Datenschutzkonzept der *Gesellschaft*

Wodianka
privacy
legal

Inhaltsverzeichnis

Präambel ... **3**

1. Geltungsbereich des Datenschutzkonzeptes ... **4**

2. Datenschutzorganisation ... **4**

2.1 Verantwortlichkeit ... *4*

2.2 Datenschutzbeauftragter ... *4*

2.3 Ansprechpartner/ Koordinator ... *5*

3. Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten ... **5**

3.1 Rechtmäßigkeit ... *5*

3.2 Zweckbindung ... *5*

3.3 Informationspflicht/ Transparenz ... *6*

3.4 Datenminimierung ... *6*

3.5 Privacy by Design & Privacy by Default ... *6*

3.6 Löschung ... *6*

4. Dokumentation von Datenverarbeitungstätigkeiten ... **7**

5. Informationssicherheit ... **7**

6. Umgang mit den Rechten der betroffenen Person ... **7**

6.1 Auskunftserteilung ... *8*

6.2 Berichtigung von Daten und Widerspruch gegen die Datenverarbeitung ... *8*

6.3 Löschung und Sperrung von Daten ... *8*

6.4 Übertragbarkeit von personenbezogenen Daten ... *8*

7. Mitarbeiterdatenschutz ... **9**

8. Kundendatenschutz ... **9**

9. Datenverarbeitung außerhalb der *Gesellschaft* ... **9**

9.1 Auftragsdatenverarbeitung ... *10*

9.2 Gemeinsame Verantwortlichkeit ... *10*

10. Umgang mit Datenschutzverletzungen ... **11**

11. Datenschutzfolgenabschätzung und Transfer-Impact-Assessment ... **11**

12. Online-Präsenz der *Gesellschaft* ... **12**

13. Videoüberwachung ... **13**

14. Überwachung und Fortschreibung des Datenschutzkonzeptes ... **13**

Präambel

Dieses Datenschutzkonzept ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten bei *Gesellschaft*.

Mit diesem Datenschutzkonzept sollen die Persönlichkeitsrechte von Betroffenen (u.a. Mitarbeiter, Kunden und Lieferanten) nach den Vorgaben der EU-Datenschutzgrundverordnung (DSGVO) sowie lokal geltenden Datenschutzgesetzen gewahrt und geschützt werden.

Das Datenschutzkonzept muss für alle Beschäftigten und leitenden Angestellten verbindlich und jederzeit leicht zugänglich sein.

1. Geltungsbereich des Datenschutzkonzeptes

Dieses Konzept hat Geltung für *Gesellschaft* an allen Standorten. Sie gilt persönlich für alle beschäftigten sowie leitenden Angestellten der Standorte.

Die Gebote und Verbote dieses Datenschutzkonzeptes gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob diese elektronisch oder in Papierform verarbeitet werden.

Kundendaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Hierzu zählen beispielsweise der Name eines Ansprechpartners und seine persönliche E-Mail-Adresse. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so. z.B. beim Autokennzeichen/ Halter. Auch Fotos, Video- oder Tonaufnahmen können Personen identifizieren und somit dem Schutzbereich des Datenschutzes unterfallen.

2. Datenschutzorganisation

2.1 Verantwortlichkeit

Verantwortlicher nach Art. 4 Nr. 7 DSGVO ist die

Anschrift

2.2 Datenschutzbeauftragter

Die *Unternehmen* hat einen Datenschutzbeauftragten nach Maßgabe der gesetzlichen Bestimmungen der europäischen Datenschutzgrundverordnung und der lokal geltenden Gesetze bestellt. Entsprechende Nachweise zur Bestellung (z.B. Meldebestätigung Aufsichtsbehörde, Bestellungsurkunde) sind der **Anlage 1** zu entnehmen.

Als externer Datenschutzbeauftragter ist gem. Art. 37 DSGVO bestellt:

Name + Anschrift

Der DSB nimmt dabei seine gesetzlich festgelegten Pflichten war, insbesondere

- das Hinwirken auf die Einhaltung der DSGVO und anderer Vorschriften über den Datenschutz,
- die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungs-programme, mit deren Hilfe personenbezogene Daten verarbeitet werden,
- die Schulung und das Vertraut machen von mit der Verarbeitung personenbezogener Daten beschäftigten Personen hinsichtlich der relevanten Datenschutzvorschriften,
- die Unterstützung bei der erforderlichen Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO,
- die Unterstützung der *Gesellschaft* bei der Erstellung der internen Verarbeitungsübersicht nach Art. 30 DSGVO,

- die Informationsvermittlung an die *Gesellschaft*, z.B. über Gesetzesnovellen, EU-Richtlinien und Verordnungen sowie Rechtsprechung zu datenschutzrechtlich relevanten Themen.

