigung angemessener Implementierungskosten eine entsprechende Technologie einzusetzen.

Art. 18 - Erfüllung des Rechts auf Einschränkung der Verarbeitung

Betroffene haben das Recht, hinsichtlich ihrer Daten eine eingeschränkte Verarbeitung zu verlangen, falls

- Betroffene deren Richtigkeit bestreiten oder
- die Daten ohne Rechtsgrundlage verarbeitet werden und ein Verantwortlicher eine Löschung ablehnt oder
- die Daten zwar nicht mehr für den ursprünglichen Verarbeitungszweck, jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden oder
- bei einem Widerspruch des Betroffenen gegen eine Datenverarbeitung, der gestützt wird entweder auf ein überwiegendes öffentliches bzw. berechtigtes (z. B. bei Profiling) Interesse oder auf die Ausübung öffentlicher Gewalt, die einer verantwortlichen Stelle übertragen worden ist. Eine Einschränkung der Verarbeitung bleibt bestehen, bis nachgeprüft ist und feststeht, ob ein Verantwortlicher die Daten rechtmäßig verarbeitet, weil er berechtigte Gründe hierfür geltend machen kann und diese diejenigen überwiegen, die der Betroffenen vorträgt.

Eine Einschränkung der Verarbeitung hat zur Folge, dass Verantwortliche derartige Daten zwar speichern, jedoch nur noch sehr eingeschränkt weiterhin verwenden dürfen, d. h. entweder nur mit der Einwilligung der Betroffenen oder zur Durchsetzung von Rechtsansprüchen oder bei Vorliegen eines wichtigen Interesses der Union oder eines Mitgliedstaates.

Verlangt ein Betroffener dies, so hat ein Verantwortlicher ihn auch darüber zu informieren, dass er eine Einschränkung einer Verarbeitung aufhebt. Auch dies sollte dokumentiert werden.

Art. 19 - Mitteilungspflicht an Dritte

Betroffene können verlangen, dass Verantwortliche allen, denen gegenüber sie Daten über diese Person (z. B. im Internet) offengelegt haben, jede Berichtigung, Löschung oder Einschränkung dieser personenbezogenen Daten mitteilen. Möchte ein Betroffener dies wissen, so hat der Verantwortliche ihm zudem die Empfänger der Daten zu nennen. Eine Mitteilungspflicht entfällt, falls sich dies als unmöglich oder als mit einem unverhältnismäßigen Aufwand verbunden erweist (Rat: Gründe hierfür festhalten). Um dieses Betroffenenrecht erfüllen zu können, ist eine Dokumentation derartiger Empfänger unerlässlich.

Art. 20 - Erfüllung des Rechts auf Datenübertragung (Datenportabilität)

Die DS-GVO führt neu das Recht auf Datenübertragbarkeit ein.

Dieses Recht gilt allerdings nicht uneingeschränkt. Vielmehr umfasst es nur diejenigen personenbezogenen Daten, die eine Person einem Verantwortlichen bereitgestellt hat

- im Zusammenhang mit der Abgabe einer Einwilligung oder dem Abschluss eines Vertrags **und**
- sofern die Datenverarbeitung automatisiert, d. h. IT-gestützt, erfolgt ist **und**

- soweit Rechte Dritter hierdurch nicht beeinträchtigt werden.

Verantwortliche sollten Umfang und Grenzen dieses Rechts kennen. Dieses bezieht sich ausschließlich auf sog. „bereit gestellte“ und damit auf solche Daten, die vom Betroffenen selbst stammen. Diese sind ihm auf Verlangen in einem strukturierten, gängigen und maschinenlesbarem Format zu übermitteln. Besteht dieses Recht, kann ein Betroffener fordern, dass ein Verantwortlicher seine Daten direkt an einen anderen Verantwortlichen übermittelt, soweit dies technisch machbar ist. „Soweit technisch machbar“ bedeutet, dass Verantwortliche bereits über entsprechende Einrichtungen verfügen, diese aber nicht neu implementieren müssen, um ein Recht auf Datenportabilität erfüllen zu können.

Um diesem Betroffenenrecht nachkommen zu können, sollten Verantwortliche ermitteln, welche Datensätze von diesem Recht betroffen sein könnten.

Art. 7 Abs. 3, Art. 13 Abs. 2, Art. 14 Abs. 2d – Widerruf einer Einwilligung

Ein Betroffener kann eine Einwilligung jederzeit widerrufen. Der Widerruf sollte hierbei so einfach wie die Einwilligung sein. Wichtig ist, dass Verantwortliche durch entsprechende Dokumentation (z. B. durch eine schriftlich abgegebene Einwilligung) nachweisen können, dass sie Betroffene bei der Erhebung der Einwilligung darüber informiert haben, dass sie die Einwilligung jederzeit widerrufen können.

Art. 21 - Ausübung des Widerspruchsrechts

Betroffene können jederzeit einer Verarbeitung ihrer Daten widersprechen, die Verantwortliche auf die Rechtsgrundlagen „überwiegende öffentliche Interessen“, „berechtigte Interessen“ oder auf die „Ausübung öffentlicher Gewalt, die einem Verantwortlichen übertragen worden ist“, stützen und zwar auch dann, soweit ein Profiling hierauf gestützt wird. Der Rechtsanspruch besteht nicht, falls Verantwortliche zwingende schutzwürdige Gründe nachweisen können, die die Interessen des Betroffenen überwiegen, oder die Daten für die Durchsetzung von Rechtsansprüchen noch benötigt werden. Die Gründe für die Ablehnung eines Widerspruchsrechts sollten Verantwortliche festhalten, um diese bei Bedarf nachweisen zu können.

Einer Direktwerbung mit seinen Daten (einschließlich einem hierauf gestützten Profiling) kann ein Betroffener ebenfalls jederzeit widersprechen. Ein Widerspruch bewirkt, dass seine Daten nicht mehr verwendet werden dürfen, um ihn mittels Werbung direkt anzusprechen.

Verantwortliche sollten diejenigen Sachverhalte ermitteln, in denen Betroffenen ein derartiges Widerrufsrecht zusteht. Ferner sollten sie nachweisen können, dass sie Betroffene – und dies spätestens bei der ersten Kommunikation – auf ein Widerspruchsrecht hingewiesen haben. Dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

Art. 24 technisch-organisatorische Maßnahmen

Verantwortliche sind verpflichtet, geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten einzusetzen, um sicherzustellen und nachweisen zu können, dass sie die Vorgaben der DS-GVO einhalten. Bei der Festlegung von Maßnahmen sind Art, Umfang, Umstände, die Verarbeitungszwecke ebenso wie unterschiedliche Eintrittswahrscheinlichkeiten und die Schwere der Risiken zu berücksichtigen. Der Nachweis erfolgt über eine entsprechende Beschreibung dieser Maßnahmen z. B. in einem Vertrag über Auftragsverarbeitung und/oder im sog. Verzeichnis für Verarbeitungstätigkeiten. Können Verantwortliche im Zusammenhang mit der Verarbeitung auf genehmigte Verhaltensregeln oder auf genehmigte Zertifizierungen zurückgreifen, so können diese herangezogen werden, um die Umsetzung dieser Verpflichtung nachzuweisen. Dieser Punkt sollte bei einer Dokumentation berücksichtigt werden.

Vertragsmanagement

Verantwortliche sollten über ein Vertragsmanagement ihre Verträge verwalten. Dies ermöglicht eine Übersicht über beauftragte Dienstleister. Datenschutzbeauftragte sollten prüfen und festhalten, welche Verträge datenschutzrelevant sind, um welche Art von Datenschutzverträgen (z. B. Joint Controllership oder Vertrag über Auftragsverarbeitung) es sich hierbei handelt sowie ob und in welchen Punkten diese Verträge an die DS-GVO angepasst werden müssen.

Art. 26 – Gemeinsame Verantwortliche (Joint Controllership)

Bei einem sog. Joint Controllership sind mehrere verantwortliche Stellen gemeinsam für eine Verarbeitung personenbezogener Daten verantwortlich, weil sie Mittel und Zwecke der Verarbeitung gemeinsam (nicht notwendigerweise in gleichem Umfang!) festlegen können. Die DS-GVO schreibt vor, dass gemeinsame Verantwortliche in einer Vereinbarung

- festlegen müssen, wer bezogen auf die Wahrnehmung von Rechten Betroffener welche Pflichten (z. B. Informationspflicht) übernimmt, soweit Unionsrecht oder nationales Recht dies nicht festlegen
- eine Anlaufstelle für Betroffene angeben können und
- ferner wesentliche Punkte der Vereinbarung (z. B. die tatsächlichen Funktionen und Beziehungen der gemeinsamen Verantwortlichen) den Betroffenen zur Verfügung zu stellen haben.

Diese Festlegungen wirken jedoch verbindlich nur im Innenverhältnis zwischen den gemeinsam Verantwortlichen, so z. B. wenn nachgewiesen werden muss, dass ein gemeinsamer Verantwortlicher seine vertraglich übernommenen Pflichten auch tatsächlich erfüllt hat. Unabhängig von getroffenen Vereinbarungen haben Betroffene das Recht, ihre Rechte gegenüber jedem einzelnen der Verantwortlichen geltend zu machen. Gemeinsam

Verantwortliche sollten eine Haftungsklausel in den Vertrag aufnehmen und hierin festlegen, wer im Innenverhältnis für welche Datenvorfälle haftet. Betroffene können frei wählen, welcher der gemeinsam Verantwortlichen ihnen gegenüber haften soll.

Art. 28 – Vereinbarung über eine Auftragsverarbeitung (ADV)

Eine Vereinbarung über eine Auftragsverarbeitung ist abzuschließen, wenn eine verantwortliche Stelle einen Dienstleister (sog. „Auftragsverarbeiter“) beauftragt, personenbezogene Daten ausschließlich nach ihrer Weisung und nur zum Zwecke der Vertragserfüllung zu verarbeiten. Verantwortliche sollten hierbei in der Lage sein, gegenüber einer Datenschutzaufsichtsbehörde Folgendes darlegen zu können:

- dass der Auftragsverarbeiter die Anforderungen der DS-GVO erfüllen kann und er insoweit hinreichende Garantien bietet, insbesondere die Sicherheit der Datenverarbeitung über geeignete technische und organisatorische Maßnahmen und angemessene Schutzmaßnahmen gewährleisten kann,
- dass eine Beauftragung von Unterauftragnehmern ausschließlich mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Verantwortlichen erfolgt, und
- dass die ADV den gesetzlich vorgeschriebenen Mindestinhalt enthält.

