Unternehmensrichtlinie Datenschutz

I. Ziel/Zweck der Datenschutzrichtlinie; Möglichkeit der Kenntnisnahme

1. Die Datenschutzrichtlinie ist die unternehmensinterne, verbindliche Grundlage für die Erhebung, die Verarbeitung, die Übermittlung und die Nutzung sämtlicher personenbezogener Daten.

2. Sie bezweckt den Schutz personenbezogener Daten von Betroffenen und die langfristige Wahrung eines angemessenen Schutzniveaus, indem alle datenschutzrelevante Handlungen des Unternehmens im Einklang mit den geltenden datenschutzrechtlichen Vorschriften (insb. DS-GVO, BDSG) stehen.

3. Allen Mitarbeitern des Unternehmens muss es jederzeit, schnell und ohne besondere Hindernisse möglich sein, Kenntnis von der Datenschutzrichtlinie zu erlangen. Dafür wird die Richtlinie jedem Mitarbeiter ausgehändigt

II. Persönlicher und sachlicher Anwendungsbereich; Änderungen; Verhältnis zum nationalen Recht

1. Diese Datenschutzrichtlinie findet Anwendung für das gesamte Unternehmen.

2. Sachlich ist diese Richtlinie bei jeglichem Umgang mit personenbezogenen Daten natürlicher oder juristischer Personen zu beachten, insbesondere bei Datenerhebungen, Datenverarbeitungen und Datenübermittlungen. Sie gilt nicht für anonymisierte Daten.

3. Persönlich findet diese Richtlinie für alle Mitarbeiter und leitenden Angestellten des Unternehmens Anwendung. Sie wird von der Unternehmensführung in Kraft gesetzt und ist für alle ihr Unterworfenen verbindlich.

4. Für Änderungen dieser Richtlinie ist die Zustimmung des unternehmensinternen Datenschutzbeauftragten erforderlich. Erhebliche Veränderungen dieser Richtlinie sind jährlich der nationalen Datenschutzbehörde zu melden.

5. Diese Datenschutzrichtlinie ergänzt bestehende nationale Datenschutzregelungen, ohne diese zu ersetzen. Nationale gesetzliche Verpflichtungen bleiben durch diese Richtlinie unberührt. Im Kollisionsfall oder im Falle einer Abweichung zwischen nationalen Vorschriften und Verpflichtungen dieser Datenschutzrichtlinie genießt das staatliche Recht Anwendungsvorrang. Die Regelungen der Richtlinie entfalten auch dann verbindliche Wirkung, wenn es an einer staatlichen Bestimmung zum Datenschutz fehlt.

III. Datenschutzorganisation; unternehmensinterner Datenschutzbeauftragter

1. Der Datenschutzbeauftragte ist für die Einhaltung der gesetzlichen Datenschutzvorschriften und der Bestimmungen dieser Datenschutzrichtlinie verantwortlich. Er steht der Unternehmensführung bei der Erfüllung ihrer über datenschutzrechtlichen Verpflichtungen beratend zur Verfügung, überwacht die Konformität mit gesetzlichen Vorgaben und etwaige Risiken und ist für Rücksprachen mit den Aufsichtsbehörden zuständig. Im Übrigen arbeitet er weisungsfrei, gewissenhaft und entsprechend seines Fachwissens.

2. An den Datenschutzbeauftragten kann sich jederzeit vertrauensvoll mit Beschwerden, Auskunftsersuchen und sonstigen datenschutzrechtlichen Anliegen gewendet werden.

3. Der Datenschutzbeauftragte kann wie folgt erreicht werden:

RA Dipl. iur. Julian Akich, LL.B.