Der Datenschutzbeauftragte wird zudem die Einhaltung der gebotenen technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus überwachen. Er ist stets der Leitung der *Gesellschaft* unterstellt und berichtet an diese. Bezüglich der Ausübung seiner Fachkunde ist er weisungsfrei. Von der besonderen Verschwiegenheitsverpflichtung über ihm zur Kenntnis gelangten Tatsachen, die Rückschlüsse auf einen Betroffenen zulassen, kann er nur vom Betroffenen entbunden werden.

Bei der Erfüllung seiner Aufgabe ist der betriebliche Datenschutzbeauftragte von allen Organisationseinheiten zu unterstützen. Soweit sie personenbezogene Daten verarbeiten, können die Mitarbeiter bei der Einführung neuer Verfahren oder Änderungen bestehender Verfahren sowie bei der Erarbeitung unternehmensinterner Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten den Datenschutzbeauftragten nach Bedarf frühzeitig beteiligen. Alle Mitarbeiter können sich jederzeit vertraulich in Angelegenheiten des Datenschutzes an die betrieblichen Datenschutzbeauftragten wenden.

2.3 Ansprechpartner/ Koordinator

Innerhalb des Unternehmens wurden einzelne oder mehrere Ansprechpartner und/oder Koordinatoren für das Thema Datenschutz bestimmt. Ansprechpartner und/ oder Koordinator für den Datenschutz bei der *Gesellschaft* ist/ sind

Name + Kontaktdaten

3. Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten sind auf rechtmäßige Weise nach Treu und Glauben zu verarbeiten. Die Verarbeitung muss dabei stets in einer für die betroffene Person nachvollziehbaren Weise stattfinden.

3.1 Rechtmäßigkeit

Die Verarbeitung von personenbezogenen Daten ist grundsätzlich unzulässig. Einzig eine in Art. 6 DSGVO oder in einer anderen gesetzlichen Vorschrift genannte Bedingung kann die Verarbeitung der personenbezogenen Daten rechtfertigen.

3.2 Zweckbindung

Personenbezogene Daten dürfen nur für den legitimen Zweck verarbeitet werden, welcher vor der Datenerhebung definiert wurde.

Nachträgliche Änderungen des Zwecks der Verarbeitung sind nur zulässig, wenn die Verarbeitung mit dem Zweck, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar sind.

3.3 Informationspflicht/ Transparenz

Die betroffene Person ist nach Art. 13 und 14 DSGVO über diesbezügliche Datenverarbeitung zu informieren. Die Information erfolgt gemäß Art. 12 Abs. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Diese Information muss grundsätzlich zum Zeitpunkt der ersten Erhebung der personenbezogenen Daten erfolgen. Dabei ist zu beachten, dass diese der Betroffenen ohne Aufforderung zur Verfügung gestellt werden muss.
Eine individualisierbare Datenschutzinformation ist der **Anlage 2** zu entnehmen.

Kommentiert [LP|Wpl1]: Erstellen und anfügen

3.4 Datenminimierung

Jede Verarbeitung personenbezogener Daten muss so gestaltet sein, dass sie auf das, für die Erreichung des Zweckes, erforderliche Maß beschränkt ist. Dies ist bereits beim Umfang der Datenerhebung zu berücksichtigen.
Sofern es der Zweck, für die die personenbezogenen Daten erhoben wurden, zulässt und der Aufwand angemessen ist, sind vorzugsweise anonymisierte Daten zu verwenden.

3.5 Privacy by Design & Privacy by Default

Der Grundsatz Datenschutz durch Technikgestaltung („Privacy by Design“) nach Art. 25 Abs. 1 DSGVO zielt bereits im Entwicklungsstadium von Projekten auf die Berücksichtigung des Datenschutzes durch technische und organisatorische Maßnahmen ab. Dieses Prinzip beschränkt sich nicht nur auf Software- oder Hardwareentwicklung, sondern kann beispielsweise auch bei der Gestaltung unserer Webseite oder anderweitiger Projekte relevant sein.