Art. 5 Abs. 1f, Art. 29, Art. 32 Abs. 4 – Beschäftigte als Weisungsempfänger, Verpflichtung zur Vertraulichkeit

Die DS-GVO regelt, dass Beschäftigte personenbezogene Daten nur auf Anweisung des Verantwortlichen verarbeiten dürfen. Diese sind verpflichtet, ihre Mitarbeiter entsprechend anzuhalten. Insoweit sollten Verantwortliche notwendige interne Datenschutzregelungen (Betriebsvereinbarungen, Dienstanweisungen) erstellen und die Mitarbeiter in diesen Fragen entsprechend informieren und schulen. Interne Datenschutzregelungen sowie sonstige Anweisungen zum Datenschutz sollten dokumentiert und regelmäßig auf Änderungsbedarf geprüft werden.

Private Arbeitgeber sind nach der DS-GVO nicht mehr ausdrücklich verpflichtet, ihre Mitarbeiter auf das Datengeheimnis zu verpflichten. Jedoch haben Verantwortliche aufgrund ihrer Organisationspflicht Beschäftigte zur Vertraulichkeit anzuweisen (idealerweise über eine Verpflichtung zur Vertraulichkeit und ggf. zur Wahrung sonstiger Berufsgeheimnisse. (Ferner sollten Mitarbeiter stets auf die Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse verpflichtet werden).

Auftragsverarbeiter haben zu gewährleisten und nachzuweisen, dass sie ihre Mitarbeiter zur Vertraulichkeit verpflichtet haben.

Beschäftigte sollten ferner Kenntnis davon haben, dass sie für eine unbefugte Verarbeitung personenbezogener Daten einstehen müssen. Je nach Sachverhalt kann diese u. U. als Ordnungswidrigkeit oder als Straftat verfolgt werden, arbeitsrechtliche Folgen (Abmahnung, Kündigung) haben und eine Haftung sowohl der Betroffenen als auch dem Arbeitgeber gegenüber bewirken.

Art. 30 – Verzeichnis von Verarbeitungstätigkeiten

Die DS-GVO verpflichtet Verantwortliche, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Dieses enthält für jede Anwendung die wesentlichen Informationen. Die Datenschutzaufsichtsbehörden werden entsprechende Mustervorlagen veröffentlichen. Neu führt die DS-GVO die Pflicht ein, dass auch Auftragsverarbeiter ein Verzeichnis zu allen Kategorien von Tätigkeiten führen müssen, die sie im Auftrag eines Verantwortlichen verarbeiten.

Art. 32 – Sicherheit der Verarbeitung

Verantwortliche und Auftragsverarbeiter sind verpflichtet zu eruieren, welche Risiken eine Verarbeitung personenbezogener Daten für Betroffene hat (Risikoanalyse). Hierauf gestützt haben sie über geeignete technische und organisatorische Maßnahmen ein angemessenes technisches Schutzniveau für personenbezogene Daten zu gewährleisten. Der hiermit verbundene Dokumentations- und Überarbeitungsaufwand kann vielfach reduziert werden durch eine zweigeteilte Dokumentation, d. h. eine „Standard“-Variante, die für alle oder bestimmte Gruppen gilt, und eine ergänzende Dokumentation verfahrensspezifischer Maßnahmen. Die Dokumentation sollte umfassen, dass zum einen bei der Festlegung der Schutzmaßnahmen der Stand der Technik, Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung sowie zum anderen die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere des Risikos für von der Datenverarbeitung Betroffene berücksichtigt worden sind.

Angemessene Sicherheit personenbezogener Daten ist hierbei zu gewährleisten vor

- unbefugter oder unrechtmäßiger Verarbeitung und
- vor unbeabsichtigtem Verlust/Zerstörung/Schädigung.

Dementsprechend sollten die Maßnahmen und ihre Dokumentation Folgendes umfassen:

ob eine Anwendung eine Pseudonymisierung und/oder Verschlüsselung personenbezogener Daten ermöglicht,

- die Fähigkeit einer Anwendung und die ergriffenen Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastung der Systeme und Dienste sicherzustellen,
- die Fähigkeit einer Anwendung und die ergriffenen Maßnahmen, um die Verfügbarkeit und den Zugang zu den Daten nach einem Zwischenfall wiederherzustellen,

- ein Verfahren, um regelmäßig überprüfen, bewerten und evaluieren zu können, ob getroffene Schutzmaßnahmen noch wirksam sind (Prüfroutinen).

Datenpannen und Meldepflichten

Verantwortliche sollten Vorkehrungen (Notfall-Management) treffen, um auf Datenpannen sachgemäß reagieren zu können. Sie müssen insoweit bestehende Melde- und Informationspflichten kennen. Ferner sollten sie einen Prozess etablieren und so sicherstellen, dass Mitarbeiter Datenpannen erkennen und über entsprechende Vorfälle den Datenschutzbeauftragten und/oder die Geschäftsleitung informieren, so dass geprüft werden kann, ob eine Meldepflicht besteht und weitere Schritte veranlasst werden können. Festgelegt werden muss auch, wer in einer verantwortlichen Stelle zu dem Team gehört, das intern Datenpannen prüft und bearbeitet.

Art. 33 - Meldung von Datenverletzungen

Ein Verantwortlicher hat jede Datenverletzung binnen 72 Stunden der zuständigen Datenschutzaufsichtsbehörde zu melden. Die Datenschutzaufsichtsbehörden werden für die Meldung von Datenpannen ein Online-Tool bereitstellen, das Verantwortliche in derartigen Fällen verwenden müssen.

Eine Meldepflicht entfällt, wenn die Datenverletzung voraussichtlich nicht zu einem Risiko für Betroffene führt (z. B. weil die Daten auf dem als verloren gemeldeten iPad sicher nach dem Stand der Technik verschlüsselt sind).

Die DS-GVO verpflichtet Verantwortliche, jede Datenverletzung zu dokumentieren und hierbei alle Fakten, Auswirkungen und ergriffene Abhilfemaßnahmen festzuhalten.

Stellt ein Auftragsverarbeiter eine Datenpanne fest, so hat er diese unverzüglich dem Verantwortlichen zu melden

Art. 34 - Meldung von Datenverletzungen an Betroffenen

Der Verantwortliche hat Betroffene unverzüglich in klarer und einfacher Sprache zu benachrichtigen, falls eine Datenpanne ein hohes Risiko für diese zur Folge hätte und dieses hohe Risiko nicht durch geeignete technische und organisatorische Maßnahmen aller Wahrscheinlichkeit nach ausgeschlossen werden kann. Eine Benachrichtigung Betroffener entfällt, falls diese mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesen Fällen hat ein Verantwortlicher (anstelle einer individuellen Benachrichtigung) Betroffene über eine öffentliche Bekanntmachung der Datenpanne oder eine vergleichbar wirksame Maßnahme zu informieren.

Art. 35 - Datenschutz-Folgenabschätzung

Für jede Verarbeitung personenbezogener Daten ist zu ermitteln, welches Risiko für die Rechte Betroffener damit verbunden ist (Risikobewertung). Dies ist zu dokumentieren. Stellt ein Verantwortlicher fest, dass die beabsichtigte Datenverarbeitung ein hohes Risiko für die Person

zur Folge hätte, deren Daten verarbeitet werden sollen, und kann dieses hohe Risiko nicht minimiert werden, so hat ein Verantwortlicher eine sog. „Datenschutz-Folgen-abschätzung“ durchzuführen. Kann das als Ergebnis festgestellte hohe Risiko nicht durch technische und/oder organisatorische Maßnahmen zum Schutz der Daten minimiert werden, ist dies zu dokumentieren und die Aufsicht vorab, d. h. vor einem Einsatz, zu konsultieren. Dies hat ferner zu erfolgen bei all den Verarbeitungen, die Datenschutzaufsichtsbehörden als hoch risikoreich einstufen und deshalb in einer sog. „Blacklist“ veröffentlichen, die die Datenschutzaufsichtsbehörden demnächst veröffentlichen werden.

Art. 36 - vorherige Konsultation der Aufsicht

Diese ist immer dann erforderlich, wenn eine Datenschutz-Folgenabschätzung zu dem Ergebnis kommt, dass die Datenverarbeitung ein hohes Risiko für Betroffene bedeuten würde. Bei einer Vorabkonsultation hat ein Verantwortlicher der Aufsicht alle gesetzlich vorgeschriebenen Informationen zur Verfügung zu stellen.

Art. 37 - Benennung eines betrieblichen/behördlichen Datenschutzbeauftragten

Sowohl im Falle einer Bestellpflicht als auch bei einer freiwilligen Bestellung eines Datenschutzbeauftragten sollte diese aus Nachweisgründen schriftlich erfolgen. Eine verantwortliche Stelle sollte in der Bestellurkunde festhalten, welche Aufgaben, die ihr nach der DS-GVO obliegen, sie auf den Datenschutzbeauftragten überträgt (wie z. B. die Führung eines Verzeichnisses für Verarbeitungstätigkeiten). Eine derartige Aufgabenübertragung stellt eine Zuständigkeitszuweisung im Innenverhältnis dar. Im Außenverhältnis verbleibt die Verantwortung hierfür bei der verantwortlichen Stelle.

Art. 40 - Verhaltensregeln

Von dem Europäischen Datenschutzausschuss (europaweite Geltung) oder der zuständigen Datenschutzaufsicht (Geltung innerhalb eines Mitgliedstaates) genehmigte Verhaltensregeln können als Nachweis für die Einhaltung von Pflichten nach der DS-GVO (z. B. im Rahmen von Auftragsverarbeitungen oder als Nachweis für die Gewährleistung der Sicherheit einer Verarbeitung) herangezogen werden. Eine entsprechende Dokumentation ist insoweit unerlässlich.

Art. 42 - Zertifizierung

Von einer Datenschutzaufsicht genehmigte Zertifizierungen können ebenfalls als Nachweis für die Einhaltung von Pflichten nach der DS-GVO herangezogen werden. Auch dies ist entsprechend zu dokumentieren.