Karlstraße 3-5

76133 Karlsruhe

0721 91511420

IV. Begriffsbestimmungen

Nach dem Vorbild des Art. 4 der europäischen Datenschutzgrundverordnung (DS-GVO) liegen dieser Datenschutzrichtlinie folgende Begriffsbestimmungen zugrunde

1. Personenbezogene Daten (vgl. Art. 4 Nr. 1 DS-GVO) sind alle Informationen über eine natürliche Person, durch die sie direkt oder indirekt identifiziert wird oder identifizierbar ist. Identifizierbar ist eine Person, sobald zu ihr eine Verbindung mittels personenbezogener Daten hergestellt werden kann, beispielsweise durch Zuordnung einer Kennung, Standortdaten, oder eines oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der natürlichen Person sind. Dies ist auch dann der Fall, wenn ein Rückschluss auf eine natürliche Person durch eine Kombination von Informationen – wenn auch erst mit zufälligem Zusatzwissen verknüpft – möglich ist. Unter personenbezogenen Daten fallen insbesondere der Name, die Adresse, die Telefonnummer, die E-Mail-Adresse, oder Fotos und Videoaufzeichnungen der natürlichen Person sowie Kunden- und Personaldaten. Eine Identifizierung der Person kann mit Hilfe einer Anonymisierung oder Pseudonymisierung ausgeschlossen werden.

2. Besonders schutzwürdige personenbezogene Daten sind alle Informationen über die rassische und ethische Herkunft, über religiöse oder weltanschauliche Überzeugungen, über politische Meinungen, über eine Gewerkschaftszugehörigkeit, über die Gesundheit oder über die sexuelle Orientierung bzw. das Sexualleben einer betroffenen Person.

3. Unter einem Betroffenen versteht man jede natürliche Person, über die personenbezogene Daten verarbeitet werden.

4. Die Verarbeitung personenbezogener Daten (vgl. Art. 4 Nr. 2 DS-GVO) bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verarbeitung oder einer andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

5. Die Einschränkung der Verarbeitung (vgl. Art. 4 Nr. 3 DS-GVO) ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

6. Die Übermittlung ist jede Bekanntgabe von personenbezogenen Daten durch den Verantwortlichen an Dritte.

7. Das Profiling (Art. 4 Nr. 4 DS-GVO) bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

8. Anonymisierung meint die Verarbeitung von personenbezogenen Daten in der Gestalt, dass ein Personenbezug auf Dauer nicht mehr hergestellt werden kann oder der Rückschluss auf eine natürliche Person nur mit unverhältnismäßigen Aufwand möglich ist.

9. Pseudonymisierung (Art. 4 Nr. 5 DS-GVO) ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

10. Dateisystem (Art. 4 Nr. 6 DS-GVO) ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

11. Verantwortlicher (Art. 4 Nr. 7 DS-GVO) bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

12. Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

13. Empfänger (Art. 4 Nr. 9 DS-GVO) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

14. Dritter (Art. 4 Nr. 10 DS-GVO) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

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

16. Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DS-GVO) ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

17. Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO) sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

18. Unternehmen (Art. 4 Nr. 18 DS-GVO) ist eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

19. Unternehmensgruppe (Art. 4 Nr. 19 DS-GVO) ist eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

20. Datenschutzvorfall bezeichnet alle Umstände, die den Verdacht begründen, dass personenbezogene Daten rechtswidrig durch Mitarbeiter oder Dritte erhoben, übermittelt, kopiert, genutzt oder ausgespäht wurden.

V. Grundsätze für die Verarbeitung personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten müssen die folgenden gesetzlichen Grundsätze eingehalten werden (vgl. Art. 5 DS-GVO):

1. Rechtmäßigkeit:

Personenbezogene Daten werden auf rechtmäßige Weise, nach Treu und Glauben erhoben.

2. Zweckbindung:

Die Nutzung personenbezogener Daten muss einem vorher festgelegten, eindeutigen und legitimen Zweck dienen und darf nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise erfolgen. Nachträgliche Zweckänderungen sind nur ausnahmsweise zulässig und rechtfertigungsbedürftig. Sie müssen mit dem ursprünglichen Zweck vereinbar sein.