Durch die Einhaltung des Grundsatzes der datenschutzfreundlichen Voreinstellungen („Privacy by Default“) nach Art. 25 Abs. 2 DSGVO soll sichergestellt werden, dass lediglich die zur Zweckerreichung erforderlichen personenbezogenen Daten verarbeitet werden. Dies umfasst neben dem Verarbeitungsvorgang ebenso die Speicherdauer und die Zugänglichkeit der personenbezogenen Daten.

3.6 Löschung

Personenbezogene Daten dürfen gemäß Art. 5 Abs. 1 lit. b DSGVO nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Entfallen diese Zwecke, sind die Daten entsprechend zu löschen. Sofern Daten gesetzlichen Aufbewahrungsfristen unterliegen, welche sodann eine neue Zweckbindung darstellen, sind die Daten entsprechend nach diesen Fristen zu löschen bzw. zu vernichten.

Das Löschkonzept der *Gesellschaft*, welches **Anlage 3** zu entnehmen ist, erläutert die Grundlagen einer datenschutzrechtlichen Löschung bzw. Sperrung und zeigt auf, wie eine Löschung bzw. eine Sperrung in der Praxis umzusetzen ist. Die konkreten Löschregeln und Löschfristen sind in der Löschmatrix der *Gesellschaft* enthalten (siehe **Anlage 4)**, für dessen Verwendung zusätzlich eine Erläuterung (hierzu **Anlage 5**) existiert.

4. Dokumentation von Datenverarbeitungstätigkeiten

Die Verfahren, in denen personenbezogene Daten verarbeitet werden, werden in einem Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO dokumentiert.
Dieses Verfahrensverzeichnis ist der **Anlage 6** zu entnehmen und wird regelmäßig fortgeschrieben.

5. Informationssicherheit

Die Verarbeitung personenbezogener Daten kann stets ein Risiko für die Rechte und Freiheiten der betroffenen Person mit sich bringen. Die Sicherheit der Verarbeitung sollte daher in jedem Fall hohe Priorität haben. Gemäß Art. 32 DSGVO sind daher im Zuge der Verarbeitung von personenbezogenen Daten technische und organisatorische Maßnahmen zu treffen, die diese Sicherheit garantieren. Die Auswahl der Maßnahmen orientiert sich dabei gem. Art. 32 Abs. 1 an dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang und dem Zweck der Verarbeitung, sowie den daraus resultierenden Risiken und deren Eintrittswahrscheinlichkeiten. Besonders die folgenden Aspekte sollten durch diese Maßnahmen abgedeckt sein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die bei der *Gesellschaft* implementierten technischen und organisatorischen Maßnahmen sind der **Anlage 7** zu entnehmen.

6. Umgang mit den Rechten der betroffenen Person

Gemäß Kapitel 3 der Datenschutzgrundverordnung hat die betroffene Person gegenüber dem Verantwortlichen verschiedene Rechte. Anfragen und Beschwerden, die sich auf diese Rechte beziehen, müssen innerhalb von einem Monat beantwortet werden. Unter Berücksichtigung der Komplexität und der Anzahl der Anträge kann dieser Zeitraum höchstens um zwei weitere Monate verlängert werden, worüber der Betroffene entsprechend unterrichtet werden muss.

Die Beschäftigten der *Gesellschaft* erhalten ein Merkblatt zum Umgang mit den Betroffenenrechten, welches der **Anlage 8** entnommen werden kann. Darüber hinaus existieren eine Vorlage eines Auskunftsschreibens an die auskunftsersuchende Person sowie eine Vorlage einer Stellungnahme an die Aufsichtsbehörde, welche in **Anlage 9** und **Anlage 10** zu finden sind.

Die Kommunikation mit auskunftsersuchenden Personen und ggf. mit der Aufsichtsbehörde erfolgt, in Absprache mit dem Verantwortlichen, durch den Datenschutzbeauftragten.

6.1 Auskunftserteilung

Betroffene haben gem. Art. 15 DSGVO das Recht auf Auskunft über die, über ihre Person gespeicherten personenbezogene Daten.

Die Auskunftserteilung erfolgt auf schriftlichem Weg und beinhaltet, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten sowie den Zweck der Speicherung. Als Vorlage dient das in **Anlage 9** zu findende Dokument.

