Von: **Rechtsanwalt Marc Dimolaidis LL.M.**
Rechtsanwaltskanzlei Dimolaidis
Wilhelm-Dieß-Weg 13, 81927 München
Tel.: 089-92549895
E-Mail: md@dimolaidis.de
Web: www.dimolaidis.de

Stand: **03.07.2018**

Leitfaden zur DSGVO

Der Leitfaden orientiert sich in den Abschnitten 1. bis 6. an dem Fragebogen des Bayerischen Landesamts für Datenschutzaufsicht (nachstehend „LDA Bayern“) zur Datenschutzgrundverordnung (nachstehend „DSGVO“). Die Fragen aus dem Fragebogen sind im Leitfaden jeweils unterstrichen dargestellt.

Wichtige Hinweise:

Dieser Leitfaden soll **Kleinst- und kleineren** Unternehmen, insbesondere Online-Shops und sonstigen Internetportalen, eine Orientierung bei der Umsetzung grundlegender Vorgaben der DSGVO geben.

Der Leitfaden erhebt keinerlei Anspruch auf Vollständigkeit.

Abgesehen davon ist der Leitfaden **nicht geeignet für andere als Kleinst- und kleinere Unternehmen oder Unternehmen, bei denen der Datenschutz eine Sonderbehandlung erfordert** (bspw. beim Umgang mit besonderen Kategorien von Daten wie bspw. Gesundheitsdaten oder bei Profilbildung, bspw. für Scoring für Bonitätszwecke) nicht geeignet.

Inhalt

EINFÜHRUNG: Hinweise zur praktischen Umsetzung

Die große Herausforderung besteht im aktuellen Stadium wohl darin, aus den vielfältigen und häufig sehr allgemein formulierten Vorgaben der DSGVO abzuleiten, was konkret zu tun ist.

Das richtet sich natürlich in erster Linie nach inhaltlichen Kriterien wie der Art der personenbezogenen Daten und den Zwecken der Verarbeitung durch das betreffende Unternehmen. In praktischer Hinsicht stellt sich allerdings gerade für Kleinst- und kleinere Unternehmen angesichts des hohen Aufwands die Frage, in welchem Umfang und in welchem Detail die diversen Empfehlungen zur Erfüllung der Vorgaben der DSGVO in ihrem Falle umzusetzen sind.

Sofern der Datenschutz bei einem Unternehmen keine Sonderbehandlung erfordert (was insbesondere immer dann der Fall ist, wenn – unabhängig von er Anzahl der mit der Datenverarbeitung beschäftigten Mitarbeiter – einer der sonstigen Tatbestände vorliegt, die zur Benennung eines Datenschutzbeauftragten verpflichten), **könnten bei der Umsetzung der DSGVO in Kleinst- und kleineren Unternehmen insbesondere folgende Vereinfachungen in Betracht gezogen werden**:

• Kleinstunternehmen:

Kleinstunternehmen könnten sich dem Umfang nach an folgender Zusammenfassung orientieren, wie sie das LDA Bayern für kleinere Unternehmen – u.a. für (kleinere) Online-Shops - herausgegeben hat. Die Umsetzung der dort aufgeführten Anforderungen sollte dokumentiert werden, bspw. die interne Maßgabe zur Löschung von Daten, soweit es sich bei der betreffenden Maßnahme nicht ohnehin um eine Dokumentation handelt (bspw. das Verarbeitungsverzeichnis). Weitergehende Anforderungen, wie sie aus dem Fragebogen des LDA Bayern hervorgehen (die Fragen sind im Leitfaden durch Unterstreichung gekennzeichnet), können Kleinstunternehmen wohl außen vor lassen (auch wenn die o.g. Zusammenfassung des LDA Bayern ausdrücklich keinen Anspruch auf Vollständigkeit erhebt). Das betrifft insbesondere die Aufstellung einer Datenschutzrichtlinie und eines – über die in der Zusammenfassung aufgestellten Anforderungen hinausgehenden - Datenschutzmanagementsystems.