3. Transparenz:

Der Umgang mit personenbezogenen Daten soll auf eine für den Betroffenen nachvoll-ziehbare, transparente Weise erfolgen. Er soll dafür i. S. d. Art. 13 DS-GVO informiert werden. Aus der Information soll für den Betroffenen ersichtlich sein, welchem Zweck die Datenverarbeitung dient, an welche verantwortliche Stelle er sich wenden kann und ob bzw. an welche Dritte die Daten übermittelt werden. Eine umfassende Informationspflicht iSd Art. 14 DS-GVO besteht gegenüber dem Betroffenen nachträglich auch im dem Fall, dass die personenbezogenen Daten über den Betroffenen nicht bei diesem selbst, sondern bei einem Dritten erhoben werden. Gleiches gilt, sobald die Zweckbestimmung der Datenverarbeitung geändert wird.

4. Datensparsamkeit; Speicherbegrenzung:

Es ist stets vor der Verarbeitung personenbezogener Daten zu prüfen, ob und inwiefern der Zweck der Verarbeitung mit der beabsichtigten Vorgehensweise erreicht wird. Sofern der Zweck auch ohne Rückgriff auf personenbezogene Daten erreicht werden kann, etwa durch anonymisierte oder pseudonymisierte Daten, ist diese mildere Vorgehensweise vorzuziehen. Vorbehaltlich anderer staatlicher Regelungen ist eine Speicherung personenbezogener Daten auf Vorrat für anlasslose oder zukünftige Zwecke unzulässig. Die Speicherung von personenbezogenen Daten soll nur solange erfolgen, wie sie für den Verarbeitungszweck erforderlich ist.

5. Richtigkeit; Datenaktualität:

Die Richtigkeit, Vollständigkeit und Aktualität der erhobenen personenbezogenen Daten ist sicherzustellen. Anderenfalls sind unrichtige, unvollständige und nicht mehr aktuelle Daten unverzüglich zu berichtigen, zu ergänzen, zu aktualisieren oder zu löschen.

6. Integrität; Vertraulichkeit:

Personenbezogene Daten sind vertraulich zu behandeln und durch geeignete technische wie auch organisatorische Maßnahmen sicherzustellen, dass ein angemessener Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung gewährleistet wird.

7. Löschung:

Sobald die gesetzlichen oder betriebsbedingten Aufbewahrungsfristen abgelaufen sind, sind personenbezogene Daten zu löschen.

8. Dokumentation; Verarbeitungsverzeichnis:

Über alle Datenverarbeitungen hat das Unternehmen schriftlich oder elektronisch ein Verzeichnis zu führen, das den in Art. 30 Abs. 1, Abs. 2 DS-GVO vorgeschriebenen Mindestangaben entspricht. Hierfür hat jede datenverarbeitende Abteilung des Unternehmens einen Verantwortlichen zu beauftragen, dem die Führung des Verarbeitungsverzeichnisses obliegt. Dem Verantwortlichen steht der Datenschutzbeauftragte beratend zur Seite. Einer Aufforderung der Aufsichtsbehörde, ein Datenverarbeitungsverzeichnis bereitzustellen, ist vom Datenschutzbeauftragten mit Einwilligung der Unternehmensleitung Folge zu leisten.

VI. Rechtmäßigkeit der Datenverarbeitung

1. Nach Art. 6 Abs. 1 DS-GVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn mindestens einer der folgenden Erlaubnistatbestände vorliegt:

a) Einwilligung in die Datenverarbeitung

Der Betroffene kann seine Einwilligung zur zweckbezogenen Verarbeitung, insbesondere zur werblichen Ansprache geben. Vor der Einwilligung ist der Betroffene umfassend zu informieren. Die Einwilligungserklärung muss freiwillig und grundsätzlich schriftlich oder elektronisch erfolgen. Die Einwilligung muss ordnungsgemäß dokumentiert werden. Sobald der Verwendung der Daten zu Werbezwecken durch den Betroffenen widersprochen wird, muss eine Sperrung seiner personenbezogenen Daten erfolgen und eine erneute Verwendung dieser Daten unterlassen werden.

b) Datenverarbeitung aufgrund vertraglicher Beziehungen

Die Verarbeitung ist zulässig, soweit sie der Begründung, der Abwicklung, der Beendigung oder der Erfüllung eines bestehenden Vertrages, oder die Verarbeitung zur Erfüllung oder Durchführung vorvertraglicher Maßnahmen oder einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist.