Art. 47 - verbindliche interne Datenschutzvorschriften

Von der zuständigen Datenschutzaufsichtsbehörde genehmigte sog. „verbindliche interne Datenschutzvorschriften“ stellen für eine konzerninterne Datenübermittlung in Drittländer eine

Rechtsgrundlage dar. Ihr Vorliegen ist auf Verlangen nachzuweisen. Damit verbunden ist eine entsprechende Informationspflicht gegenüber Betroffenen.

Art. 49 Abs. 6 – Ausnahmen für bestimmte Fälle / Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

Im Verzeichnis für Verarbeitungstätigkeiten hat ein Verantwortlicher die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien zu erfassen, die ausnahmsweise eine Datenübermittlung in ein Drittland gemäß Art. 49 Abs. 1 Satz 2 DS-GVO rechtfertigen.

Publikation

Bitkom e. V., Leitfäden zu Verzeichnis für Verarbeitungstätigkeiten, Risk Assessment & Datenschutz-Folgenabschätzung, Joint Controllership in der EU-Datenschutz-Grundverordnung, Anlage Auftragsverarbeitung und Begleitende Hinweise, Link: https://www.bitkom.org/Bitkom/Publikationen/index.jsp

J) Privacy by design / Privacy by default - Standardmäßiger Datenschutz für mehr Privatsphäre

Vorbemerkungen

In Zeiten der Digitalisierung steigt die Menge erfasster Daten sowie datenverarbeitender Anwendungen stetig. Dies führt wiederum dazu, dass die Wahrung eines angemessenen Persönlichkeitsschutzes maßgeblich von der jeweiligen Technikgestaltung abhängt. Im Hinblick auf die Gestaltung von Systemen, angefangen von der Produktentwicklung bis hin zu ihrer Implementierung, wurden daher bereits in der Vergangenheit zunehmend die Ansätze Datenschutz durch Technik („privacy by design“) und datenschutzfreundliche Voreinstellungen („privacy by default“) thematisiert.

Was sagt die DS-GVO?

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) im Mai 2016 haben diese Gestaltungsprinzipien nun auch ihren gesetzlichen Niederschlag gefunden (vgl. Art. 24, 25 DS-GVO). Die Berücksichtigung von „privacy by design“ und „privacy by default“ ist damit kein Nice-to-have mehr. Vielmehr handelt es sich um eine explizite Anforderung an die Entwicklung und Implementierung von Produkten zur Verarbeitung personenbezogener Daten, mit dem Ziel, das Prinzip der Datenvermeidung und Datensparsamkeit in Verarbeitungssystemen wirksam umzusetzen. Oder anders gesagt: Damit der Datenschutz nicht von der technischen Entwicklung abgehängt wird, sind Produkte/ Systeme frühzeitig um angemessene Datenschutzfunktionen zu ergänzen, so dass das Risiko datenschutzkritischer Entwicklungen, welche unmittelbar aus der Nutzung technischer Systeme resultieren, von vornherein verringert wird (z. B. durch frühzeitige Pseudonymisierung der Daten).

Empfehlungen, inwiefern, d. h. mit welchen Strategien Datenschutz im Wege von „privacy by design“ in Produkten und Systemen verankert werden kann, hat die Europäische Agentur für Netz- und Informationssicherheit (ENISA) im Hinblick auf die DS-GVO bereits in einem Bericht vom Dezember 2014 veröffentlicht. Die Umsetzungsmöglichkeiten spiegeln sich dabei in den folgenden acht Strategien wider:

1. *MINIMISE: Bei diesem Punkt geht es um die Forderung nach Datensparsamkeit. Es sollen also keine oder zumindest keine unnötigen personenbezogenen Daten gesammelt und ihre Verarbeitung auf ein Minimum beschränkt werden. Wichtig ist daher also immer die Beantwortung der Frage, ob die Verarbeitung personenbezogener Daten zur Erreichung des jeweiligen Zwecks erforderlich ist oder ob dieser nicht auch auf anderem Weg erreicht werden kann.*
2. *HIDE: Der Grundgedanke dieser Strategie ist es, einem Missbrauch personenbezogener Daten in der Form entgegen zu wirken, dass diese schlicht nicht mehr zur Kenntnis genommen werden können. Ziel ist dabei die Schaffung von Unverfolgbarkeit, Unbeobachtbarkeit sowie Unverknüpfbarkeit. An dieser Stelle spielen also beispielsweise die Pseudonymisierung und Anonymisierung personenbezogener Daten eine entscheidende Rolle.*
3. *SEPARATE: Diese Empfehlung bezieht sich auf eine verteilte Datenhaltung, sprich Daten zu einer Person sollen möglichst an verschiedenen Orten gespeichert und verarbeitet werden. So kann die Erstellung umfassender Profile verhindert werden.*
4. *AGGREGATE: An dieser Stelle geht es darum, dass personenbezogene Daten so früh wie möglich zu Gruppen zusammengefasst werden sollten. Die Rückschlussmöglichkeiten auf einzelne Personen können so minimiert bzw. gänzlich ausgeschlossen werden.*
5. *INFORM: Dieser Punkt spiegelt den datenschutzrechtlichen Grundsatz der „Transparenz“ wider. Wenn Personen ein System verwenden, so sollen sie darüber informiert werden, welche Daten über sie gesammelt werden, zu welchem Zweck und mit welchen Technologien. Auch sind sie darüber zu informieren, wie die Daten geschützt werden und ob eine Datenweitergabe an Dritte erfolgt. Ferner ist von Bedeutung, dass sie über ihre Datenzugriffsrechte informiert werden und wie sie diese ausüben können.*
6. *CONTROL: Hier geht es um den Aspekt, dass Personen die Kontrolle über diejenigen Daten behalten sollen, welche über sie gesammelt werden. Faktoren wie z. B. die Bearbeitung von Datenschutzeinstellungen über Benutzeroberflächen sowie eine insgesamt benutzerzentrierte Gestaltung spielen dabei eine maßgebliche Rolle.*
7. *ENFORCE: Es sollte eine den rechtlichen Anforderungen entsprechende Datenschutzrichtlinie, sprich ein Regelwerk zum Schutz der Privatsphäre der betroffenen Personen vorhanden sein, die auch faktisch umgesetzt wird. Dies impliziert zumindest, dass geeignete technische Schutzmechanismen vorhanden sind, die Verletzungen der Daten verhindern.*
8. *DEMONSTRATE: Bei dieser Strategie geht es darum, den Nachweis darüber zu führen, wie datenschutzrechtliche Vorgaben effektiv in das IT-System implementiert worden sind. Diese Strategie geht damit also einen Schritt weiter als die ENFORCE-Strategie.*

Wurden die datenschutzrechtlichen Anforderungen beim Erwerb von IT-Produkten sowie auch bei werkvertraglichen oder eigenen Individualentwicklungen bislang also eher vernachlässigt, so sind diese nun ausdrücklich zu berücksichtigen. Dies gilt umso mehr, da gegenüber der verantwortlichen Stelle nunmehr ein Bußgeld von bis zu 10.000.000 EUR verhängt werden kann (vgl. Art. 83 Abs. 4 a DS-GVO), wenn diese sich trotz der Existenz datenschutzkonformer Alternativen für den Einsatz datenschutzkritischer IT-Lösungen entscheidet.

Praxistipp:

- Beachtung von „privacy by design“ und „privacy by default“-Grundsätzen bei Einkauf und Gestaltung von IT-Lösungen
- Bestehende IT-Verfahren überprüfen und ggf. Anpassungen der inhaltlich/technischen Gestaltung vornehmen
- Produktanforderungen mit dem Datenschutz- und IT-Sicherheitsbeauftragten abstimmen

K) Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen

Nach der Europäischen Datenschutzgrundverordnung (DS-GVO) unterliegen Unternehmen im Falle einer Verletzung des Schutzes personenbezogener Daten folgenden Pflichten:

der Meldepflicht gegenüber der Aufsichtsbehörde gemäß Art. 33 und der Benachrichtungspflicht des Betroffenen gemäß Art. 34. Diese Pflichten sind im Vergleich zu der bisher geltenden Regelung des § 42a Bundesdatenschutzgesetz (BDSG) umfangreicher.

I. Meldepflicht gegenüber Aufsichtsbehörde

1. Für wen gilt die Meldepflicht?

Adressat der Regelung ist jeder Verantwortliche im Sinne der DS-GVO. Dies ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die – allein oder gemeinsam – über die Zwecke und Mittel der Verarbeitung entscheidet. Innerhalb eines Unternehmensverbundes können auch mehrere als gemeinsam Verantwortliche kooperieren, sog. Joint Controllers.

Liegt eine Auftragsverarbeitung vor, ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen unverzüglich zu informieren. Dieser nimmt dann die Meldung an die Aufsichtsbehörde vor.

2. Wann besteht die Meldepflicht?

Grundsätzlich ist ein Unternehmen verpflichtet, jede Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde zu melden. Nach Artikel 4 Nr.

12 DSGVO stellt jede 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, eine meldepflichtige Verletzung dar.

Die Meldung ist unverzüglich und möglichst binnen 72 Stunden vorzunehmen. Kann die 72 Stunden-Frist nicht eingehalten werden, ist der Meldung eine Begründung für die Verzögerung beizufügen.

Eine Meldung kann ausnahmsweise unterbleiben, wenn die Datenschutzverletzung nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

Ein Risiko – und damit eine Meldepflicht – besteht nach Erwägungsgrund 75 der DS-GVO immer bei solchen Verarbeitungen, die

- zu physischem, materiellen oder immateriellen Schaden, Diskriminierung, Identitätsdiebstahl/-betrug, finanziellem Verlust, Rufschädigung, Vertraulichkeitsverlust von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugter Aufhebung der Pseudonymisierung, erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen können,
- betroffene Personen um Rechte und Freiheiten bringt oder diese an der Kontrolle personenbezogener Daten hindert,
- die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, Gesundheitsdaten, Angaben zum Sexualleben oder strafrechtliche Verurteilungen betreffen,
- die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Zuverlässigkeit, Verhalten, Aufenthaltsort oder den Ortswechsel betreffen, analysieren oder prognostizieren zwecks Profilings,
- personenbezogene Daten schutzbedürftiger Personen, insbesondere Kinder, betreffen oder
- große Mengen personenbezogener Daten und eine große Anzahl von betroffenen Personen betreffen.