> *Link zur o.g. Zusammenfassung der Pflichten, die sich dem LDA Bayern zufolge aus der DSGVO für Betreiber von kleineren Online-Shops ergeben:*
>
> *https://www.lda.bayern.de/media/muster_9_online-shop.pdf*
>
> *Auch für eine Reihe anderer Arten kleiner Unternehmen wie bspw. Handwerksbetriebe, Arztpraxen, Produktionsunternehmen etc. hält das LDA Bayern entsprechende Aufstellungen bereit:*
>
> *https://www.lda.bayern.de/de/kleine-unternehmen.html*

- Kleinere Unternehmen:

Kleinere Unternehmen könnten sich an den Anforderungen orientieren, wie sie mit dem Fragebogen des LDA Bayern abgefragt werden, der diesem Leitfaden zugrunde liegt (die Fragen sind im Leitfaden jeweils unterstrichen). Etwaige Anforderungen, die im Fragebogen nicht thematisiert werden, könnten sie dabei außen vor lassen. Bspw. ergibt sich aus dem Fragebogen nicht, welche Inhalte eine Datenschutzrichtlinie und/oder ein Datenschutzmanagementsystem konkret umfassen sollten; kleinere Unternehmen könnten daher beides sehr kurz halten bzw. eine (sinnvolle) Auswahl der möglichen Inhalte treffen.

> *Tipp: Als erste (allerdings unvollständige) Orientierung zu den Pflichten aus der DSGVO können die vorstehend unter „Kleinstunternehmen" verlinkten Zusammenfassungen des LDA Bayern herangezogen werden.*

- Mittlere und große Unternehmen:

Mittleren und großen Unternehmen wird man keine der vorstehend angesprochenen Erleichterungen bei der Umsetzung empfehlen können.

> *Tipp: Als erste (allerdings unvollständige) Orientierung zu den Pflichten aus der DSGVO können die vorstehend unter „Kleinstunternehmen" verlinkten Zusammenfassungen des LDA Bayern herangezogen werden.*

1. Struktur und Verantwortlichkeit im Unternehmen

1.1 Datenschutzmanagementsystem und Datenschutzrichtlinie

Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist, beispielsweise durch

- Vorhandensein einer Datenschutzrichtlinie und eines Datenschutzmanagementsystems?

Die Datenschutzgrundverordnung (DSGVO) verpflichtet Unternehmen an verschiedenen Stellen ein sog. Datenschutzmanagementsystem einzuführen. Nicht zuletzt, weil die Unternehmen nach Art. 5 Abs. 2 DSGVO einer umfassenden Nachweispflicht nachkommen müssen. Hinzu kommen zahlreiche Maßnahmen, die definiert, umgesetzt, dokumentiert und kontrolliert werden müssen. Eine Datenschutzrichtlinie dient dazu all diese Anforderungen, die die DSGVO stellt, unternehmensintern zu strukturieren und kann gleichzeitig als Nachweis für die Einhaltung der datenschutzrechtlichen Vorgaben dienen.

„**Datenschutzmanagementsystem**":

„Datenschutzmanagementsystem" meint vereinfacht gesagt die Planung, Steuerung, Kontrolle und Dokumentation des Datenschutzes im Unternehmen und betrifft damit letztlich sämtliche Maßnahmen, die das Unternehmen in Sachen Datenschutz ergreift.

Die insoweit erforderlichen Maßnahmen werden mit dem Fragebogen des LDA Bayern abgefragt und in diesem Leitfaden erläutert. Verschiedentlich werden auch Maßnahmen empfohlen, die im Fragebogen des LDA Bayern nicht angesprochen sind, so etwa Schulungen, ein Vertragsmanagement oder ein Qualitätsmanagementsystem, so bspw. hier:

> I*https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_9.pdf*

Zur Frage, ob und in welcher Weise der Verantwortliche sich auf eine Auswahl der allgemein empfohlenen Maßnahmen beschränken könnte, siehe die einführenden Hinweise zur praktischen Umsetzung am Anfang dieses Leitfadens.

Grundsätzlich empfiehlt es sich, die geplanten Maßnahmen zu dokumentieren, unter anderem im Hinblick darauf, dass der Verantwortliche gemäß Art. 5 Abs. 2 DSGVO nachweisen können muss, dass personenbezogene Daten im Einklang mit der DSGVO verarbeitet werden.