c) Datenverarbeitung aufgrund lebenswichtiger und berechtigter Interessen

Die Verarbeitung ist zulässig, soweit sie zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen natürlichen Person erforderlich ist. Zudem darf eine Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erfolgen, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Eine Verarbeitung ist unzulässig, wenn schutzwürdige Interessen des Betroffenen das Interesse des Verantwortlichen an der Verarbeitung im Einzelfall überwiegen. Dies ist vor jeder Verarbeitung sorgfältig zu prüfen.

d) Gesetzliche Erlaubnis zur Datenverarbeitung

Die Verarbeitung ist zulässig, wenn sie durch nationale Rechtsvorschriften verlangt, vorausgesetzt, gestattet oder auf andere Weise erlaubt wird.

e) Datenverarbeitung bei besonders schutzwürdigen Daten

Besonders schutzwürdige personenbezogene Datendürfen nur dann verarbeitet werden, wenn eine Einwilligung des Betroffenen vorliegt oder sie gesetzlich erlaubt oder zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche gegen den Betroffenen erforderlich ist.

f) Automatisierte Einzelentscheidungen

Automatisierte Verarbeitungen personenbezogener Daten dürfen für den Betroffenen nicht ausschließlich die Grundlage für eine Entscheidung bilden, die ihm gegenüber negative rechtliche Folgen oder erhebliche Beeinträchtigungen bewirken. Vielmehr ist dem Betroffenen der Umstand einer automatisierten Verarbeitung offenzulegen sowie das Ergebnis dieser mitzuteilen.

g) Personenbezogene Daten im Internet und Tracking

Werden personenbezogene Daten auf Internetseiten oder in Apps oder mittels Cookies verarbeitet, erhoben oder genutzt, besteht in jedem Fall die Pflicht den Betroffenen in leicht erkennbarer, unmittelbar erreichbarer und ständig verfügbarer Weise darüber durch Hinweise zu informieren. Gleiches gilt für das Tracking, dem Erstellen von Nutzungsprofilen zur Auswertung des Internetnutzungsverhalten. Personenbezogenes Tracking ist ausschließlich aufgrund einer gesetzlichen Erlaubnis oder der Einwilligung des Betroffenen zulässig. Bei einem Tracking unter einem Pseudonym besteht die Pflicht zu einer Opt-out-Möglichkeit.

2. Gleiches gilt, wenn Dritte Auskunft über personenbezogene Daten Betroffener begehren.

VII. Rechtmäßigkeit der Datenübermittlung

1. Eine Übermittlung personenbezogener Daten an Dritte ist nur unter den Voraussetzungen dieser Datenschutzrichtlinie für eine rechtmäßige Datenverarbeitung zulässig. Folglich ist eine Übermittlung ist nur dann rechtmäßig, wenn eine Einwilligung des Betroffenen vorliegt oder sie gesetzlich erlaubt ist und sie einem vorher festgelegten Zweck dient.

2. Bei einer Datenübermittlung an einen Empfänger außerhalb der Europäischen Wirtschaftsraumes muss ein angemessenes Datenschutzniveau sichergestellt werden, dass dem dieser Datenschutzrichtlinie gleichwertig ist.

VIII. Auftragsdatenverarbeitung

1. Verarbeitet eine externe natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle personenbezogene Daten im Auftrag des Verantwortlichen ist mit dem Auftragnehmer schriftlich eine Auftragsdatenverarbeitungsvereinbarung mit dem in Art. 28 DS-GVO zwingend vorausgesetztem Inhalt zu schließen. Dabei ist die Datenverarbeitung nach den konkreten Weisungen des Auftraggebers durchzuführen.

2. Das beauftragende Unternehmen trägt die Verantwortung für die rechtskonforme Durchführung und Umsetzung der Verarbeitung. Es hat den Auftragnehmer sorgfältig auszusuchen, besonders nach der fachlichen Eignung, der Qualität seiner technisch-organisatorischen Datensicherungsstandards oder vergleichbaren Indikatoren der Zuverlässigkeit.

