INDUSTRIE- UND HANDELSKAMMER
Arnsberg, Hellweg-Sauerland
Königstr. 18 – 20, 59821 Arnsberg
Telefon: 02931/878149 – Fax: 02931/878147

Ein Merkblatt Ihrer Industrie- und Handelskammer

EU-Datenschutz-Grundverordnung – Dokumentationspflichten

Stand: August 2017

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 finden Sie im Merkblatt zur Einwilligung.

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 im Merkblatt zu Betroffenenrechten)
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

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

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, 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

Hinweis:
Dieses Merkblatt soll – als Service Ihrer IHK – nur erste Hinweise geben und erhebt daher keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.