Zumindest teilweise erfolgt diese Dokumentation bereits durch sonstige erforderliche Unterlagen wie bspw. das Verzeichnis über Verarbeitungstätigkeiten oder Verträge zur Auftragsverarbeitung (dazu nachstehend jeweils ausführlicher).

Zur Frage, ob und in welchem Umfang eine weitergehende Dokumentation über das Datenschutzmanagementsystem erstellt werden sollte, siehe die einführenden Hinweise zur praktischen Umsetzung am Anfang dieses Leitfadens.

„**Datenschutzrichtlinie**“:

Sinn und Zweck einer Datenschutzrichtlinie (auch „Datenschutz-Policy“) ist es, den Mitarbeitern eine Orientierung über die datenschutzrechtlichen Anforderungen im Unternehmen zu geben.

Zur Frage, ob und in welchem Umfang eine Datenschutzrichtlinie erstellt werden sollte, siehe die einführenden Hinweise zur praktischen Umsetzung am Anfang dieses Leitfadens.

> *Ein Musterbeispiel für eine Datenschutzrichtlinie finden Sie hier:*
> *https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_8.pdf*

1.2 Datenschutzbeauftragter

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 gemäß Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde gemeldet?

Wenn die Kerntätigkeit des Unternehmens darin liegt, Verarbeitungsvorgänge vorzunehmen, die aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Beobachtung von betroffenen Personen oder die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten nach Art. 9 DSGVO, Daten nach Art. 10 DSGVO oder nach § 22 oder § 24 BDSG (neu) liegt, so ist ein betrieblicher Datenschutzbeauftragter zu bestimmen.

Nach § 38 BDSG (neu) ist ein Datenschutzbeauftragter außerdem in folgenden Fällen zu benennen:

- es werden in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (wobei der maßgebliche Personenkreis weit zu verstehen ist. Unerheblich ist die arbeitsrechtliche Stellung der mit der Verarbeitung befassten Personen. Ebenso unerheblich ist der Umfang ihrer Beschäftigung, sodass neben Voll- und Teilzeitbeschäftigten auch freie Mitarbeiter, Leiharbeitnehmer, Praktikanten, Volontäre und Auszubildende von der Regelung erfasst werden. Es kann sich um eine feste Besetzung oder auch um regelmäßig wechselnde Mitarbeiter handeln, solange die vorgegebene Anzahl insgesamt erreicht wird und es sich um eine auf gewisse Dauer angelegte Stelle handelt. Nicht einzubeziehen sind Urlaubsvertretungen, da der vertretene Mitarbeiter regelmäßig bereits berücksichtigt wird. Schwankungen von kurzer Dauer bleiben für die Ermittlung der regelmäßig mit der Verarbeitung von Daten beschäftigten Personen unberücksichtigt).oder

- es werden Verarbeitungen vorgenommen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen (dazu siehe auch weiter unten in dieser Unterlage) oder

- es werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung (das betrifft bspw. den Handel mit Adresslisten) oder für Zwecke der Markt- oder Meinungsforschung verarbeitet

Informationen zum betrieblichen Datenschutzbeauftragten finden Sie hier:
https://www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf

Informationen dazu, wann besondere Kategorien personenbezogener Daten vorliegen, finden Sie hier:
https://www.lda.bayern.de/media/dsk_kpnr_17_besondere_kategorien.pdf

1.3 Verantwortlichkeit im Unternehmen

Mehr Informationen zu Verantwortlichkeiten und Aufgaben innerhalb des Unternehmens finden Sie hier:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_2.pdf

2. Übersicht über Verarbeitungen

2.1 Verzeichnis über Verarbeitungstätigkeiten

Haben Sie ein Verzeichnis ihrer Verarbeitungstätigkeiten gemäß Art. 30 DSGVO?

- Wenn nein, warum nicht? Ist das dokumentiert?

Zum Nachweis der Einhaltung der DSGVO haben Verantwortliche und Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten zu führen.

Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern müssen unter den in Art. 30 Absatz 5 DSGVO näher bezeichneten weiteren Voraussetzungen kein Verzeichnis von Verarbeitungstätigkeiten führen, wenn sie nur gelegentlich personenbezogene Daten verarbeiten. Diese Ausnahme wird aber eher selten greifen, weil personenbezogene Daten häufig auf regelmäßiger Basis erfasst werden, bspw. Kunden- oder Beschäftigtendaten.