3. Der Auftragsnehmer untersteht den Weisungen und der Kontrolle des Auftraggebers. Das beauftragende Unternehmen soll durch Weisungen, beispielsweise im Hinblick auf Datensicherheitsmaßnahmen, Zuständigkeiten und Verantwortlichkeiten zwischen Auftragnehmer und Auftraggeber, ein möglichst hohes Datenschutzniveau des Auftragnehmers sicherstellen.

4. Im Übrigen gelten für die Auftragsverarbeitung die Grundsätze zur „Rechtmäßigkeit der Datenverarbeitung“ unter Abschnitt VI.

IX. Rechte der Betroffenen

Gemäß der Europäischen Datenschutzgrundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz (BDSG) können die Betroffenen folgende Datenschutzrechte ausüben, sofern die Tatbestandsvoraussetzungen der jeweiligen Normen erfüllt sind:

1. Recht auf Auskunft, Art. 15 DS-GVO, § 34 BDSG

a) Der Betroffene hat das Recht Auskunft darüber zu verlangen, ob im Unter-nehmen ihn betreffende personenbezogene Daten verarbeitet werden, und bejahendenfalls welche Daten zu welchem Zweck und aus welcher Herkunft und in welcher Dauer gespeichert sind. Im Falle einer Datenübermittlung an Dritte, ist auch über die Identität des Empfängers sowie der Kategorien von Empfängern Auskunft zu erteilen.

b) Vor der Auskunftserteilung hat der Verantwortliche die Identität der betroffenen Person festzustellen und ggf. Maßnahmen zu ergreifen, um aufkommende Zweifel an der Identität der beantragenden Person auszuräumen.

c) Sofern das Auskunftsersuchen nicht elektronisch erfolgt ist, ist dem Betroffenen die Auskunft schriftlich zu erteilen. Darüber hinaus stellt der Verantwortliche eine Kopie der in Art. 15 Abs. 1 DS-GVO aufgeführten personenbezogenen Daten und Informationen zur Verfügung, die Gegenstand der Verarbeitung sind. Stellt der Betroffene den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen.

2. Recht auf Berichtigung, Art. 16 DS-GVO

Der Betroffene kann die unverzügliche Berichtigung oder Ergänzung der ihn betreffenden personenbezogenen Daten verlangen, die unrichtig oder unvollständig sind.

3. Recht auf Löschung („Recht auf Vergessenwerden“), Art. 17 DS-GVO, § 35 BDSG

a) Der Betroffene hat einen Anspruch auf unverzügliche Löschung der ihn betreffenden personenbezogenen Daten, sobald einer der folgenden Löschungsgründe einschlägig ist:

- Der Zweck der Datenverarbeitung besteht nicht oder nicht mehr.
- Eine Rechtsgrundlage für die Datenverarbeitung fehlt oder ist weggefallen, indem der Betroffene seine Einwilligung widerrufen hat.
- Der Betroffene widerspricht der Datenverarbeitung und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die Datenverarbeitung ist unrechtmäßig.
- Zur Erfüllung einer rechtlichen Verpflichtung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen ist die Verarbeitung personenbezogener Daten nicht (mehr) erforderlich.
- Ein die Rechte des Betroffenen überwiegendes öffentliches Interesse an der Verarbeitung besteht nicht.

b) Sofern personenbezogene Daten öffentlich bekannt gemacht wurden und eine Löschungspflicht besteht, müssen weitere Verantwortliche darüber informiert werden, dass der Betroffene von ihnen die Löschung aller Links zu den einschlägigen personenbezogenen Daten oder Kopien oder Vervielfältigungen dieser verlangt hat.

4. Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO

a) Der Betroffene hat das Recht auf Einschränkung der Verarbeitung der ihn betreffenden personenbezogenen Daten, sobald einer der folgenden Gründe einschlägig ist:

- Der Betroffene bestreitet die Richtigkeit der personenbezogenen Daten. Eine Einschränkung erfolgt für den Zeitraum, in dem der Verantwortliche die Richtigkeit überprüft
- Die Datenverarbeitung ist unrechtmäßig, jedoch verlangt der Betroffene die Nutzungseinschränkung anstelle einer Löschung der personenbezogenen Daten
- Die personenbezogenen Daten werden vom Verantwortlichen für die Zwecke der Verarbeitung nicht mehr benötigt, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Der Betroffene hat gegen die Verarbeitung Widerspruch eingelegt. Eine Einschränkung erfolgt für den Zeitraum, in dem der Verantwortliche den Widerspruch überprüft.

b) Nach einer wirksamen Einschränkung der Verarbeitung dürfen die betreffenden personenbezogenen Daten nur mit Einwilligung des Betroffenen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutze Rechte anderer oder aufgrund eines wichtigen öffentlichen Interesses verarbeitet werden.

c) Der Betroffene ist über die Aufhebung der Einschränkung zu informieren.

5. Recht auf Datenübertragbarkeit, Art. 20 DS-GVO

Sofern die Datenverarbeitung auf einer Einwilligung beruht oder zur Durchführung eines Vertrages erforderlich war, hat der Betroffene das Recht die ihn betreffenden personenbezogenen Daten an einen anderen Verantwortlichen zu übermitteln, soweit dies technisch möglich ist.

6. Recht auf Widerspruch, Art. 21 DS-GVO

Der Betroffene hat jederzeit das Recht gegen die Datenverarbeitung Widerspruch einzulegen, die auf einer Einwilligung beruht oder zur Wahrung berechtigter Interessen erforderlich ist. Dafür muss das Ergebnis einer Abwägung ergeben, dass das aufgrund einer besonderen Situation ergebende,

schutzwürdige Interesse des Betroffenen das Interesse des Unternehmens an der Verarbeitung überwiegt. Ein Widerspruchsrecht besteht nicht, wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

7. Recht auf Aufsichtsbeschwerde, Art. 77 DS-GVO i. V. m. § 19 BDSG

Darüber hinaus steht dem Betroffenen das Recht zu, eine Beschwerde bei der zuständigen Aufsichtsbehörde einzulegen, wenn er der Auffassung ist, dass die Verarbeitung seiner personenbezogenen Daten unrechtmäßig erfolgt ist.

8. Um ein Datenschutzrecht auszuüben, kann sich der Betroffene an den unternehmensinternen Datenschutzbeauftragten wenden. Sein Anliegen ist umgehend von der verantwortlichen Stelle umzusetzen und darf ihm nicht zum Nachteil gereichen.

9. Dem Betroffenen ist innerhalb eines Monats die durchgeführte Maßnahme anzuzeigen.

X. Datenschutzkontrolle

1. Für die Gewährleistung eines angemessenen Schutzniveaus und die Konformität mit den geltenden Datenschutzbestimmungen wird regelmäßig die Einhaltung dieser Richtlinie durch Audits und andere Kontrollmechanismen überprüft. Die Kontrolle obliegt dem unternehmensinternen Datenschutzbeauftragten oder intern oder extern mit Auditrechten beauftragten Prüfern.

2. Die Ergebnisse des Audits sind zu dokumentieren und dem zuständigen Datenschutzbeauftragten oder anderen Prüfern mitzuteilen. Zur Wahrung seiner Berichtpflichten ist der Aufsichtsrat des Unternehmens [falls vorhanden] über die wesentlichen Erkenntnisse der Datenschutzkontrolle zu informieren.

3. Eine Datenschutzkontrolle ist erfolgreich beendet, wenn bei allen dokumentierten Mängeln durch die Implementierung geeigneter Maßnahmen Abhilfe geschaffen wurde. Dies ist entsprechend zu überprüfen.

XI. Vertraulichkeit der Datenverarbeitung

1. Alle Beschäftigten unterliegen der Pflicht den Datenschutz einzuhalten („Datengeheimnis“). Eine unbefugte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist den Beschäftigten untersagt. Unbefugt handelt ein Mitarbeiter, wenn er personenbezogene Daten verarbeitet, ohne dazu zur Erfüllung seiner Tätigkeit beauftragt, angewiesen oder berechtigt zu sein.