3. Inhalt der Meldung

Die Meldung an die Aufsichtsbehörde muss mindestens die Beschreibung der Art der Verletzung, die Angabe von Kategorien und ungefährer Zahl der Betroffenen und der Datensätze enthalten. Außerdem ist Name und Kontakt des Datenschutzbeauftragten zu benennen. Abschließend hat eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung, sowie der von dem Verantwortlichen ergriffenen und vorgeschlagenen Maßnahmen zur Behebung zu erfolgen.

- Es muss im Unternehmen geregelt sein/werden, wie die interne Meldung und an wen (Verantwortlicher/betrieblicher Datenschutzbeauftragter/IT-Sicherheitsbeauftragter) zu erfolgen hat.
- Ist eine Meldung notwendig, sind aber noch keine Einzelheiten der Verletzung bekannt, sollte innerhalb der 72 Stunden eine kurze Meldung an die Aufsichtsbehörde erfolgen mit dem Hinweis, dass weitere Einzelheiten folgen werden.
- Die Aufsichten beabsichtigen, für eine Meldung von Datenverletzungen ein Internet-basiertes Formular zur Verfügung zu stellen.

II. Benachrichtigungspflicht gegenüber dem Betroffenen

1. Wann ist zu benachrichtigen?

Hat die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person zur Folge, hat der Verantwortliche den Verstoß nicht wie dargestellt nur der zuständigen Aufsichtsbehörde zu melden, sondern muss darüber hinaus die betroffene Person ohne unangemessene Verzögerung benachrichtigen.

2. Ausnahme von der Benachrichtigungspflicht

Eine Benachrichtigung muss nicht erfolgen, wenn

- Risiken für die betroffene Person durch geeignete technische und organisatorische Sicherheitsvorkehrungen ausgeschlossen wurden oder
- der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für Rechte und Freiheiten der betroffenen Person nicht mehr besteht oder
- dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat eine öffentliche Bekanntmachung o. ä. zu erfolgen.

3. Inhalt der Benachrichtigung

Die Benachrichtigung muss Angaben über die Art der Verletzung, die wahrscheinlichen Folgen sowie die zur Behebung ergriffenen oder vorgeschlagenen Maßnahmen enthalten. Diese Angaben müssen in klarer und einfacher Sprach abgefasst werden. Darüber hinaus sind Name und Kontakt des Datenschutzbeauftragten zu nennen.

III. Was passiert bei Verstoß gegen die Melde-/ oder Benachrichtigungspflicht?

Die DS-GVO sieht vor, dass bei einem Verstoß gegen die Pflichten aus Artikel 33 und 34 Bußgeldern von bis zu zwei Prozent des weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahres verhängt werden können.

Hiervon trifft § 43 Abs. 4 BDSG-neu eine abweichende Regelung: Danach kann eine Meldung nach Art. 33 DS-GVO oder eine Benachrichtigung nach 34 DS-GVO in einem Ordnungswidrigkeitenverfahren gegen den Meldepflichtigen oder Benachrichtigenden nur mit dessen Zustimmung verwendet werden. Ob diese Abweichung im nationalen Recht zukünftig Bestand haben wird, bleibt abzuwarten. Über die Vereinbarkeit der Ausnahme mit Europarecht besteht aktuell Uneinigkeit. Letztendlich werden wohl die Gerichte hierüber entscheiden. Es empfiehlt sich daher aus Unternehmersicht, sich an den Anforderungen der DS-GVO zu orientieren und die weitere Entwicklung aufmerksam zu beobachten.

Weitere Dokumente:

Hinweise des Bayerischen Landesamts für Datenschutzaufsicht: https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

L) Datenschutz für kleine Unternehmen nach der EU-Datenschutz-Grundverordnung – was ändert sich?

Vorbemerkungen:

Sie wollen ein Unternehmen gründen oder besitzen bereits ein Unternehmen, das Kontakt zu Endkunden hat? Dann sollten Sie bezüglich des Datenschutzes folgendes beachten:

Die EU-Datenschutz-Grundverordnung (DSGVO) erhöht zwar die Anforderungen an den Datenschutz, vieles ist aber bisher schon geltende Rechtslage in Deutschland nach dem Bundesdatenschutzgesetz (BDSG). Nachfolgend soll an einem praktischen Beispiel des Muster-Unternehmens „Homedreams“, Inh.: Miranda Mustera, Geschäftszweig: Einzelhandel mit selbst genähten Wohnaccessoires, Angebot von Selbstnähkursen und Einrichtungsberatung; MitarbeiterInnen: 4 [ab 10 Beschäftigte: Bestellung eines betrieblichen Datenschutzbeauftragten] dargestellt werden, welche Anforderungen sich (neu) aus der DSGVO ergeben.

1. Rechtsgrundlage für Ihre Datenverarbeitung

a) Vertrag

Wenn Sie Kunden etwas verkaufen wollen oder Ihnen eine Dienstleistung erbringen wollen, handelt es sich um die Anbahnung bzw. Erfüllung eines Vertragsverhältnisses. Hierzu benötigen Sie entsprechende Angaben ihrer Kunden (z. B. Name, Anschrift, Telefonnummer, vielleicht auch darüberhinausgehende Angaben wie das Geburtsdatum, Kontodaten, Fotos). Für die Grunddaten zur Abwicklung des Vertrags benötigen Sie keine gesonderte Einwilligung ihrer Kunden, für darüberhinausgehende Daten ja. Falls der Vertrag erfüllt ist und es keine gesetzlichen Gründe für seine Aufbewahrung mehr gibt (z. B. steuerliche oder handelsrechtliche Gründe), müssen die Daten gelöscht werden.

b) Einwilligung

In der Einwilligungserklärung müssen Sie auf die jederzeitige Widerrufbarkeit dieser Einwilligung hinweisen. Sie sollten hier nach obligatorischen und freiwilligen Daten trennen. Sie können eine elektronische Einwilligung einholen, dürfen aber keine voreingestellte Einwilligung in Form eines Häkchens benutzen („double-opt-in“). Zudem müssen Sie ihre Kunden darüber informieren, zu welchem Zweck Sie diese Daten verarbeiten wollen. Sie müssen die Einwilligungen dokumentieren.

c) Sie müssen Informationspflichten erfüllen:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters,
- Kontaktdaten des Datenschutzbeauftragten,
- Zwecke der Verarbeitung und Rechtsgrundlage,
- wenn die Verarbeitung auf Art. 6 Abs. 1 f beruht: berechtigtes Interesse des Verantwortlichen,
- ggf. Empfänger oder Kategorien von Empfängern,
- Absicht der Übermittlung in ein Drittland/internationale Organisation sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission,
- Dauer der Datenspeicherung,
- Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und Recht auf Datenübertragbarkeit,
- Recht auf Widerruf einer Einwilligung (bei Verarbeitung mit Art. 6 Abs. 1 a o. Art. 9 Abs. 2 a),
- Bestehen eines Beschwerderechts gegenüber einer Aufsichtsbehörde,
- Information, ob die Bereitstellung der personenbezogenen Daten gesetzlich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und welche möglichen Folgen die Nichtbereitstellung hätte,
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (Art. 22).

Diese Informationspflichten müssen zum Zeitpunkt der Erhebung gegenüber dem – zukünftigen – Kunden erfüllt werden.

Falls die Daten nicht bei der betroffenen Person erhoben wurden, muss die Quelle angegeben werden.

Für die Nutzer Ihrer Internetseite müssen Sie bekannt geben, ob und welche Cookies Sie verwenden und ob Sie die Nutzer der Seiten tracken. Nutzen Sie hierfür einen Dienstleister, müssen Sie dazu eine Vereinbarung über die Auftragsverarbeitung schließen. Hat der Dienstleister seinen Sitz in einem Drittland, z. B. den USA, müssen Sie prüfen, ob die Weitergabe der Daten über EU-Standardvertragsklauseln oder über Privacy Shield abgesichert ist. Dabei handelt es sich um eine Vereinbarung zwischen der EU und den USA zur Angemessenheit des Datenschutzniveaus bei denjenigen Unternehmen, die die Anforderungen von Privacy Shield erfüllen.

2. Dienstleister

a) Wo verarbeiten Sie diese Daten? Auf Ihrem eigenen Server oder bei einem Dritten?

Bei letzterem müssen Sie eine schriftliche (oder elektronische) Vereinbarung über die Auftragsverarbeitung schließen, denn der IT-Dienstleister darf die Daten nur nach Ihrer Weisung verarbeiten. Liegen die Daten auf Ihrem eigenen Server, nutzen Sie aber eine Cloud-Anwendung, müssen Sie klären, ob die Daten in Deutschland, in Europa oder in den USA gespeichert sind. Im letzteren Fall handelt es sich um einen Datentransfer in Drittländer, so dass Sie hierfür eine besondere Grundlage benötigen, wenn die Daten in die USA übermittelt werden.

b) Haben Sie einen Internetauftritt, der von einer Webdesignagentur gestaltet wird? Hat die Webdesignagentur Zugriff auf die personenbezogenen Daten, die Ihre Interessenten/Kunden dort angeben? Dann müssen Sie auch hier eine Vereinbarung über die Auftragsverarbeitung schließen. Zudem sind Sie nach dem Telemediengesetz verpflichtet, ein sogenanntes Impressum zu haben, d. h. Sie müssen hier angeben: Name, Anschrift, Rechtsform, E-Mail-Adresse, Umsatzsteuer-Identnummer usw. [Bei mehr als 10 Beschäftigten müssen Sie zusätzlich angeben, inwieweit Sie bereit oder verpflichtet sind, an einem Verfahren vor einer Verbraucherschlichtungsstelle teilzunehmen (§§ 36, 37 Verbraucherstreitbeilegungsgesetz).] Bei Online-Verträgen müssen Sie Ihrer Informationspflicht nach Art. 14 der sog ODR-Verordnung nachkommen.

c) Wollen Sie Ihre Buchführung, insbesondere auch die Gehaltsabrechnung Ihrer Mitarbeiter, über einen Steuerberater abwickeln, müssen Sie hierzu einen entsprechenden Dienstvertrag schließen.

d) Wollen Sie ein Inkassounternehmen einschalten, um säumige Kunden zur Zahlung auffordern zu lassen, benötigen Sie hierfür ebenfalls einen Dienstvertrag.

e) Falls Sie einen elektronischen Bezahldienst nutzen, müssen Sie mit ihm einen Dienstleistungsvertrag schließen.