Die zuständige Aufsichtsbehörde kann eine Vorlage des Verarbeitungsverzeichnisses verlangen. Das Verarbeitungsverzeichnis muss deswegen in elektronischer oder gedruckter Form exportierbar sein. Art. 30 DSGVO enthält Vorgaben zum Inhalt und zu den formalen Anforderungen an das Verarbeitungsverzeichnis.

Allgemeine Informationen zum Verzeichnis ihrer Verarbeitungstätigkeiten finden Sie hier:
https://www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf

Muster des Bundes der deutschen Datenschutzbeauftragten finden Sie hier:

- *Für Verantwortliche: https://www.bvdnet.de/wp-content/uploads/2017/06/Muster_Verz_der_Verarbeitungstätigkeiten_Verantwortlicher.pdf*

- *Für Auftragsverarbeiter: https://www.bvdnet.de/wp-content/uploads/2017/06/Muster_Verz_der_Verarbeitungstätigkeiten_Auftragsverarbeiter.pdf*

- *Anlage technische und organisatorische Maßnahmen: https://www.bvdnet.de/wp-content/uploads/2017/06/Muster_Verz_der_Verarbeitungstätigkeiten_TOMs.pdf*

Hinweise zur Ausfüllung dieser Muster finden Sie hier: https://www.bvdnet.de/wp-content/uploads/2017/06/Hinweise_zum_VVT_Art_30_final.pdf

Ein Beispiel für ein Verarbeitungsverzeichnis speziell für Online-Shops finden Sie hier: https://www.lda.bayern.de/media/muster_9_online-shop_verzeichnis.pdf

2.2 Privacy by Design

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)

Privacy by Design meint datenschutzfreundliche Technikgestaltung. Der Verarbeiter personenbezogener Daten ist verpflichtet, technische und organisatorische Maßnahmen zur Einhaltung der Anforderungen der DSGVO einzuführen. Die Ausgestaltung dieser Maßnahmen unterliegt einem gewissen Beurteilungsspielraum, für den unter anderem der Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zweck der Datenverarbeitung sowie Eintrittswahrscheinlichkeit und Schwere möglicher Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen sind. Bei Einführung neuer Software im Unternehmen ist also beispielsweise darauf zu achten, dass sie nur solche Daten erhebt, die für die jeweiligen Verarbeitungszwecke erforderlich sind. Diese Vorschrift wird ergänzt durch den Grundsatz der Privacy by Default, also Datenschutz durch datenschutzfreundliche Voreinstellungen, der bestimmt, dass der Verantwortliche auch durch Voreinstellungen in technischen Verfahren sicherzustellen hat, dass grundsätzlich nur Daten verarbeitet werden, deren Verarbeitung für den jeweiligen Verarbeitungszweck erforderlich sind.

3. Zusammenarbeit mit anderen Unternehmen

3.1 Gemeinsame Verantwortlichkeit

Gemeinsam Verantwortliche: Gemäß Art. 26 Abs. 1 DSGVO sind mehrere Stellen „gemeinsam für die Verarbeitung Verantwortliche“, wenn sie gemeinsam die Zwecke der Verarbeitung und die Mittel zur Verarbeitung festlegen. Dies kann bspw. der Fall sein beim gemeinsamen Betrieb einer IT-Plattform, die von mehreren Unternehmen für unterschiedliche eigene Zwecke betrieben wird, oder bei einer Marktforschung durch unterschiedliche Beteiligte, die jeweils in Teilbereichen Entscheidungen über die Verarbeitung treffen.

Verpflichtungen: Gemeinsam Verantwortliche müssen eine Vereinbarung abschließen, in der sie transparent festlegen, wer von ihnen welche in der DSGVO geregelten Verpflichtungen erfüllt.

Abgrenzung: Abzugrenzen ist die gemeinsame Verantwortlichkeit insbesondere von der Auftragsverarbeitung nach Art. 28 DSGVO (dazu nachstehend ausführlicher), und von einer Übermittlung personenbezogener Daten an einen anderen Verantwortlichen. In diesen Fällen werden die Zwecke und Mittel der Verarbeitung nicht gemeinsam festlegt.