2. Alle Beschäftigten müssen sich vor Beginn ihrer Tätigkeit schriftlich zur Vertraulichkeit verpflichten. Dabei ist zu versichern, dass die im Rahmen der Tätigkeit erlangten personenbezogene Daten nicht für private oder wirtschaftliche Interessen genutzt, an Unbefugte weitergeleitet oder in sonstiger Weise zugänglich gemacht werden. Diese Pflicht besteht über das Ende des Beschäftigungsverhältnisses hinaus. Bei Aufnahme der Tätigkeit ist der Beschäftigte über seine Pflicht zur Vertraulichkeit zu informieren und schriftlich zu verpflichten.

3. Um ein hohes Maß an Vertraulichkeit zu gewährleisten, darf den Beschäftigten Zugang zu personenbezogenen Daten nur in dem Umfang eingeräumt werden, der konkret zur Erfüllung ihrer Tätigkeiten notwendig ist („Need-to-know-Prinzip“). Es ist ein detailliertes und vollständiges Berechtigungskonzept zu etablieren und sorgfältig zu pflegen, durch das die Beschäftigten

entsprechend ihrer Rollen und Zuständigkeiten mit festgelegten Zugangsberechtigungen ausstattet sind.

XII. Datensicherheit; Fortbildungen

1. Durch das Unternehmen ist jederzeit der Schutz von personenbezogenen Daten vor unbefugten Zugriff, unrechtmäßige Verarbeitung oder unberechtigten Verlust, Veränderung oder Zerstörung sicherzustellen. Dafür sind wirksame technisch-organisatorische Maßnahmen in einem Sicherheitskonzept zusammenzustellen, das dem aktuellen Stand der Technik, den verarbeitungsspezifischen Risiken und der Schutzbedürftigkeit der verarbeiteten Daten entspricht. Geeignete Maßnahmen stellen die Pseudonymisierung personenbezogener Daten oder die konkrete Zuweisung von Zuständigkeiten, Rollen und Verantwortlichkeiten dar, beispielsweise Schließsysteme und Zutrittskontrollen von Geschäftsräumen und Arbeitsgeräten, passwortgeschützte Zugänge zu Systemen und Datenbänken sowie verschlüsselte Kommunikationswege oder Datenübertragungen.

2. Diese Maßnahmen sind auch vor jeder Einführung neuer IT-Systeme zur Datenverarbeitung zu beachten.

3. Das Sicherheitskonzept soll kontinuierlich überprüft und an die technisch-organisatorischen Änderungen und Entwicklungen zum Schutz von personenbezogenen Daten angepasst werden.

4. Es ist durch technisch-organisatorische Maßnahmen sicherzustellen, dass personenbezogene Daten getrennt verarbeitet werden, die zu verschiedenen Zwecken erhoben worden sind.

5. Dritte sind während eines Aufenthalts im Unternehmen, etwa zu Wartungsarbeiten, zu beaufsichtigen und es ist zu verhindern, dass diese in irgendeiner Weise Zugang zu personenbezogenen Daten erhalten. Ist dies ausnahmsweise nicht möglich, soll ein umfassender Schutz von Daten durch Protokollierungs- und Aufzeichnungspflichten gewährleistet werden.

6. Um ein hohes Datenschutzniveau im Unternehmen aufrechtzuerhalten, sind diejenigen Mitarbeiter im erforderlichen Umfang über datenschutzrechtlichen Anforderungen fortzubildendie regelmäßig oder fortlaufend personenbezogene Daten verarbeiten oder Zugang zu solchen haben.

XIII. Datenschutzvorfälle; Rechtsfolgen von Verstößen

1. Im Falle eines Datenschutzvorfalls, einem Verstoß gegen diese Richtlinie oder gegen andere Regelungen zum Schutz personenbezogener Daten ist der verantwortliche Mitarbeiter verpflichtet, den Datenschutzvorfall umgehend seinem Vorgesetzten sowie dem Datenschutzbeauftragten zu melden. Dabei ist über alle zur Sachverhaltsaufklärung notwendigen Informationen zu unterrichten, vorwiegend über den Empfänger, die konkret betroffenen personenbezogenen Daten und die Art und der Umfang der vom Vorfall betroffenen Daten.