3. Lieferanten

Haben Sie Lieferanten, von denen Sie ebenfalls Daten, wie Name, Anschrift, Telefonnummer, Produktangebot, Ansprechpartner, URL der Homepage und E-Mail-Adressen gespeichert haben, so fallen auch diese Angaben unter das Vertragsverhältnis bzw. Sie benötigen für bestimmte Angaben ebenfalls die Einwilligung der Person zur Speicherung ihrer Daten.

4. Mitarbeiter

Sie müssen Ihre Mitarbeiter darüber informieren, welche Daten und zu welchem Zweck sie diese verarbeiten. Sollten Sie Ihren Mitarbeitern die private Nutzung von E-Mails und des Internets in der Arbeitszeit gestatten, sollten Sie dazu klären, welchen Umfang diese Nutzung umfassen darf und dass die Nutzung bestimmte Inhalte nicht betreffen darf. Die Gestattung können Sie mit einer Einwilligung verbinden, dass die Mitarbeiter Ihre Kontrollen gestatten, damit weder Inhalt noch Umfang der Nutzung gegen Gesetze und die arbeitsrechtlichen Pflichten verstoßen. Diese Einwilligung muss in Schriftform erfolgen.

5. datenschutzrechtliche Anforderungen

Sie müssen Ihre Verfahren in einem sogenannten Verzeichnis für die Verarbeitungstätigkeiten mit folgenden Angaben dokumentieren:

- Name und Kontaktdaten des Verantwortlichen, des Vertreters, ggfs. des gemeinsam Verantwortlichen sowie des etwaigen Datenschutzbeauftragten
- Zweck der Verarbeitung
- Rechtsgrundlage
- Kategorie der betroffenen Personen und personenbezogenen Daten
- Kategorie von Empfängern der Daten
- Übermittlung in Drittstaaten
- Löschfristen
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherung

Falls Sie Mitarbeiter haben, müssen Sie sie auf die Vertraulichkeit von Daten verpflichten (auf das Berufsgeheimnis müssen Sie verpflichten, soweit solche Daten verarbeitet werden) und sie auf den Datenschutz hinweisen bzw. sie angemessen schulen und dies dokumentieren. Sie sollten überlegen, wie Sie mit einem Auskunftsersuchen umgehen, wenn jemand erfahren möchte, welche Daten Sie über ihn gespeichert haben. Sie sollten zusätzlich schauen, ob Sie einen Prozess aufsetzen, falls es zu Datenverstößen kommt und Sie dies innerhalb von 72 Stunden der Aufsicht melden müssen. Die betroffene Person müssen Sie unverzüglich über den Datenverstoß informieren.

Sie müssen ein Löschkonzept vorsehen (geregelt für: 6 Jahre Geschäftsbriefe, 10 Jahre steuerrelevante Unterlagen, 6 Monate Bewerbungsunterlagen). Alle anderen Daten bzw. Dokumente mit personenbezogenen Daten müssen gelöscht bzw. vernichtet werden, wenn sie nicht mehr benötigt werden. Daran schließt sich die Frage an, wie datenschutzkonform Unterlagen vernichtet werden können und müssen (Datenträger zerstören, Papierunterlagen mit personenbezogenen Daten schreddern).

6. technisch-organisatorische Maßnahmen

Sie betreffen die Frage, wie sicher Ihre Informationssicherheit (IT, Sicherheit im Büro/Geschäft) ist; auch dies muss dokumentiert werden. Sie müssen insbesondere mit Ihrem Steuerberater

klären, wie die sensiblen Daten ihrer Mitarbeiter (Gesundheitsdaten, Religionszugehörigkeit) gut geschützt sind. Hierzu müssen bestimmte Maßnahmen ergriffen werden (Risikobewertung/Datenschutz-Folgenabschätzung). Eine Übermittlung per E-Mail ohne weitere Sicherheitsmaßnahmen ist datenschutzrechtlich nicht zulässig. Nachstehende Punkte geben einen groben Anhaltspunkt für solche Maßnahmen:

a) Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

aa) Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

bb) Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

cc) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

dd) Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

b) Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

aa) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

bb) Eingabekontrolle/Verarbeitungskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

cc) Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

dd) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

ee) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

ff) Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten)

Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

Haben Sie Ihre Daten so gesichert, dass Sie sie bei einem eventuellen Verlust wiederherstellen können?

Bei der Einholung der Einwilligung Ihrer Kunden müssen Sie nicht nur die datenschutzrechtlichen Anforderungen erfüllen, sondern auch bei einer Einwilligung zur Werbung das Gesetz gegen unlauteren Wettbewerb (UWG) beachten.

M) Datenschutz-Folgenabschätzung

Vorbemerkung:

Die Datenschutz-Grundverordnung (DSGVO) regelt die Rahmenbedingungen für Datenschutz und Datensicherheit. Hierbei führt sie für die Verarbeitung von personenbezogenen Daten einen risikobasierten Ansatz ein. Dies bedeutet: Je risikoreicher und schadensgeneigter eine Verarbeitung von Daten für Betroffene sein kann, umso höhere Anforderungen stellt die DSGVO an die Anwendung, Art. 24, 32 DSGVO. Immer dann, wenn eine Datenverarbeitung für die Rechte und Freiheiten einer Person ein hohes oder ein sehr hohes Risiko zur Folge hat, hat der Verantwortliche vor deren Einführung eine sog. Datenschutz-Folgenabschätzung (DSFA) vorzunehmen und zu ermitteln, welche Folgen eine geplante Verarbeitung für den Schutz der Daten Betroffener hätte. Über das Instrumentarium der DSFA sollen Risiken beschrieben, bewertet und reduziert werden.

Lässt sich ein (sehr) hohes Risiko nicht durch angemessene technische und/oder organisatorische Maßnahmen reduzieren, ist für den Einsatz der Anwendung vorab eine Genehmigung der zuständigen Datenschutzaufsichtsbehörde einzuholen.

Eine DSFA ist zu überprüfen und anzupassen, sollten neue Risiken hinzukommen, die bereits behandelte Risiken ändern oder wesentlich erschweren. Über Prüfroutinen kann sichergestellt werden, dass eine DSFA noch aktuell ist.

Behandlung bereits vorhandener Datenverarbeitungen
Für diese gibt es keinen Bestandsschutz, d. h. eine DSFA ist durchzuführen, wenn die Voraussetzungen hierfür vorliegen oder neue Risiken zu einer entsprechenden Wertung führen. Gestützt auf Erwägungsgrund 171 der DS-GVO sehen die Leitlinien zu DSFA der Art.-29-Datenschutzgruppe (Stand: 04.10.2017)* vor, dass eine DSFA nicht durchzuführen ist, wenn eine Datenschutzaufsicht oder ein Datenschutzbeauftragter eine Datenverarbeitung im Wege einer sog. „Vorabkontrolle“ vorab geprüft hat. Derartige Prüf-entscheidungen bleiben in Kraft, bis diese geändert, ersetzt oder aufgehoben sind.

Vorgehensweise

1. Für jede Verarbeitung ist mittels einer systematischen Risikobewertung (sog. „Schwellenwertanalyse“) zu klären, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Das Ergebnis ist zu dokumentieren (z. B. bei der Beschreibung der Verarbeitung im sog. Verzeichnis von Verarbeitungstätigkeiten).
2. Für mehrere ähnliche Verarbeitungsvorgänge (umfasst alle Daten, Systeme [Hard- und Software] und Prozesse) reicht eine Abschätzung, sofern diese ein ähnlich hohes Risiko haben.
3. Vorstufe einer Risikobewertung ist eine Schutzbedarfsfeststellung der zu verarbeitenden personenbezogenen Daten anhand der Datenarten (Kundendaten, Mitarbeiterdaten, Steuerdaten, Gesundheitsdaten etc.):

Schutzbedarfskategorien – Schadensschwere

Schutz-bedarf	Klasse	Erläuterungen Beeinträchtigung des Persönlichkeitsrechts	Beispiele
Normal (Gering oder mittel)	1	Wäre für Betroffene als tolerabel einzustufen. Ein möglicher Datenmissbrauch hätte nur geringfügige Auswirkungen (wirtschaftlich/gesellschaftspolitisch) für Betroffene. • Nicht zur Veröffentlichung bestimmte Daten • Geringfügige Schäden bei Veröffent-lichung/Verfälschung	Gering: Öffentliche Register, Anschrift, Kontaktdaten Mittel: Daten über Geschäfts- und Vertragsbeziehungen, Kontostände, Prüfungsergebnisse, Personaldaten (soweit nicht Stufe 2), Kreditauskünfte
Hoch	2	Wäre für Betroffene als erheblich einzustufen. Ein möglicher Datenmissbrauch hätte erhebliche Auswirkungen (wirtschaftlich/gesellschaftspolitisch, ggf. Beeinträchtigung der persönlichen Unversehrtheit) für Betroffene. • Sensible Daten • Hohe Folgeschäden bei Veröffentli-chung/Verfälschung	Steuerdaten, strafbare Handlungen; Daten, die einem Berufs-, Geschäfts-, Fernmelde- oder Mandantengeheimnis unterliegen; Personaldaten (soweit nicht Stufe 1) wie z. B. Beurteilungen, berufliche Laufbahn, Angaben über Behinderung etc.
sehr hoch	3	Wäre für Betroffene als besonders bedeutsam und als nicht tolerabel einzustufen. Ein möglicher Datenmissbrauch bedeutet für Betroffene wirtschaftlichen/gesellschaftspolitischen Ruin oder beeinträchtigt die persönliche Unversehrtheit gravierend. • Hochsensible Daten	Adressen von polizeilichen V-Leuten, Adressen von Zeugen in bestimmten Strafverfahren

		• Veröffentlichung/Verfälschung verletzt Persönlichkeitsrechte, verursacht Schaden an Leib und Leben oder Ansehender Betroffenen	

Bestandteile einer Datenschutz-Folgenabschätzung

1. Risikobewertung

Das Datenschutzrisiko für den Betroffenen, dessen Daten verarbeitet werden (nicht ein Schadensrisiko für das Unternehmen), ist anhand objektiver Kriterien (Art, Umfang, Umstände und Zwecke einer Verarbeitung) zu bestimmen