Informationen zu gemeinsam Verantwortlichen finden Sie hier: https://www.lda.bayern.de/media/dsk_kpnr_16_gemeinsam_verantwortliche.pdf

3.2 Auftragsverarbeiter

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?

Wie auch nach dem bisher geltenden BDSG (alt) legt auch die DSGVO Sonderregelungen für die Verarbeitung von personenbezogenen Daten im Auftrag fest. Grundsätzlich wird dem Verantwortlichen die Verarbeitung durch Auftragsverarbeiter zugerechnet. Die Art. 28 bis 30 DSGVO enthalten Regelungen zur Auftragsverarbeitung. Der Verantwortliche wird dort unter anderem verpflichtet, den Auftragsverarbeiter gemäß Art. 28 Abs. 3 DSGVO auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments mit der Verarbeitung zu beauftragen.

Informationen zur Auftragsverarbeitung finden Sie hier:
https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

Für einen Mustervertrag zur Auftragsverarbeitung geben Sie folgende Zeile in Google ein und klicken Sie auf das erste Ergebnis:
Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO – GDD

Außerdem ist gemäß Art. 30 DSGVO auch über die Auftragsverarbeitung in der Regel ein Verzeichnis über Verarbeitungstätigkeiten zu führen (hierzu s.o. im Abschnitt zum Verarbeitungsverzeichnis).

4. Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte

Die DSGVO geht mit einer bewussten Stärkung der Betroffenenrechte einher. Eine wesentliche Neuerung der DSGVO sind neben einem strengeren Haftungsregime und den neuen Einzelansprüchen Betroffener vor allem auch die erweiterten Transparenzpflichten bei der Verarbeitung von Daten.

4.1 Datenschutzerklärung

Die Datenschutzerklärung ist nach der DSGVO deutlich umfangreicher zu gestalten als zuvor.

Haben Sie ihre Texte zur datenschutzrechtlichen Information der betroffenen Person bei der Datenerhebung an die Anforderungen nach Art. 13 und 14 DSGVO angepasst?

- Wenn nein, warum nicht?

Haben Sie insbesondere folgende Informationen neu aufgenommen, sofern nicht bereits vorher enthalten:

- Kontaktdaten des Datenschutzbeauftragten
- Rechtsgrundlagen für die Verarbeitung personenbezogener Daten
- Falls Sie die Verarbeitung mit ihren berechtigten Interessen oder berechtigten Interessen eines Dritten begründen: die jeweiligen 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 der besonderen Situation einer betroffenen Person sowie auf Datenportabilität
- Sofern die 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 stammen die personenbezogenen Daten und ggf., ob sie aus öffentlichen Quellen stammen

Hier geht es um die einzelnen Inhalte, die eine Datenschutzerklärung nach der DSGVO enthalten muss.

Zu den Informationspflichten finden Sie hier weitere Informationen:
https://www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf

Zur Erstellung einer für Ihre Online-Präsenz geeigneten Vorlage für Ihre Datenschutzerklärung wenden Sie sich gerne an die Kanzlei Dimolaidis (www.dimolaidis.de).

4.2 Werbe-Einwilligung

Haben Sie ihre Werbe-Einwilligungserklärung für Kunden, Interessenten usw., an die Anforderungen von Art. 7 und 13 DSGVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?

Für die Ausgestaltung der Werbe-Einwilligung ändert sich durch die DSGVO nicht viel. Zuvor (rechtskonform) eingeholte Einwilligungen haben auch weiterhin Geltung. Eine Neuerung ist, dass der Widerruf so einfach sein muss wie die Erteilung der Einwilligung; dieser Anforderung genügt bei einem Newsletter bspw. ein Abmeldelink.

Hier finden Sie weitere Informationen zur Einwilligung:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_13.pdf

4.3 Auskunft an Betroffene

Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DSGVO zeitnah und vollständig erfüllen zu können (Art. 12 DSGVO)?

4.4 Datenübertragbarkeit

Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art. 20 DSGVO)?

5. Verantwortlichkeit, Umgang mit Risiken

5.1 Nachweis rechtmäßiger Verarbeitung

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 DSGVO)?