Bei der Bearbeitung von Betroffenenersuchen ist die Identität des Betroffenen zweifelsfrei festzustellen. Hierzu sind Authentifizierungsprozesse zu wählen, die dem Schutzbedarf der angefragten Daten entsprechen.

6.2 Berichtigung von Daten und Widerspruch gegen die Datenverarbeitung

Zudem haben betroffene Personen gem. Art. 16 DSGVO einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen.

Widerspricht der Betroffene gem. Art. 21 DSGVO der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung, ist eine weitere Verarbeitung oder Nutzung für diese Zwecke unzulässig.

6.3 Löschung und Sperrung von Daten

Mit Betroffenenanfragen gehen oftmals Löschersuchen gem. Art. 17 DSGVO einher. Ergänzend zu der Ziffer 3.6 sind personenbezogene Daten unter den folgenden Voraussetzungen zu löschen:

- Ihre Speicherung ist unzulässig, oder
- es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann, oder
- die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht länger erforderlich.

An die Stelle einer Löschung kann eine Sperrung von Daten gem. Art. 18 DSGVO treten, wenn

- eine Kenntnis der Daten für die Erfüllung des Zwecks der Speicherung zwar nicht länger erforderlich ist, jedoch gesetzlich, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, oder
- schutzwürdige Interessen der Betroffenen beeinträchtigt würden, oder
- eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist,
- oder die Richtigkeit der personenbezogenen Daten zum aktuellen Zeitpunkt bestritten wird.

6.4 Übertragbarkeit von personenbezogenen Daten

Die betroffene Person hat gem. Art. 20 DSGVO außerdem das Recht auf sogenannte Datenübertragbarkeit. Sie kann demnach von dem Verantwortlichen verlangen, dass dieser ihr die bereitgestellten personenbezogenen Daten in einer strukturierten, gängigen und

maschinenlesbaren Form zur Verfügung stellt. Auch eine Übermittlung von der *Gesellschaft* als bisherigen Verantwortlichen an einen neuen/anderen Verantwortlichen ist möglich.

7. Mitarbeiterdatenschutz

Ein Mitarbeiter ist aus datenschutzrechtlicher Sicht zweifach befangen. Zum einen verarbeitet er während seiner Tätigkeit bei der *Gesellschaft* selbst personenbezogene Daten von Kunden o.ä. und zum anderen werden im Rahmen des Beschäftigtenverhältnisses die personenbezogenen Daten des Mitarbeiters von der *Gesellschaft* verarbeitet.

Mit Beginn des Beschäftigungsverhältnisses erhält jeder Mitarbeiter die entsprechend dafür vorliegende Datenschutzinformation. Dort erhält der Mitarbeiter alle notwendigen Informationen zur Verarbeitung seiner personenbezogenen Daten. Die Datenschutzinformation können Sie der **Anlage 11** entnehmen.

Mit Beginn des Beschäftigungsverhältnisses wird der Mitarbeiter außerdem zur Vertraulichkeit verpflichtet. Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung des Arbeitsverhältnisses fort. Das Muster für das Verpflichtungsschreiben ist **Anlage 12** zu entnehmen.

Beschäftigte, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Die Vorgaben des Datenschutzbeauftragten über Form und Turnus der entsprechenden Schulung sind zu berücksichtigen. Die aktuelle Schulungspräsentation ist der **Anlage 13** zu entnehmen.

8. Kundendatenschutz

Kommentiert [LP|Wpl2]: Noch auszuführen

In Abhängigkeit des Geschäftsmodells der *Gesellschaft* werden auch personenbezogene Daten der jeweiligen Kunden verarbeitet. Während es sich im B2B Bereich überwiegend um die Daten der jeweiligen Ansprechpartner handelt, werden im B2C Bereich Daten der Endverbraucher verarbeitet.

Auch in diesem Fall müssen die Informationen nach Art. 13 DSGVO bereitgestellt werden. Für diese Bereitstellung nutzt die *Gesellschaff* die folgenden Optionen. Die Datenschutzerklärung der Webseite enthält einen Passus zur Verarbeitung von Kundendaten im Rahmen der geschäftlichen Tätigkeit. Dieser Passus enthält entsprechend die notwendigen Informationen nach Art. 13 DSGVO. Den Passus finden Sie in der Musterdatenschutzerklärung in der **Anlage 14.**
Des Weiteren befindet sich in der E-Mail Signatur der Mitarbeiter der *Gesellschaft* ein sogenannter Disclaimer, der auch auf die Datenschutzerklärung die darin enthaltenen Informationen verweist. Einen Muster-Disclaimer finden Sie in **Anlage 15**.