2. Besteht für den jeweiligen Datenschutzvorfall eine Meldepflicht gegenüber den Aufsichtsbehörden, hat der Datenschutzbeauftragte diese umgehend zu erfüllen.

3. Wurde ein Datenschutzvorfall, ein Verstoß gegen diese Richtlinie oder ein Verstoß gegen andere datenschutzrechtliche Bestimmungen fahrlässig oder vorsätzlich verursacht, zieht dies arbeitsrechtliche Konsequenzen nach sich, eine fristlose oder ordentliche Kündigung einbegriffen.

Daneben können strafrechtliche und zivilrechtliche Sanktionen in Erwägung gezogen werden, etwa die Geltendmachung von Schadensersatzansprüchen.

XIV. Datenschutz-Folgenabschätzung

1. Weist eine Form der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen auf, besteht für jede datenverarbeitende Abteilung des Unternehmens im Vorfeld die Pflicht, eine Folgenabschätzung der angestrebten Datenverarbeitung für den Datenschutz durchzuführen. Die Datenschutz-Folgenabwägung soll den in Art. 35 Abs. 7 DS-GVO genannten Mindestvoraussetzungen entsprechen.

2. Für die Durchführung der Datenschutz-Folgenabschätzung steht der datenverarbeitenden Abteilung des Unternehmens der Datenschutzbeauftragte beratend und unterstützend zur Seite, in erster Linie für die Feststellung eines hohen Risikos einer Datenverarbeitung.

XV. Ermittlungen arbeitsrechterheblicher Pflichtverletzungen oder Straftaten

1. Jegliche unternehmensinternen Ermittlungen müssen im Einklang mit den geltenden Normen zum Datenschutz und datenschutzrechtlichen Verpflichtungen stehen. Die mit der Ermittlung im Zusammenhang stehende Datenverarbeitung muss dabei im besonderen Maße zum Ziel der Ermittlung und in Bezug auf die schutzbedürftigen Interessen der betroffenen Personen verhältnismäßig sein, das heißt geeignet, erforderlich und angemessen. Unter unternehmensinterne Ermittlungen fallen insbesondere Handlungen, die eine erhebliche arbeitsrechtliche Pflichtverletzung oder eine Straftat verhindern, ermitteln oder konstatieren sollen.

2. Es ist sicherzustellen, dass der Datenschutzbeauftragte bei der Form, dem Umfang und der sonstigen Konkretisierung aller Ermittlungsmaßnahmen beteiligt und zu Rate gezogen wird.

3. Der Betroffene ist unverzüglich über die gegen ihn gerichtete Ermittlung und die damit verbundenen Maßnahmen zu informieren.

XVI. Verantwortlichkeiten

1. Die Verantwortung für jede Datenverarbeitung innerhalb des Unternehmens und der verbundenen Unternehmen obliegt der Unternehmensführung (Vorständen und Geschäftsführungen). Sie müssen jederzeit sicherstellen und nachweisen, dass die Bestimmungen dieser Richtlinie und die gesetzlichen Datenschutzanforderungen von ihren Mitarbeitern eingehalten werden.

2. Es sind geeignete technisch-organisatorische Maßnahmen zur Verfügung zu stellen, die eine rechtskonforme Datenverarbeitung ermöglichen, insbesondere den Verarbeitungsgrundsätzen der Rechtmäßigkeit, Transparenz und Dokumentation entsprechen.

XVII. Aktualität der Richtlinie; Änderungen

1. Die Bestimmungen dieser Richtlinie sind fortlaufend zu überprüfen und an die aktuellen datenschutzrechtlichen Anforderungen anzupassen.

2. Änderungen an dieser Richtlinie sind formlos möglich. Sie entfalten unmittelbare Wirksamkeit für alle Mitarbeiter des Unternehmens. Über Änderungen an dieser Richtlinie sind alle Verantwortlichen umgehend im erforderlichen Umfang zu informieren.