Zu dieser Anforderung siehe oben Ziffer 1.1. zum Datenschutzmanagementsystem.

5.2 Löschung von Daten

Mit vorstehender Frage wird auch das Erfordernis von Löschregeln angesprochen, d.h. es sollte dokumentiert werden, welche personenbezogenen Daten innerhalb welcher Fristen gelöscht werden.

Dieser Punkt sollte in das Verzeichnis über Verarbeitungstätigkeiten aufgenommen werden. Weitere Informationen zu den Löschregeln finden Sie in den Links zum Abschnitt über das Verzeichnis für Verarbeitungstätigkeiten.

5.3 Datenschutzeinwilligungen

Haben Sie geprüft, ob die Einwilligungen, auf die Sie eine Verarbeitung stützen, noch den Voraussetzungen der Art. 7 und/oder 8 DSGVO entsprechen?

Können Sie das Vorliegen einer Einwilligung nachweisen?

5.4 Technische und organisatorische Maßnahmen

Haben Sie ein Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass ihre Verarbeitung gemäß der DSGVO erfolgt (Art. 24 Abs. 1 DSGVO)?

Informationen bzw. Links zum Datenschutzmanagementsystem finden Sie in Ziffer 1.

Haben Sie ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 DSGVO 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?

Art. 32 DSGVO legt fest, dass technische und organisatorische Maßnahmen zu implementieren sind, die ein angemessenes Schutzniveau der jeweiligen personenbezogenen Daten sicherstellen. Diese Maßnahmen müssen laut Art. 32 DSGVO unter Berücksichtigung des Risikos für die Rechte und

Freiheiten natürlicher Personen ausgewählt werden.

> *Die technischen und organisatorischen Maßnahmen werden in das Verzeichnis über Verarbeitungstätigkeiten aufgenommen. Informationen zu den technischen und organisatorischen Maßnahmen finden Sie in den Unterlagen, die im Abschnitt zum Verzeichnis über Verarbeitungstätigkeiten (Ziffer 2.1.) verlinkt sind.*

5.5 Verpflichtung auf Vertraulichkeit

Weiter mit Bezug zur vorstehenden Frage:

Das bisherige deutsche Datenschutzrecht sah eine sog. "Verpflichtung auf das Datengeheimnis" vor. Die DSGVO schreibt eine solche Verpflichtung nicht mehr für alle Fälle vor. Im Rahmen der Dokumentations- und Nachweispflichten des Art. 5 Abs. 2 DSGVO ist die Verpflichtung der zur Verarbeitung befugten Person jedoch weiterhin ein angemessenes Mittel zur Gewährleistung der datenschutzrechtlichen Verpflichtungen.

Nähere Informationen zur Verpflichtung auf Vertraulichkeit:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_11.pdf

Muster für eine Vertraulichkeitsvereinbarung:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_11.pdf

5.6 Datenschutzfolgenabschätzung

Die DSGVO schreibt in Art. 35 für bestimmte Fälle wie bspw. Profiling oder eine umfangreiche Verarbeitung besonders sensibler Daten (bspw. Gesundheitsdaten) eine Datenschutz-Folgenabschätzung vor. Die Datenschutz-Folgenabschätzung ist ein Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Ob eine solche Datenschutz-Folgenabschätzung durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der jeweiligen Verarbeitungsvorgänge.

Haben Sie sich auf die eventuelle Notwendigkeit der Durchführung einer Datenschutzfolgenabschätzung 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?

Weitere Informationen zur Datenschutz-Folgenabschätzung finden Sie unter folgendem Link:
https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf

6. Datenschutzverletzungen

Art. 33 und 34 DSGVO regeln den Umgang mit "Datenpannen". Dort ist festgelegt, dass grundsätzlich jede Verletzung des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde gemeldet werden muss, sofern die Verletzung voraussichtlich nicht zu einem Risiko für die betroffene Person führt.

Haben Sie gemäß Art. 33 DSGVO 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?

