Konzernrichtlinie Datenschutz

Richtlinie zum Schutz der Persönlichkeitsrechte im Umgang mit personenbezogenen Daten in der Telio Group

Inhaltsverzeichnis

I. Präambel

Der Schutz personenbezogener Daten von Kunden, Mitarbeitern und anderen Personen, die mit der Telio Group in Verbindung stehen, ist ein maßgebliches Ziel aller Unternehmen der Telio Group.

Die Unternehmen der Telio Group sind sich bewusst, dass der Erfolg der Telio Group im Ganzen nicht nur von der globalen Vernetzung von Informationsflüssen, sondern vor allem auch vom vertrauensvollen und sicheren Umgang mit personenbezogenen Daten abhängt.

In vielen Bereichen wird die Telio Group aus Sicht ihrer Kunden und der Öffentlichkeit als eine Einheit wahrgenommen. Es ist deshalb das gemeinsame Anliegen der Unternehmen der Telio Group, durch die Umsetzung dieser Konzernrichtlinie einen wichtigen Beitrag zum gemeinsamen unternehmerischen Erfolg zu leisten und den Anspruch der Telio Group als Anbieter qualitativ hochwertiger und zukunftsweisender Produkte und Dienstleistungen zu unterstützen.

Mit dieser Konzernrichtlinie schafft die Telio Group ein weltweit einheitliches und hohes Datenschutzniveau. Sowohl für die unternehmensinterne, wie auch die unternehmensübergreifende Datenverwendung und sowohl für die nationale, wie die internationale Datenübermittlung. Personenbezogene Daten müssen in der Telio Group beim Empfänger von Daten entsprechend den datenschutzrechtlichen Grundsätzen verarbeitet werden, die nach der DSGVO und den weiteren Rechtsgrundlagen gelten.

II. Geltungsbereich

1. Rechtsnatur der Konzernrichtlinie Datenschutz

Die Konzernrichtlinie Datenschutz ist eine bindende Konzernrichtlinie für den Umgang mit personenbezogenen Daten. Sie gilt für alle Unternehmen der Telio Group, welche sie rechtsverbindlich in Kraft gesetzt haben. Gleiches gilt für Unternehmen, bei denen die Telio Management GmbH das Recht hat, die Übernahme dieser Konzernrichtlinie zu verlangen oder bei denen sie von den Unternehmen freiwillig übernommen wurde. Dies gilt unabhängig vom Ort der Datenerhebung.

2. Anwendungsbereich

Die Konzernrichtlinie Datenschutz gilt für alle Arten der Verwendung von personenbezogenen Daten in der Telio Group, unabhängig vom Ort ihrer Erhebung. Personenbezogene Daten werden in der Telio Group insbesondere zu folgenden Zwecken verwendet:

Zur Verwaltung von Beschäftigtendaten im Rahmen der Anbahnung, Durchführung und Abwicklung von Arbeitsverhältnissen sowie zur Ansprache der Beschäftigten zur Vorstellung von Produkten und Dienstleistungen, die die Telio Group oder Dritte den Beschäftigten darüber hinaus anbieten.

Durchführung und Abwicklung von Auftragsverarbeitungen im Rahmen des Angebots haft- und maßregelvollzugsinterner Telefonie.

Durchführung und Abwicklung von Dienstleistungen auf MYPHONIO im Rahmen der Einzahlungen von Geldbeträgen auf Telefoniekonten.

Zum ordnungsgemäßen Umgang mit sonstigen Dritten, insbesondere Gesellschaftern oder Besuchern, sowie zur Erfüllung zwingender gesetzlicher Vorschriften.

Die Verwendung der Daten findet im Rahmen der derzeitigen und zukünftigen Geschäftszwecke der Unternehmen der Telio Group statt, das sind unter anderem Telekommunikation und digitale Services für Insassen von Haftanstalten oder Personen, die sich im Maßregelvollzug befinden sowie IT-Services einschließlich und Beratungsleistungen.

3. Verhältnis zu anderen Rechtsvorschriften

Die Bestimmungen der Konzernrichtlinie Datenschutz sollen ein einheitlich hohes Datenschutzniveau in der gesamten Telio Group gewährleisten. Für einzelne Unternehmen bestehende Verpflichtungen und Regelungen zur Verarbeitung und Nutzung personenbezogener Daten, die über die hier geregelten Grundsätze hinausgehen bzw. zusätzliche Beschränkungen für die Verarbeitung und Nutzung personenbezogener Daten enthalten, bleiben von dieser Konzernrichtlinie unberührt.