Grundsätzlich gilt es auch im Bereich des Kundendatenschutzes den Datenverarbeitungsgrundsatz der Datensparsamkeit zu befolgen und nur die wirklich notwendigen personenbezogenen Daten der Kunden zu verarbeiten.

9. Datenverarbeitung außerhalb der *Gesellschaft*

Die *Gesellschaft* bedient sich zu einem für definierte Datenverarbeitungstätigkeiten externen Dienstleistern, die diese Tätigkeiten auf Weisung der *Gesellschaft* durchführen (näheres hierzu

unter 9.1). Zum anderen erfolgen ausgewählte Datenverarbeitungstätigkeiten in gemeinsamer Verantwortlichkeit der *Gesellschaft* und einer oder mehreren Parteien (näheres hierzu unter Ziffer 9.2).

Sofern ein externer Dienstleister oder ein gemeinsamer Verantwortlicher seinen Sitz außerhalb der Europäischen Union oder dem Europäischen Wirtschaftsraum hat, sind, nebst den vertraglichen Regelungen nach Art. 26 bzw. Art. 28 DSGVO sowie den generellen Datenschutzgrundsätzen, die Anforderungen aus Ziffer 11 einzuhalten.

9.1 Auftragsdatenverarbeitung

Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen oder ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, ist der Datenschutzbeauftragte vorab zu informieren. Dienstleister können zum Beispiel im Bereich Hosting, Cloud, Callcenter, Lettershop oder Datenvernichtung mit der Datenverarbeitung beauftragt sein.

Solche Dienstleister sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere folgende Aspekte berücksichtigen:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
- Technisch-organisatorische Sicherheitsmaßnahmen
- Erfahrungen des Anbieters im Markt, Zertifizierungen
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentation, Kooperationsbereitschaft, Reaktionszeit, etc.)

Sofern ein Dienstleister personenbezogene Daten im Auftrag erhebt, verarbeitet oder nutzt, bedarf es des Abschlusses eines (elektronischen) Vertrags zur Auftragsdatenverarbeitung nach Art. 28 DSGVO. Der Abschluss eines solchen „Auftragsverarbeitungsvertrages“ hat dabei unabhängig davon, ob es sich bei dem Dienstleister um eine Konzerngesellschaft oder um Dritte handelt, zu schließen. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln. Eine Vorlage eines entsprechenden Auftragsverarbeitungsvertrages ist der **Anlage 16** zu entnehmen. Von externen Dienstleistern vorgelegte Auftragsverarbeitungsverträge werden unter Hinzuziehung des Datenschutzbeauftragten vor Unterzeichnung geprüft.

Eine Vorlage technisch-organisatorischer Maßnahmen, welche im Rahmen eines Auftragsverarbeitungsvertrages von dem externen Dienstleister auszufüllen ist, ist der **Anlage 7** zu entnehmen. Der Dienstleister ist in Hinblick auf diese mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

9.2 Gemeinsame Verantwortlichkeit

Für den Fall, dass die *Gesellschaft* mit einer anderen Partei (dabei kann es sich sowohl um eine andere Konzerngesellschaft als auch um Dritte handeln) gemeinsam die Mittel und Zwecke einer Verarbeitung personenbezogener Daten festlegt, ist eine Vereinbarung nach Art. 26 DSGVO zu schließen, in der die Aufgaben und Verantwortlichkeiten gegenüber betroffenen Personen, deren Daten sie verarbeiten, geregelt werden. Ein Beispiel für eine gemeinsame Verantwortlichkeit könnte aus einem gemeinsamen Produkt zweier Firmen entstehen. Sollte diese bspw. für ein Event aus der jeweils eigenen Datenbank Kundendaten zusammentragen, um zu diesem gemeinsamen Event einzuladen, würde es sich um eine gemeinsame Verantwortlichkeit handeln.

10. Umgang mit Datenschutzverletzungen

Nach Art. 33 DSGVO sind Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden an die zuständige Aufsichtsbehörde zu melden.

Art. 4 Nr. 12 DSGVO definiert dabei die „Verletzung des Schutzes personenbezogener Daten“ als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unregelmäßig, 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.