Mehr Informationen zum Umgang mit Datenschutzverletzungen finden Sie hier:
https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

7. Übermittlung von Daten in Drittländer

Die Übermittlung von Daten in Drittländer ist in den Artikeln 44 bis 49 der DSGVO geregelt. Als Drittländer werden Länder außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums (EU-Länder plus Island, Liechtenstein und Norwegen) bezeichnet. Die Prüfung, ob eine Übermittlung an ein Drittland zulässig ist, erfolgt zweistufig. Zunächst müssen für solche Übermittlungen natürlich alle generellen Anforderungen, die die DSGVO für Datenverarbeitungen vorsieht, eingehalten werden. Zudem müssen die in Art. 45 ff. DSGVO normierten spezifischen Anforderungen an die Übermittlung in Drittländer eingehalten werden.

Für nichtöffentliche Stellen sieht die DSGVO drei Möglichkeiten für Datenübermittlungen in Drittländer vor: Die Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses der EU-Kommission nach Art. 45 DSGVO, die Datenübermittlung auf Grundlage geeigneter Garantien nach Art. 46 DSGVO und in den Ausnahmefällen des Artikel 49 DSGVO (bspw. dann, wenn die Übermittlung für die Erfüllung eines Vertrages zwischen dem Verantwortlichen und dem Betroffenen erforderlich ist) .

7.1 Angemessenheitsbeschluss der EU-Kommission

Wenn in einem Drittland ein mit der DSGVO vergleichbares Niveau im Bereich des Datenschutzes besteht, kann die EU-Kommission die Angemessenheit des Datenschutzniveaus für dieses Land (der Beschluss kann aber auch auf ein bestimmtes Gebiet, einen bestimmten Sektor oder auf bestimmte Datenkategorien beschränkt sein) feststellen. Liegt ein solcher Angemessenheitsbeschluss vor, können Daten ohne weitere Genehmigung an das entsprechende Drittland übermittelt werden.

Ein solcher Angemessenheitsbeschluss wurde bislang von der EU-Kommission für folgende Länder gefasst (Stand 3.7.2018; der jeweils aktuelle Stand kann hier abgerufen werden):

- Andorra
- Argentinien
- Kanada
- Färöer Inseln
- Guernsey
- Israel
- Isle of Man
- Jersey
- Neuseeland
- Schweiz
- Uruguay

- USA

:

In Verhandlung:

- Japan
- Südkorea

7.2 Datenübermittlung auf Grundlage geeigneter Garantien

Bei der Datenübermittlung auf Grundlage geeigneter Garantien hat der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien zur Gewährleistung eines angemessenen Datenschutzniveaus vorzusehen. Als geeignete Garantien gelten verbindliche interne Datenschutzvorschriften (innerhalb einer Gruppe von Unternehmen), deren Mindestinhalt Art. 47 Abs. 2 DSGVO festschreibt, die Standarddatenschutzklauseln der EU-Kommission oder einer Aufsichtsbehörde nach Art. 46 Abs. 2 c) und d) DSGVO, genehmigte Verhaltensregeln und genehmigte Zertifizierungsmechanismen nach Art. 46 Abs. 2 e) und f) DSGVO sowie einzeln ausgehandelte Vertragsklauseln nach Art. 46 Abs. 3 DSGVO.

7.3 Ausnahmetatbestände nach Art. 49 DSGVO

Daneben sind in Art. 49 DSGVO verschiedene Ausnahmetatbestände normiert, die eine Übermittlung von Daten an Drittländer erlauben, wenn kein Angemessenheitsbeschluss und keine geeignete Garantie vorliegt. Dazu gehören die Einwilligung der betroffenen Person (Art. 49 Abs. 1 UAbs. 1 lit. a)), die Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 UAbs. 1 lit. b) und c)), wichtige Gründe des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 lit. d)), die Verfolgung von Rechtsansprüchen (Art. 49 Abs. 1 UAbs. 1 lit. e)) der Schutz lebenswichtiger Interessen (Art. 49 Abs. 1 UAbs. 1 lit. f)), und die Wahrung zwingender berechtigter Interessen (Art. 49 Abs. 1 UAbs. 2 S. 1).