Für die in Europa erhobenen Daten, richten sich die Anforderungen an die datenschutzkonforme Verwendung der Daten grundsätzlich und unabhängig vom Ort der Verwendung nach den gesetzlichen Regelungen der DSGVO, sowie nach den gesetzlichen Regelungen des Landes in dem die Daten erhoben wurden, mindestens jedoch nach den Anforderungen in dieser Konzernrichtlinie Datenschutz.

Die Geltung nationaler Vorschriften, die aus Gründen der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit sowie der Verhütung, Ermittlung und Verfolgung von Straftaten erlassen wurden und zur Weitergabe von Daten an Dritte verpflichten, bleibt von den Regelungen in dieser Konzernrichtlinie Datenschutz unberührt. Sollte ein Unternehmen feststellen, dass wesentliche Teile dieser Konzernrichtlinie landesgesetzlichen Datenschutzbestimmungen widersprechen und dies der Unterzeichnung der Konzernrichtlinie entgegensteht, ist der Konzerndatenschutzbeauftragte der Telio Group unverzüglich zu unterrichten. Die zuständige Aufsichtsbehörde des Unternehmens ist vermittelnd mit einzubeziehen.

4. Beendigung und Kündigung

Die Bindungswirkung dieser Konzernrichtlinie endet, wenn ein Unternehmen die Telio Group verlässt oder die Konzernrichtlinie außer Kraft setzt. Die Beendigung oder Außerkraftsetzung der Konzernrichtlinie befreit das Unternehmen jedoch nicht von den Verpflichtungen und/oder Regelungen dieser Konzernrichtlinie Datenschutz für die Verwendung bereits übermittelter Daten. Jeder weitere Datentransfer von oder zu diesem Unternehmen kann nur stattfinden, wenn andere

angemessene Verfahrensgarantien gemäß den Anforderungen des Europäischen Rechts eingehalten werden.

III. Transparenz der Datenverarbeitung

1. Informationspflicht

Die Betroffenen werden über die Verwendung ihrer personenbezogenen Daten vom Verantwortlichen entsprechend den gesetzlichen Regelungen sowie den nachfolgenden Bestimmungen informiert.

2. Inhalt und Gestaltung der Information

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

1. den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
2. gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
3. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
4. wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
5. gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
6. gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

1. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

2. das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

3. wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

4. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

5. ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

6. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

3. Verfügbarkeit von Informationen

Die Informationen müssen den Betroffenen bei der Erhebung der Daten sowie danach stets bei Bedarf zur Verfügung stehen.

IV. Zulässigkeitsvoraussetzungen für die Verwendung personenbezogener Daten

1. Grundsatz

Personenbezogene Daten dürfen nur nach Maßgabe der nachfolgenden Bestimmungen und nur für die Zwecke verwendet werden, für die sie ursprünglich erhoben wurden.

Die Verwendung von bereits erhobenen Daten für andere Zwecke ist nur dann zulässig, wenn dafür die Zulässigkeitsvoraussetzungen nach Maßgabe der folgenden Bestimmungen vorliegen.

2. Zulässigkeit der Verwendung personenbezogener Daten

Die Verwendung personenbezogener Daten darf erfolgen, wenn eine oder mehrere der folgenden Voraussetzungen erfüllt sind:

a. Sie ist ausdrücklich gesetzlich zulässig.
b. Der Betroffene hat in die Verwendung seiner Daten eingewilligt.
c. Die Verwendung der Daten ist erforderlich für die Erfüllung der Verpflichtungen des Unternehmens aus einem Vertrag mit dem Betroffenen, einschließlich der vertraglichen Informations- und/oder Nebenpflichten, oder für die Durchführung von vor- und/oder nachvertraglicher Maßnahmen, die der Anbahnung oder Abwicklung des Vertragsverhältnisses auf Antrag der betroffenen Person erfolgen.
d. Die Verwendung der Daten ist für die Erfüllung einer gesetzlichen bzw. rechtlichen Verpflichtung erforderlich, der das Unternehmen unterliegt.
e. Die Verwendung der Daten ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person.
f. Die Verwendung der Daten ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und die dem Unternehmen oder dem Dritten, dem die Daten übermittelt werden, auferlegt wurde.
g. Die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem Unternehmen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das schutzwürdige Interesse des Betroffenen offensichtlich überwiegt.