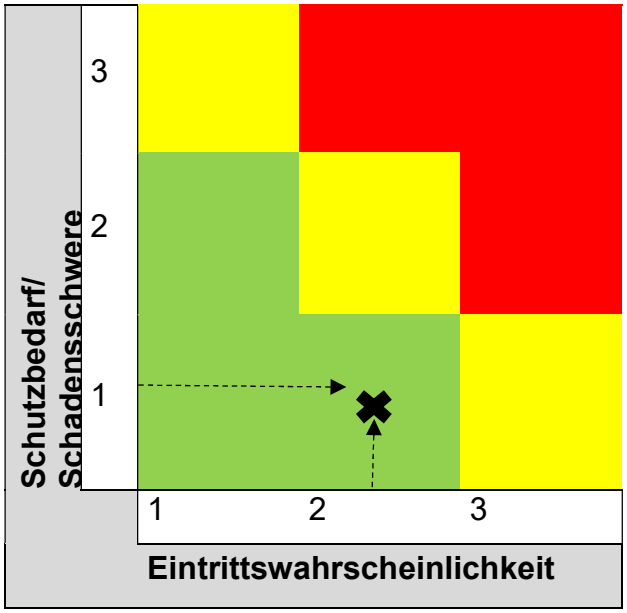
- nach der Eintrittswahrscheinlichkeit (zu berücksichtigen ist hier auch die Risiko-Quelle, also der Angreifer und ein durch diesen zu verursachender Schaden)
- nach der Schwere des Schadens
  - In einer Skalierung
    a) vernachlässigbar/begrenzt (normal)
    b) wesentlich (hoch)
    c) maximal (sehr hoch)

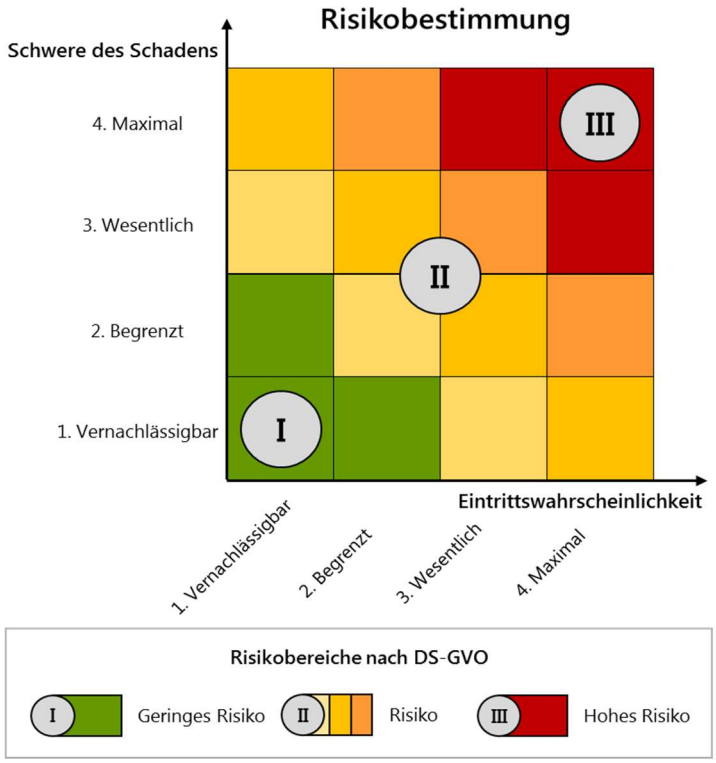
Eine Datenschutz-Folgenabschätzung ist nur durchzuführen, wenn eine Risikobewertung ergibt, dass eine Datenverarbeitung ein hohes oder sehr hohes Risiko (in der Skalierung: ausschließlich die gelben und roten Felder) für die Betroffenen, deren Daten verarbeitet werden, zur Folge hat.

Ergebnis: Hohes Risiko + Sehr hohes Risiko ➔ Datenschutz-Folgenabschätzung

Verfahren zur Risikobestimmung

- Hierfür gibt es *keine einheitliche*, gesetzlich vorgeschriebene Methode. Daher sollte eine Risikobestimmung nach einem gängigen Verfahren (Best Practice: CNIL, ISO) erfolgen wie z. B. nach dem Standard-Datenschutzmodell oder dem Muster einer Datenschutzaufsicht.





Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Praxis-Tipps:

- ✓ EU-weit anerkannte Vorgehensmodelle zur Risikobestimmung einsetzen.
- ✓ Das verwendete Vorgehensmodell muss das Verfahren gut dokumentieren (wichtiges Kriterium für einen massenhaften Einsatz).
- ✓ Maßnahmenkataloge (technisch-organisatorische Maßnahmen zur Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit) zur Behandlung von Risiken sollten gut dokumentiert und erprobt sein.

- Jedoch gibt es *einheitliche Kriterien* für eine Risikobestimmung. Die Art. 29-Datenschutzgruppe hat in den Leitlinien zur DSFA* Kriterien festgelegt, anhand deren geprüft werden sollte, ob eine DSFA durchgeführt werden muss. Dies soll umso wahrscheinlicher sein, wenn mindestens zwei und mehr der nachfolgenden und als besonders riskant eingestuften Kriterien erfüllt sind:

  - Scoring und Evaluierung, inkl. Profilbildung und Vorhersagen
  - Automatisierte Entscheidungen mit rechtlicher oder im Gewicht vergleichbarer Wirkung
  - systematische Beobachtung (z. B. von Arbeitsräumen)
  - Sensible Daten
  - Datenverarbeitung in großem Umfang
  - Datensätze, die abgeglichen oder kombiniert werden
  - Daten von besonders schutzbedürftigen Personen (z. B. Arbeitnehmer, Kinder)
  - Innovative Nutzung oder Verwendung von technologischen und organisatorischen Lösungen (z. B. eine Kombination aus Fingerabdruckscan und Gesichtserkennung)
  - Betroffene können ein Recht oder eine Dienstleistung ohne vorgeschaltete Datenverarbeitung nicht in Anspruch nehmen (z. B.: Eine Bank verlangt die Durchleuchtung von Daten eines potenziellen Kreditkunden vor einer Entscheidung über einen Vertragsabschluss)

2. <u>Schaden</u>

Ein Mensch kann durch eine Datenverarbeitung physische, materielle und immaterielle Schäden erleiden. Bezogen auf die geplante Anwendung ist zu klären, welche Schäden aus der Datenverarbeitung für Betroffene resultieren können.

Beispielhaft nennt die DS-GVO hier

- Diskriminierung
- Identitätsdiebstahl
- Rufschädigung
- Finanzieller Verlust
- Hinderung der Kontrolle über eigene Daten
- Profilbildung mit Standortdaten

3. Risikominimierung

Wer personenbezogene Daten verarbeiten will, ist verpflichtet, im Verhältnis zum Risiko nach dem Stand der Technik angemessene (nicht: neueste und teuerste) Maßnahmen zum Schutz der Daten zu ergreifen, diese regelmäßig, bei Bedarf sogar unverzüglich zu überprüfen und erforderlichenfalls upzudaten. In der Regel handelt es sich um eine Kombination aus

- organisatorischen Maßnahmen (z. B. Datenschutzschulung von Mitarbeitern, interne Regelungen zum Datenschutz, Notfallkonzept) und
- technischen Maßnahmen (z. B. Einsatz von Firewall und Virenscanner und deren zeitgemäßer Update, Verschlüsselung von Daten).

4. Nachweise hierüber erbringen (Dokumentation!)

Die Durchführung einer Datenschutz-Folgenabschätzung ist eine gesetzliche Pflicht. Deren Einhaltung müssen verantwortliche Stellen nachweisen. Der Nachweis ist Bestandteil der Rechenschaftspflicht. Diese verpflichtet verantwortliche Stellen, alle Vorgaben der DS-GVO einzuhalten, wirksam umzusetzen, zu überprüfen und bei Bedarf nachzubessern.

Zu dokumentieren sind:

- die Durchführung einer Risikobewertung,
- das Ergebnis der Analyse (normales, hohes, sehr hohes Risiko) und
- eine daraus ggf. abzuleitende DSFA

    - Ergebnis ➔ keine DSFA, da
        - Whitelist
          Datenschutzaufsichtsbehörden können (optional) eine Liste von Verarbeitungstätigkeiten (sog. Whitelist) veröffentlichen, die aus ihrer Sicht nie hochrisikobehaftet sind und damit keiner DSFA bedürfen.
          Offen ist, ob die Datenschutzaufsichtsbehörden von dieser gesetzlichen Möglichkeit Gebrauch machen werden.
        - Die Verarbeitungsvorgänge vor dem 25.05.2017 von einer Datenschutzaufsichtsbehörde oder einem Datenschutzbeauftragten im Wege einer Vorabkontrolle geprüft worden sind.
        - die Verarbeitung eine gesetzliche Aufgabe nach Art. 6 Abs. 1 c DS-GVO (Erfüllung einer rechtlichen Verpflichtung) oder Art. 6 Abs. 1 e DS-GVO (Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt) ist; eine allgemeine DSFA hierfür ist bereits bei Erlass der Rechtsgrundlage (z. B. Gewerberegister) vorgenommen worden, und der Mitgliedstaat hat die Durchführung einer DSFA für nicht notwendig erklärt.
        - Kein hohes Risiko als Ergebnis der Prüfung.

- Ergebnis ➔ DSFA, da
  - Blacklist
    Datenschutzaufsichtsbehörden müssen eine sog. Blacklist veröffentlichen. Diese enthält Datenverarbeitungen, die aus Sicht der Datenschutzaufsicht generell ein hohes Risiko haben und daher stets (ohne weitere sonstige Prüfung) vor deren Einsatz eine Vorabkonsultation der Aufsicht erfordern.
  - Ergebnis der Risikobewertung:
    (sehr) hohes Risiko und eine Risikoreduzierung ist nicht möglich.

Führen geeignete technische und/oder organisatorische Maßnahmen dazu, dass für die Daten Betroffener ein (sehr) hohes Risiko in ein normales Risiko reduziert werden kann, ist keine Datenschutz-Folgenabschätzung durchzuführen. So muss ein hoher Schutzbedarf (z. B. biometrische Daten, Personalaktendaten) für sich allein nicht zwingend zu einem hohen Risiko führen, sondern nur dann, wenn gleichzeitig die Eintrittswahrscheinlichkeit für einen Vorfall hoch ist.