7.4 Weiterführende Informationen

Hier finden Sie weitere Informationen zur Übermittlung von Daten in Drittländer:

https://www.lda.bayern.de/media/dsk_kpnr_4_drittlaender.pdf

8. Besondere Kategorien von Daten (bspw. Gesundheitsdaten)

8.1 Was sind besondere Kategorien personenbezogener Daten?

Besondere Kategorien personenbezogener Daten sind solche, die eines besonderen Schutzes bedürfen. Zu den besonderen Kategorien von Daten gehören nach Art. 9 Abs. 1 DSGVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

8.2 Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten

Grundsätzlich ist eine Verarbeitung besonderer Kategorien von Daten untersagt. Allerdings sieht Art. 9 Abs. 2 DSGVO folgende Ausnahmen von diesem Verbot der Verarbeitung vor:

8.2.1 Ausdrückliche Einwilligung

So ist nach Art. 9 Abs. 2 a) DSGVO eine Verarbeitung besonderer Kategorien personenbezogener Daten nach ausdrücklicher Einwilligung der betroffenen Person erlaubt. Aufgrund der besonderen Schutzbedürftigkeit besonderer Kategorien von Daten muss die Einwilligung „ausdrücklich" sein. Das bedeutet jedenfalls, dass die Einwilligung nicht stillschweigend, etwa durch bereits angekreuzte Kästchen oder durch Untätigkeit erfolgen kann, sondern eine eindeutige, bestätigende Handlung verlangt wird. Darüber hinaus ist ein hohes Maß an Bestimmtheit hinsichtlich der Nennung der betroffenen Daten und des Verwendungszwecks erforderlich.

8.2.2 Sonstige Rechtfertigungsgründe

In Art. 9 Abs. 2 Abs. b) bis j) DSGVO sind weitere Rechtfertigungsgründe aufgeführt bei deren Vorliegen besondere Kategorien von Daten ausnahmsweise verarbeitet werden dürfen, bspw. wenn der Betroffene die Daten offensichtlich öffentlich gemacht hat, oder wenn die Verarbeitung zur Geltendmachung von Rechtsansprüchen erforderlich ist, oder wenn die Verarbeitung zur Gesundheitsvorsorge erforderlich ist und unter der Verantwortung beruflich zur Verschwiegenheit verpflichteten Fachpersonals erfolgt, etc.

Zusätzlich müssen natürlich auch alle anderen Vorschriften der DSGVO, die die Verarbeitung von Daten betreffen, eingehalten werden.

8.3 Was ist bei besonderen Kategorien personenbezogener Daten sonst zu beachten?

Bei der Verarbeitung besonderer Kategorien personenbezogener Daten sind alle einschlägigen Vorschriften der DSGVO, insbesondere die allgemeinen Rechtmäßigkeitsanforderungen an Datenverarbeitungen aus Art. 6 DSGVO, einzuhalten. Zusätzlich müssen die spezifischeren Anforderungen, die Art. 9 DSGVO aufstellt, beachtet werden.

Die DSGVO knüpft außerdem über Art. 9 DSGVO hinaus an verschiedenen Stellen an den Begriff der besonderen Kategorien personenbezogener Daten an. So muss nach Art. 6 Abs. 4 c) DSGVO bei der Zweckänderung berücksichtigt werden, ob besondere Kategorien personenbezogener Daten verarbeitet werden. Art. 22 Abs. 4 DSGVO schließt automatisierte Entscheidungen im Einzelfall einschließlich Profiling bei besonderen Kategorien personenbezogener Daten grundsätzlich aus. Nach Art. 27 Abs. 1 a) DSGVO kann bei der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten keine Freistellung von der Pflicht zur Bestellung eines Vertreters für nicht in der Union niedergelassene Verantwortliche und Auftragsverarbeiter erfolgen. Auch eine Freistellung von der Dokumentationspflicht wird nach Art. 30 Abs. 5 DSGVO ausgeschlossen, wenn besondere Kategorien personenbezogener Daten verarbeitet werden. Art. 35 Abs. 3 b) DSGVO schreibt weiterhin vor, dass bei umfangreicher Verarbeitung besonderer Kategorien von Daten immer eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Außerdem besteht nach Art. 37 Abs. 1 c) DSGVO die Pflicht einen Datenschutzbeauftragten zu benennen, wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten liegt.

8.4 Weiterführende Informationen

Weitere Informationen zu besonderen Kategorien von Daten finden Sie hier:

https://www.lda.bayern.de/media/dsk_kpnr_17_besondere_kategorien.pdf