

Datenschutzrichtlinie

AQUA CONSULTING & MAINTENANCE

TINO KREBS





Datenschutzrichtlinie

(Stand 2018-05-16)

Vorwort

Im digitalen Zeitalter besteht überall die Möglichkeit Daten zu senden und zu empfangen. Dies setzt voraus, dass Daten erfasst und verarbeitet werden. Ein hohes Maß an Datensicherheit ist zu gewährleisten. Dies gilt für Daten von Mitarbeitern, Kunden, Interessenten und Geschäftspartnern. Datenschutz ist Schutz der Person und der Privatsphäre.

Die Ziele der Datenschutz-Grundverordnung DSGVO

- a.) Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- b.) Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- c.) Schutz des freien Verkehrs personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Dies entspricht den Anforderungen der Europäischen Datenschutzrichtlinie und stellt die Einhaltung der Prinzipien der weltweit geltenden nationalen und internationalen Datenschutzgesetze sicher.

Unserer Mitarbeiter sind verpflichtet, diese Richtlinie zum Datenschutz einzuhalten und die jeweiligen Datenschutzgesetze zu wahren.

Personenbezogene Daten müssen

- a.) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- b.) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
- c.) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- d.) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- e.) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen



Datenschutzrichtlinie

(Stand 2018-05-16)

Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

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

Als Inhaber des Unternehmens trage ich dafür Sorge, dass die gesetzlichen Regelungen und Prinzipien zum Datenschutz im Unternehmen geachtet werden.

Tino Krebs



Datenschutzrichtlinie

(Stand 2018-05-16)

Inhaltsverzeichnis

1. Ziel der Datenschutzrichtlinie.....	4
2. Geltungsbereich und Änderung	4
3. Verarbeitung personenbezogener Daten	5
4. Zulässige Datenverarbeitung.....	6
5. Mitarbeiterdaten	8
6. Übermittlung personenbezogener Daten.....	10
7. Rechte der Betroffenen.....	11
8. Vertraulichkeit der Verarbeitung	11
9. Sicherheit der Verarbeitung	12
10. Datenschutzkontrolle.....	12
11. Datenschutzvorfälle	12



Datenschutzrichtlinie

(Stand 2018-05-16)

1. Ziel der Datenschutzrichtlinie

Die Firma Aqua Consulting & Maintenance verpflichtet sich im Rahmen seiner gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten. Diese Datenschutzrichtlinie gilt in allen Bereichen des Unternehmens und beruht auf den Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist die Grundlage für vertrauensvolle Geschäftsbeziehungen und die Reputation des Unternehmens.

Die Datenschutzrichtlinie schafft eine der notwendigen Rahmenbedingungen für die Datenübermittlung. Sie gewährleistet das von der Europäischen Datenschutzrichtlinie und den nationalen Gesetzen verlangte angemessene Datenschutzniveau für den Datenverkehr.

2. Geltungsbereich und Änderung

Diese Datenschutzrichtlinie gilt für alle Unternehmen

Aqua Consulting & Maintenance
Tino Krebs
Neuwiesenstraße 8
97828 Marktheidenfeld

Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten.

Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzrichtlinie.

Eine Änderung dieser Datenschutzrichtlinie findet in Abstimmung mit dem Verantwortlichen für den Datenschutz innerhalb des für die Änderung von Richtlinien vorgegebenen Verfahrens statt. Die Änderungen werden unverzüglich gemeldet.

Die aktuelle Version der Datenschutzrichtlinie kann unter den Datenschutzhinweisen auf der Internetseite, www.tino-krebs.com, abgerufen werden.



Datenschutzrichtlinie

(Stand 2018-05-16)

3. Verarbeitung personenbezogener Daten

a.) Fairness und Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise und fair erhoben und verarbeitet werden.

b.) Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

c.) Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden.

Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- Die Identität der verantwortlichen Stelle
- Den Zweck der Datenverarbeitung
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden.

d.) Datenvermeidung und Datensparsamkeit

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

e.) Löschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde oder die Unternehmensarchive den Datenbestand auf seine Archivwürdigkeit für historische Zwecke bewerten konnten.

f.) Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.



Datenschutzrichtlinie

(Stand 2018-05-16)

g.) Vertraulichkeit und Datensicherheit

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

4. Zulässige Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung und Änderung personenbezogener Daten ist nur zulässig, wenn einer der folgenden Punkte vorliegt.

a.) Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrages – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten. Für darüber hinausgehende Werbemaßnahmen müssen die folgenden Voraussetzungen unter 4 b.) beachtet werden.

b.) Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an das Unternehmen (z.B. Wunsch nach Zusendung von Informationsmaterial oder Kontaktaufnahme), so ist die Datenverarbeitung für die Erfüllung dieses Anliegen zulässig.