Wenn eine solche Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen zu Folge hat, so ist gemäß Art. 34 DSGVO neben der Aufsichtsbehörde auch die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person unverzüglich zu benachrichtigen.

Im Rahmen der Bewertung einer „Datenschutzverletzung“ gibt die Erheblichkeitsschwelle, die in Erwägungsgrund 85 der DSGVO genannt wird, ein Indiz, ob eine Meldung an die Aufsichtsbehörde zu erfolgen hat.
Sollte die Bewertung ergeben, dass keine Meldung an die Aufsichtsbehörde erfolgt, wird die Datenschutzverletzung mit entsprechender Begründung, weshalb keine Meldung erfolgte, intern dokumentiert.

Die Mitarbeiter der *Unternehmen* sind angehalten eine Datenschutzverletzung intern an *Ansprechpartner* zu melden und keine externe Meldung vorzunehmen. Der detaillierte Umgang bei einer Verletzung des Schutzes personenbezogener Daten ist der **Anlage 17** zu entnehmen und bezieht den Datenschutzbeauftragten mit ein.

Kommentiert [JM|Wpl3]: Bitte den Ansprechpartner ergänzen. Ggf. die intern für den Datenschutz zuständige Person oder zunächst die jeweilige Fachbereichsleitung.

11. Datenschutzfolgenabschätzung und Transfer-Impact-Assessment

Bei der Verarbeitung von personenbezogenen Daten kann in einigen Fällen ein hohes Risiko für die von der Datenverarbeitung betroffene Person bestehen. Dieses Risiko kann zum einen aus einer Gefahr der Rechte und Freiheiten der betroffenen Person entstehen und zum anderen auch aus der Übermittlung von personenbezogenen Daten in sogenannte Drittstaaten resultieren.

Gemäß Art. 35 DSGVO ist bei Verarbeitungsvorgängen, die wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen bergen, eine Datenschutz-Folgenabschätzung durchzuführen.

Dabei wird der Rat des Datenschutzbeauftragten eingeholt, welcher während des gesamten Prozesses beratend unterstützt. Die Vorgehensweise bei der Ermittlung der Notwendigkeit und der Durchführung einer Datenschutz-Folgenabschätzung ist in einer entsprechenden Richtlinie (siehe **Anlage 18**) festgeschrieben.

Im Falle grenzüberschreitender Datenübermittlungen an Empfänger außerhalb der Europäischen Union und des Europäischen Wirtschaftsraumes sind, neben den unter Ziffer 9 angeführten Voraussetzungen und den generellen Datenschutzgrundsätzen der DSGVO, gemäß Art. 44 DSGVO die niedergelegten Bedingungen des Kapitel V DSGVO einzuhalten.

Darüber hinaus sind, seit der „Schrems II Entscheidung“ des Europäischen Gerichtshofs und mit dem Erlass der neuen Standardvertragsklauseln der Europäischen Kommission, Datenexporteure aus der EU nunmehr verpflichtet, alle Übermittlungen personenbezogener Daten in Nicht-EU-Länder (sog. Drittländer) mittels eines sogenannten Transfer Impact Assessments kurz „TIA“ zu überprüfen und angemessene Sicherheitsvorkehrungen zu treffen. Die Vorlage, die bei der Durchführung von TIAs hinzuzuziehen ist, ist der **Anlage 19** zu entnehmen.

Die TIA ist unabhängig davon durchzuführen, ob es sich bei dem Datenempfänger um eine im Drittland ansässige Konzerngesellschaft oder eine Dritte handelt.

12. Online-Präsenz der *Gesellschaft*

Die *Gesellschaft* bietet den Kunden auch verschiedene Online-Angebote. Dazu zählen die Webseite und die Präsenz in den sozialen Medien.

Um eine Webseite datenschutzkonform zu betreiben, müssen verschiedene Vorkehrungen getroffen werden. Grundsätzlich muss besonders die Datenschutzerklärung der Webseite leicht zugänglich für den Webseitenbesucher angelegt sein und stets aktualisiert werden.
In die Datenschutzerklärung gehört neben dem Verantwortlichen auch ein Hinweis zu der potenziellen Verwendung von sogenannten Cookies, sowie eine Aufzählung der verschiedenen Prozesse der Webseite, die (potenziell) personenbezogene Daten verarbeiten. Dabei müssen zu jedem Verarbeitungsprozess die in Art. 13 DSGVO als notwendig festgelegten Informationen genannt werden. Die Datenschutzerklärung muss darüber hinaus auf die Rechte der betroffenen Person hinweisen. In **Anlage 14** finden Sie eine Vorlage für eine Datenschutzerklärung, die weiter auf die Bedürfnisse der *Gesellschaft* angepasst werden kann.