Mindestinhalt einer Datenschutz-Folgenabschätzung

Diesen legt die DSGVO wie folgt fest

- Systematische Beschreibung der Verarbeitungsvorgänge und Zwecke
- Notwendigkeit und Verhältnismäßigkeit der Verarbeitung im Verhältnis zum Zweck der Verarbeitung
- Risikobewertung (s. o.)
- Geplante Abhilfemaßnahmen zur Bewältigung der Risiken

➔ Verbleibt ein (sehr) hohes Restrisiko, bedeutet dies Folgendes:

- Der Verantwortliche hat eine Datenschutz-Folgenabschätzung durchzuführen.
- Ferner hat er **vor** einem Einsatz einer derartigen Datenverarbeitung die zuständige Datenschutzaufsichtsbehörde zu konsultieren und
- deren Entscheidung (z. B. Einsatz nur nach Ergreifung weiterer Schutzmaßnahmen, Verbot der geplanten Verarbeitung) zu beachten.

Rolle des Datenschutzbeauftragten

Hat eine verantwortliche Stelle freiwillig oder aufgrund gesetzlicher Vorgabe einen betrieblichen Datenschutzbeauftragten bestellt, so legt die DSGVO bezogen auf Datenschutz-Folgenabschätzungen Folgendes fest:

- Die verantwortliche Stelle hat den Rat des Datenschutzbeauftragten einzuholen.
- Zu den Aufgaben eines Datenschutzbeauftragten gehört auf Anfrage die Beratung im Zusammenhang mit der Durchführung einer DSFA und die Überwachung ihrer Durchführung.

Prozessschritte einer DSFA

1. DSFA-TEAM erstellen
2. Prüfplanung
3. Beurteilungsumfang festlegen

   z. B.

   a. Beschreibung des Verarbeitungsvorgangs

   b. inkl. der Datenflüsse und Zwecke der Verarbeitung in Abgrenzung zu anderen (Geschäfts-)Prozessen
4. Akteure und Betroffene identifizieren

   d. h. Datenschutzbeauftragten, Betriebsrat und ggf. Betroffene einbinden
5. Prüfung der Notwendigkeit/Verhältnismäßigkeit bezogen auf den Verarbeitungszweck
6. Rechtsgrundlagen für die Verarbeitung prüfen und dokumentieren
7. Risikoquellen identifizieren

   (Beweggründe, Ziele, Eintrittswahrscheinlichkeit)
8. Risikobewertung unter Berücksichtigung

   a. möglicher physischer, materieller oder immaterieller Schäden,

   b. deren Schwere sowie

   c. Eintrittswahrscheinlichkeit
9. Auswahl geeigneter Abhilfemaßnahmen

   a. u. a. durch technische und organisatorische Maßnahmen (toMs) und

   b. verbleibende Restrisiken eruieren und dokumentieren
10. DSFA-Bericht erstellen
11. Abhilfemaßnahmen umsetzen
12. Abhilfemaßnahmen auf Wirksamkeit testen
13. Dokumentation

    a. des DSFA-Berichts und

    b. der Überprüfung der Wirksamkeit der Maßnahmen
14. Freigabe der Verarbeitungsvorgänge

    inkl. Überprüfung und Audit einer DSFA und deren Aktualisierung
15. DSFA fortschreiben bei Aktualisierungsbedarf.

Publikationen

- *Artikel-29-Datenschutzgruppe: WP-29- Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“: 17/DE WP 248 rev.01 vom 04.04.2017 (Stand: 04.10.2017) http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- Kurzpapier Nr. 5 der Datenschutzkonferenz (DSK) – Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO https://www.lda.bayern.de/de/datenschutz_eu.html
- Bitkom e. V., Leitfaden „Risk Assessment & Datenschutz-Folgenabschätzung, https://www.bitkom.org/Bitkom/Publikationen/index.jsp
- Internationale Norm: ISO/IEC 29134 (project), Information technology – Security techniques – Privacy impact assessment – Guidelines, International Organization for Standardization (ISO) – enthält Leitlinien für Methodiken zur Durchführung einer DSFA
- Planspiel des ULD Schleswig-Holstein: https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf

Beispiele für EU-weite allgemeine Rahmenbedingungen

- Deutschland: Standard-Datenschutzmodell (SDM) https://www.datenschutzzentrum.de/sdm/
- Frankreich: Privacy Impact Assessment (PIA), Commission nationale de línformatique et des libertés (CNIL) – Leitlinien der französischen Datenschutzaufsichtsbehörde, https://www.cnil.fr/fr/node/15798

Beispiele für EU-weite branchenspezifische Rahmenbedingungen

- Privacy and Data Protection Impact Assessment Framework for RFID Applications32.[Rahmenvertrag für RFID-Anwendungen für die Datenschutz-Folgenabschätzung zu Methodiken.]
- http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme33 http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

N) Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen

Die Beschäftigten von Unternehmen, in denen personenbezogene Daten verarbeitet werden, müssen ab 25.05.2018 auf die Vertraulichkeit (bisher: Datengeheimnis) verpflichtet werden. Nachstehend finden Sie ein Muster hierfür.

Verpflichtungserklärung zur Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen*

.....

Name der verantwortlichen Stelle

Sehr geehrte(r) Frau/Herr.....

aufgrund Ihrer Aufgabenstellung verpflichte ich Sie auf die Wahrung der Vertraulichkeit personenbezogener Daten nach Art. 5 Abs. 1 f, Art. 32 Abs. 4 Datenschutz-Grundverordnung (DS-GVO), zu denen Sie im Rahmen Ihrer Tätigkeit Zugang erhalten oder Kenntnis erlangen. Es ist Ihnen untersagt, unbefugt personenbezogene Daten zu verarbeiten.

Diese Verpflichtung besteht auch nach Beendigung Ihrer Tätigkeit fort.

Verstöße gegen die Vertraulichkeit können nach Art. 83 Abs. 4 DS-GVO, §§ 42, 43 BDSG sowie nach anderen Strafvorschriften (s. Anlage) mit Freiheits- oder Geldstrafe geahndet werden.

In der Verletzung der Vertraulichkeit kann zugleich eine Verletzung arbeits- oder dienstrechtlicher Schweigepflichten liegen.

Eine unterschriebene Zweitschrift dieses Schreibens reichen Sie bitte an die Personalabteilung zurück.

....

Ort, Datum Unterschrift der verantwortlichen Stelle

Über die Verpflichtung zur Vertraulichkeit und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verpflichtungserklärung (Texte der Art. 5, Art. 32 Abs. 4, Art. 83 Abs. 4 DS-GVO, der §§ 42, 43 BDSG sowie der §§ 202a ff. StGB) habe ich erhalten.

....

Ort, Datum Unterschrift des Verpflichteten

* Diese Erklärung kann auf die Wahrung des Fernmeldegeheimnisses nach § 88 TKG (bei Mitwirkung an geschäftsmäßiger Telekommunikation) und allgemein auf die Wahrung von Betriebs- und Geschäftsgeheimnissen sowie Berufsgeheimnissen erweitert werden, Häufig ist die Verschwiegenheitsverpflichtung bei allgemeinen Betriebs- und Geschäftsgeheimnissen bereits im Arbeitsvertrag geregelt.

Merkblatt zur Verpflichtungserklärung

Artikel 5 DS-GVO

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“); 4.5.2016 L 119/35 Amtsblatt der Europäischen Union DE (1)Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Art. 32 Abs. 4 DS-GVO

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Art. 83 Abs. 4 DS-GVO

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

§ 42 BDSG

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen

den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 43 BDSG

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder
2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Strafgesetzbuch (StGB):

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 202d Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,
3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist, anvertraut worden oder sonst bekanntgeworden ist.

Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfasst worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) (weggefallen)

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen

bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Anmerkung:

§ 203 Abs. 1 Nr. 4a: Die anerkannten Beratungsstellen nach § 218b Abs. 2 Nr. 1 StGB stehen den anerkannten Beratungsstellen nach § 3 des G über die Aufklärung, Verhütung, Familienplanung und Beratung gleich gem. BVerfGE v. 4.8.1992 I 1585 - 2 BvO 16/92 u. a. -

Weiteres Muster-Dokument:

GDD- Praxishilfe Nr. XI nebst Musterformular:

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_11.pdf

(Muster einzeln als Word-Dokument: https://www.gdd.de/downloads/praxishilfen/Muster_Verpflichtung_auf_Vertraulichkeit_v1.4.docx)

O) Beschäftigtendatenschutz

Vorbemerkungen

Die EU-Datenschutz-Grundverordnung (DSGVO) trifft keine inhaltlichen Regelungen zum Datenschutz im Beschäftigungsverhältnis, sondern überlässt es dem nationalen Gesetzgeber, hierzu Vorschiften zu erlassen. Der deutsche Gesetzgeber hat das innerhalb der Änderung des Bundesdatenschutzgesetzes (BDSG) mit § 26 getan. Dieser lehnt sich weitgehend an den § 32 des noch geltenden BDSG an.

I. Rechtsgrundlagen

Die Geltung der Vorschriften der DSGVO und des BDSG setzt keine IT-gestützte Verarbeitung von Personaldaten voraus; sie gelten auch für in Papierform geführte Personalakten, § 26 Abs. 7 BDSG.

Die Datenverarbeitung ist zulässig, wenn sie zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses (z. B. Bewerberdaten), für seine Durchführung oder Beendigung erforderlich ist. Dazu gehören Pflichten, die sich aus Gesetzen (z. B. Steuer- oder Sozialgesetze), aus Tarifverträgen sowie Betriebs- oder Dienstvereinbarungen ergeben.

Die Verarbeitung besonderer Kategorien von Daten (z. B. Religionszugehörigkeit, Gesundheitsdaten) ist nach der DSGVO nach Art. 9 Abs. 2 Buchstabe b), § 26 Abs. 3 BDSG zulässig.

II. Wer ist Beschäftigter?

Nach § 26 Abs. 8 BDSG umfasst der Begriff auch LeiharbeitnehmerInnen sowie BewerberInnen und ausgeschiedene ArbeitnehmerInnen.