Kundenbindungs- oder Werbemaßnahmen bedürfen weiterer rechtlicher Voraussetzungen.

Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Werbung zu informieren. Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene soll über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert werden. Im Rahmen der Kommunikation mit dem Betroffenen soll eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Werbezwecken eingeholt werden. Der Betroffene soll im Rahmen der Einwilligung zwischen den verfügbaren Kontaktkanälen wie Post, elektronische Post und Telefon wählen können.

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden.



Datenschutzrichtlinie

(Stand 2018-05-16)

- c.) **Einwilligung in die Datenverarbeitung**
Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäß dieser Datenschutzrichtlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die **Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden.**
- d.) **Datenverarbeitung aufgrund gesetzlicher Erlaubnis**
Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.
- e.) **Datenverarbeitung aufgrund berechtigten Interesses**
Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses des Unternehmens erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.
- f.) **Verarbeitung besonders schutzwürdiger Daten**
Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Beauftragte für den Datenschutz im Vorfeld zu informieren.
- g.) **Automatisierte Einzelentscheidungen**
Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein. Dem Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden. Zur Vermeidung von Fehlentscheidungen muss eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeiter gewährleistet werden.
- h.) **Nutzerdaten und Internet**
Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. Cookie Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind. Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden. Ein personenbezogenes



Datenschutzrichtlinie

(Stand 2018-05-16)

Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden.

Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

5. Mitarbeiterdaten

a.) Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt.

Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.

Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

b.) Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

c.) Kollektivregelungen für Datenverarbeitungen

Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird. Kollektivregelungen sind Tarifverträge oder Vereinbarungen zwischen Arbeitgeber und Arbeitnehmer im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des staatlichen Datenschutzrechts gestaltbar.



Datenschutzrichtlinie

(Stand 2018-05-16)

- d.) **Einwilligung in die Datenverarbeitung**
Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene gemäß dieser Datenschutzrichtlinie informiert werden.
- e.) **Datenverarbeitung aufgrund berechtigten Interesses**
Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses des Unternehmens erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich (z.B. Bewertung von Unternehmen) begründet. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen. Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen berücksichtigt werden.
- f.) **Verarbeitung besonders schutzwürdiger Daten**
Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen.



Datenschutzrichtlinie

(Stand 2018-05-16)

Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Beauftragte für den Datenschutz im Vorfeld zu informieren.

g.) Automatisierte Entscheidungen

Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (z.B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiter sein. Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist. Dem betroffenen Mitarbeiter muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

h.) Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen und Internet werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden. Im Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das jeweils nationale geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden. Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation und Internet Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen an den Übergängen in das Unternehmens-Netzwerk implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen und Internets zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien des Unternehmens erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Unternehmensregelungen.

6. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb des Unternehmens oder an Empfänger innerhalb des Unternehmens unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Punkt 4. Im Falle einer Datenübermittlung an einen Empfänger außerhalb des Unternehmens Drittstaat muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Eine solche gesetzliche Verpflichtung kann sich aus dem Recht des Sitzlandes der Konzerngesellschaft, welche die Daten übermittelt, ergeben oder das Recht des Sitzlandes der Konzerngesellschaft erkennt das mit der gesetzlichen Verpflichtung eines Drittstaats verfolgte Ziel der Datenübermittlung an.



Datenschutzrichtlinie

(Stand 2018-05-16)

7. Rechte der Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

- a.) Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.
- b.) Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.
- c.) Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
- d.) Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.
- e.) Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.
- f.) Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

8. Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein.

Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten. Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Vorgesetzte müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses



Datenschutzrichtlinie

(Stand 2018-05-16)

unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

9. Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

10. Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem Beauftragten oder beauftragten externen Prüfern.

Die Ergebnisse der Datenschutzkontrollen sind dem Konzernbeauftragten für den Datenschutz mitzuteilen.

Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zu stehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

11. Datenschutzvorfälle

Jeder Mitarbeiter soll dem Beauftragten für den Datenschutz unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) melden. Die für die Funktion oder die Einheit verantwortliche Führungskraft ist verpflichtet, dem Beauftragten für den Datenschutz umgehend über Datenschutzvorfälle zu unterrichten. In Fällen von unrechtmäßiger Übermittlung personenbezogener Daten an Dritte, unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder bei Verlust personenbezogener Daten ist unverzüglich der Beauftragte zu unterrichten, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.