Bezüglich des Einsatzes von Cookies sind auf der Webseite weitere Maßnahmen zu treffen. Es wurde eine sogenannte Consent-Management-Plattform implementiert. Diese Plattform ermöglicht es einfach und präzise über den Einsatz von Cookies zu informieren. Das Tool kann außerdem die für den Einsatz von technisch nicht notwendigen Cookies erforderliche Einwilligung einholen. Hinweise zu der Implementierung eines datenschutzkonformen Cookie Banner finden Sie in **Anlage 20**.

Neben der Webseite betreibt die *Gesellschaft* auch Unternehmensseiten bei verschiedenen Social Media Plattformen. Ähnlich wie beim Betreiben einer Webseite kommen auch beim Betreiben von Social Media Seiten verschiedene Pflichten auf den Verantwortlichen zu. Wie bei allen Verarbeitungen von personenbezogenen Daten, wird auch in Bezug auf die Social Media Plattformen eine Rechtgrundlage für die Verarbeitung benötigt.
Des Weiteren gilt es zu klären, ob es sich im vorliegenden Fall, um eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit handelt. Je nach Fall bedarf es dann einen entsprechenden Vertrag mit dem Betreiber der Social Media Plattform.
Auch die verschiedenen Informationspflichten sind einzuhalten. Die betroffene Person muss rechtzeitig über die Datenverarbeitung informiert werden, es muss also eine Datenschutzerklärung hinterlegt werden, die die notwendigen Informationen bereitstellt.

Wichtig: Jede gewerbliche Plattform muss ein gültiges Impressum besitzen. Das gilt auch für Social Media Kanäle. Wir empfehlen einen Link zum Impressum der Webseite einzubauen.

13. Videoüberwachung

Die Videoüberwachung und die damit einhergehende Verarbeitung personenbezogener Daten greift grundsätzlich in das Recht auf informationelle Selbstbestimmung von Personen ein. Daher werden an die Zulässigkeit von Videoüberwachungen besondere Anforderungen gestellt. Der Einsatz von Videoüberwachung in den Standorten der *Unternehmen* wird daher je Einzelfall mit Unterstützung durch den Datenschutzbeauftragten datenschutzrechtlich geprüft. Das Formular, welches für die datenschutzrechtliche Prüfung geplanter Videoüberwachung herangezogen wird, ist der **Anlage 21** zu entnehmen.
Zudem wird bei geplanter Videoüberwachung im Voraus eine Datenschutz-Folgenabschätzung durchgeführt.

Um den Transparenz- und Informationspflichten gemäß Art. 12 f DSGVO nachzukommen, werden bereits vor Betreten videoüberwachter Bereiche Hinweisschilder mit den wesentlichen Informationen angebracht. Eine solches Hinweisschild ist in der **Anlage 22** ersichtlich. Die Vorlage für ein ausführliches Informationsblatt ist der **Anlage 23** zu entnehmen. Die je Einzelfall entsprechenden Informationsblätter werden zugänglich hinterlegt und sind für die Betroffenen einsehbar.

Kommentiert [JM|Wpl4]: Hier ggf. standortspezifisch ergänzen, wo die Information ausgelegt wird.

14. Überwachung und Fortschreibung des Datenschutzkonzeptes

Die Überwachung und Prüfung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen obliegt der verantwortlichen Stelle. Die Personalvertretung sowie der Datenschutzbeauftragte werden entsprechend beteiligt.

Kommentiert [JM|Wpl5]: z.B. der Betriebsrat, falls vorhanden

Das Datenschutzkonzept wird im Zusammenhang mit den technischen und organisatorischen Maßnahmen gemäß den Pflichten der Art. 24ff. DSGVO regelmäßig fortgeschrieben. Dabei wird zudem geprüft, ob sich die getroffenen Sicherheitsmaßnahmen bewährt haben.

Dr. Volker Wodianka, LL.M.
Zertifizierter Datenschutzbeauftragter