III. Einwilligung

Falls der Arbeitgeber für die Datenverarbeitung eine Einwilligung des Beschäftigten benötigt, muss sie nach § 26 Abs. 2 BDSG in Schriftform eingeholt werden. Die Freiwilligkeit der Einwilligung wird vermutet, wenn sich für den Arbeitnehmer ein rechtlicher oder wirtschaftlicher Vorteil ergibt (z. B. betriebliche Altersversorgung). Der Beschäftigte ist dabei auf die jederzeitige Widerrufsmöglichkeit seiner Einwilligung hinzuweisen. Insofern muss jedes Unternehmen überprüfen, ob bisherige Einwilligungen, die von den Beschäftigten eingeholt wurden, noch gültig sind. Die Anforderungen ergeben sich aus Art. 7 DSGVO. Fehlt es also an dem Hinweis auf das jederzeitige Widerrufsrecht und an der Darstellung des Zwecks der mit der Einwilligung verfolgten Datenverarbeitung, bestehen berechtigte Zweifel an der Gültigkeit der alten Einwilligungen nach dem 25.05.2018.

Nach Art. 22 Abs. 2 Buchstabe c) DSGVO bedarf eine automatisierte Entscheidung z. B. in Fällen elektronischer Scoring-Verfahren im Personalbereich einer ausdrücklichen Einwilligung der Beschäftigten.

Die Einwilligungen z. B. zur Verwendung eines Fotos des Beschäftigten im Internet oder zur privaten Nutzung von E-Mail und Internet mit Überprüfungsrecht des Arbeitgebers sollten auf vom Arbeitsvertrag getrennten Dokumenten eingeholt werden, weil sonst bei jedem neuen Einwilligungserfordernis der Arbeitsvertag geändert werden müsste.

IV. Kollektivvereinbarungen

Bisherige Betriebs- oder Dienstvereinbarungen müssen ebenfalls auf ihre Übereinstimmung mit der DSGVO überprüft werden. Dabei geht es insbesondere um die erhöhten Transparenzplichten nach Art. 13 und 14 DSGVO, also die Informationspflichten gegenüber der betroffenen Person, hier den Beschäftigten. Die Informationspflichten betreffen insbesondere den genauen Datenkranz, der verarbeitet wird, die Zwecke sowie die Angaben, an wen die Daten übermittelt werden. Davon umfasst ist auch der Hinweis auf etwaige Übermittlungen in Drittstaaten. Die Beschäftigten müssen auch über ihre Rechte nach Art. 12 DSGVO informiert werden:

- Auskunftsrecht, Art. 15
- Recht auf Berichtigung der Daten, Art. 16
- Recht auf Löschung von Daten, Art. 17
- Recht auf Einschränkung der Verarbeitung, Art. 18
- Recht auf Datenübertragbarkeit, Art. 20.

V. Datentransfer im Konzern

Als Rechtsgrundlage für eine Übermittlung von Personaldaten innerhalb eines Konzerns z. B. an die Tochter oder an die Konzernmutter, die die gesamte Personalverwaltung durchführt, kann auf Art. 6 Abs. 1 Buchstabe f) gestützt werden, wenn die Erforderlichkeit für den Transfer dargelegt werden kann. Damit wäre auch eine Übermittlung von Daten in Drittstaaten zulässig, wenn das angemessene Datenschutzniveau nach den Mechanismen der Art. 44 ff. DSGVO nachgewiesen werden kann.

VI. Datenschutz-Folgenabschätzung

Da zur Erfüllung z. B. der Verpflichtung zur Abführung der Kirchensteuer die Religionszugehörigkeit erfasst werden muss, muss für die Verarbeitung der Personalstammdaten eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchgeführt werden. Das gilt auch wegen der Verarbeitung von Gesundheitsdaten (z. B. Krankmeldungen, betriebliches Wiedereingliederungsmanagement) oder automatisierte Personalentscheidungen.

VII. Prüfschema für Betriebsvereinbarungen

1. Anforderungen nach DSGVO

Für Betroffene muss klar erkennbar sein, welche sie betreffenden personenbezogene Daten verarbeitet bzw. in welchem Umfang personenbezogene Daten gegenwärtig oder künftig verarbeitet werden, insbesondere muss deutlich werden:

- die Identität des Verantwortlichen
- die Zwecke der Verarbeitung
- die Informationen, die eine faire und transparente Verarbeitung gewährleisten
- das Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche personenbezogene Daten verarbeitet werden
- die Aufklärung über Risiken, Rechte, Garantien hinsichtlich der Datenverarbeitung
- die Aufklärung darüber, wie Rechte geltend gemacht werden können.

Außerdem müssen die Grundsätze nach Art. 5 DSGVO ihren Niederschlag finden.

Die Verarbeitung muss auf rechtmäßige Weise, nach Treu und Glauben in einer nachvollziehbaren Weise nur für einen festgelegten zu einem eindeutigen und legitimen Zweck erfolgen.

Dies galt auch schon nach bisherigem Recht.

Neu: Die DSGVO erfordert darüber hinaus angemessene und besondere Maßnahmen im Hinblick auf die Transparenz der Verarbeitung oder über eingesetzte Arbeitsmittel.

Zu beachten:

- die Identifizierung des Arbeitnehmers darf nur so lange möglich sein, wie es für den Zweck der Verarbeitung erforderlich ist,
- die Speicherfristen sind auf das unbedingt erforderliche Mindestmaß beschränken.

2. Prüfschema für bestehende Betriebsvereinbarungen

a) Werden auf Grundlage der Betriebsvereinbarung personenbezogene Daten verarbeitet?

b) Enthält die Betriebsvereinbarung Angaben zu den Grundprinzipien nach Art. 5 DSGVO?

aa) Rechtmäßigkeit (= Erlaubnistatbestände vorhanden?)

Verarbeitung rechtmäßig, nach Treu und Glauben und in nachvollziehbarer Weise? vgl. Art. 6 I a-f DSGVO, EG 39 und Art. 12 ff. DSGVO

bb) Zweckbindungsgrundsatz

Zweck deutlich vereinbart (konkret & detailliert)?

Falls Verarbeitung zu anderem Zweck erfolgt: Vereinbarkeit mit altem Zweck?

cc) Datenminimierung

Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke erforderliche Maß beschränkt?

Sind Strategien und Maßnahmen getroffen (Pseudonymisierung, techn. Vorrichtungen)?

dd) Datenrichtigkeit

Wurden Maßnahmen getroffen, um zu gewährleisten, dass personenbezogene Daten, die hinsichtlich des Zwecks ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden?

Dienstvereinbarung sollte Regelungen zu Korrekturprozessen enthalten.

ee) Speicherbegrenzung

Sind klare Regelungen zu Speicherdauer von personenbezogenen Daten in Dienstvereinbarung getroffen?

ff) Integrität und Vertraulichkeit

Sind technisch-organisatorischen Maßnahmen vorhanden, um den Schutz vor unbefugter, unrechtmäßiger Verarbeitung sowie vor Schädigung, Zerstörung oder Verlust zu gewährleisten? Ist die Verarbeitung besonderer Datenkategorien (z. B. Religionszugehörigkeit, Gesundheitsdaten, biometrische Daten) ausreichend gesichert?

3. Werden besondere Kategorien personenbezogener Daten verarbeitet?

Dann Art. 9 DSGVO beachten. Besonders relevant bei: Zutrittssystemen mit biometrischer Datenverarbeitung, Einsatz von elektronischen Personalakten, Ausgestaltung des BEM, Durchführung von Assessmentcentern mit elektronischer Datenverarbeitung der Bewerberdaten.

4. Sind Maßnahmen getroffen worden, um die Informationspflichten zu erfüllen?

Der Arbeitgeber muss Angaben machen zu: Name des Verantwortlichen, seines Vertreters, des betrieblichen Datenschutzbeauftragten, den Zweck sowie die Rechtsgrundlage der Verarbeitung, Speicherfristen, Betroffenenrechte, Empfänger der Daten, Beschwerderechte und Rechtsbehelfe, Datenverarbeitung im Drittland.

5. Sind Maßnahmen getroffen worden, um die Betroffenenrechte zu berücksichtigen?

Sind die Angaben zu den Betroffenenrechten nach Art. 15 sowie Mitteilungen nach Art. 16 ff. DSGVO enthalten?

Die umfangreichen Angaben sollten als Anhang zum Arbeitsvertrag oder in der Betriebsvereinbarung abgebildet werden

Praxistipp:

Eine Alternative zur Änderung aller Betriebsvereinbarungen könnte der Abschluss einer „Dach"-Betriebsvereinbarung sein, in der ausschließlich datenschutzrechtliche Aspekte geregelt werden und die Bezug nimmt auf die speziellen Vereinbarungen z. B. zur Arbeitszeit usw. Zumindest könnte aber eine schriftliche allgemeine Information der Beschäftigten darüber erfolgen, welche Daten für welche Zwecke in dem Unternehmen verarbeitet werden.

Weitergehende Informationen zum Datenschutz finden Sie unter:

https://www.magdeburg.ihk.de/recht/Wirtschaft%20und%20Recht/Datenschutz/Newsletter-zum-Datenschutz/3755368 - Newsletter der IHK Magdeburg zum Thema DSGVO

https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/kurzpapiere-zum-neuen-datenschutzrecht/ - Kurzpapiere zur DSGVO bereitgestellt auf der Homepage des Landesbeauftragten für den Datenschutz Sachsen-Anhalt

https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/ - weitere Dokumente zur DSGVO bereitgestellt auf der Homepage des Landesbeauftragten für den Datenschutz Sachsen-Anhalt, die stets aktualisiert werden

https://www.lfd.niedersachsen.de/startseite/dsgvo/fragen_zur_vorbereitung_auf_dsgvo/ - ein spezieller Fragebogen der Landesbeauftragten für den Datenschutz Niedersachsen

www.gdd.de – Gesellschaft für Datenschutz und Datensicherheit mit Mustern z. B. zu einem Vertrag über die Auftragsverarbeitung

https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/DSGVO_Kurzpapiere.html?nn=5217040 - Kurzpapier der Datenschutzaufsichtsbehörden zu bestimmten Aspekten der DSGVO

Ansprechpartner:

Sandra Froreck
Industrie- und Handelskammer Magdeburg
Alter Markt 8 | 39104 Magdeburg
Tel: +49 391 5693 185 | Fax: +49 391 5693 333185
Mail: froreck@magdeburg.ihk.de

Die Veröffentlichung von Merkblättern ist ein Service der IHK Magdeburg für ihre Mitgliedsunternehmen. Dabei handelt es sich um eine zusammenfassende Darstellung der rechtlichen Grundlagen, die erste Hinweise enthält und keinen Anspruch auf Vollständigkeit erhebt. Sie kann eine umfassende Prüfung und Beratung durch einen Rechtsanwalt/Steuerberater im Einzelfall nicht ersetzen.