3. Einwilligung des Betroffenen

Die Einwilligung des Betroffenen gemäß dieser Konzernrichtlinie ist wirksam wenn:

a. Die Einwilligung ausdrücklich und freiwillig erfolgt ist und auf einer informierten Grundlage beruht, welche dem Betroffenen insbesondere die Reichweite der Einwilligung aufzeigt.
   Die Einwilligungserklärung muss hinreichend bestimmt sein und den Betroffenen über sein jederzeitiges Widerrufsrecht informieren. Bei Geschäftsmodellen bei denen der Widerruf dazu führt, dass vertragliche Pflichten nicht erfüllt werden können, ist der Betroffene darüber zu informieren.
b. Die Einholung der Einwilligung in einer den Umständen angemessenen Form (Textform) erfolgt. Sie kann in Ausnahmefällen mündlich erfolgen, wenn hierbei die Tatsache der Einwilligung sowie die besonderen Umstände, die die mündliche Einwilligung angemessen erscheinen lassen, ausreichend dokumentiert werden.

4. Automatisierte Einzelentscheidungen

a. Entscheidungen, die einzelne Aspekte einer Person bewerten und für die Betroffenen möglicherweise rechtliche Folgen nach sich ziehen oder sie erheblich beeinträchtigen

können, dürfen nicht ausschließlich auf eine automatisierte Verwendung von Daten gestützt werden. Hierzu gehören insbesondere Entscheidungen für die die Daten über die Kreditwürdigkeit, die berufliche Leistungsfähigkeit oder den Gesundheitszustand des Betroffenen maßgeblich sind.

b. Sofern im Einzelfall die sachliche Notwendigkeit zur Vornahme automatisierter Entscheidungen besteht, ist der Betroffene über das Ergebnis der automatisierten Entscheidung zu informieren. Er muss die Möglichkeit zur Stellungnahme innerhalb einer angemessenen Frist haben. Die Stellungnahme ist angemessen zu berücksichtigen, bevor eine endgültige Entscheidung getroffen wird.

5. Besondere Arten personenbezogener Daten

a. Die Verwendung besonderer Arten von personenbezogenen Daten ist nur zulässig, wenn sie einer gesetzlichen Regelung unterliegen oder die vorherige Einwilligung des Betroffenen vorliegt. Sie kann auch erfolgen, wenn die Verarbeitung erforderlich ist, um den Rechten und Pflichten des Unternehmens auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern angemessene Schutzmaßnahmen ergriffen werden und die Verwendung aufgrund einzelstaatlichen Rechts nicht untersagt ist.

b. Vor Beginn einer solchen Erhebung, Verarbeitung oder Nutzung hat das Unternehmen den Datenschutzbeauftragten des Unternehmens zu unterrichten und dies zu dokumentieren. Bei der Beurteilung der Zulässigkeit sollen insbesondere Art, Umfang, Zweck, das Erfordernis und die Rechtsgrundlage der Verwendung der Daten berücksichtigt werden.

6. Datensparsamkeit, Datenvermeidung, Anonymisierung und Pseudonymisierung

a. Personenbezogene Daten müssen unter Berücksichtigung der Zweckbestimmung ihrer Verwendung angemessen und relevant sein und dürfen den erforderlichen Umfang nicht übersteigen (Datensparsamkeit). Daten dürfen im Rahmen einer bestimmten Anwendung nur dann verarbeitet werden, wenn dies erforderlich ist (Datenvermeidung).

b. In den Fällen, in denen es möglich und wirtschaftlich zumutbar ist, sind Verfahren zur Löschung der Identifikationsmerkmale der Betroffenen (Anonymisierung) bzw. zur Ersetzung der Identifikationsmerkmale durch andere Kennzeichen (Pseudonymisierung) einzusetzen.

7. Koppelungsverbot

Die Inanspruchnahme von Dienstleistungen oder der Erhalt von Produkten und/oder Dienstleistungen dürfen nicht davon abhängig gemacht werden, dass der Betroffene in die Verwendung seiner Daten für andere Zwecke einwilligt, als für die Zwecke der Vertragsbegründung und -erfüllung. Dies gilt nur dann, wenn dem Betroffenen die Inanspruchnahme vergleichbarer Dienstleistungen bzw. die Nutzung vergleichbarer Produkte nicht oder in nicht zumutbarer Weise möglich ist.

V. Weitergabe personenbezogener Daten

1. Arten und Zwecke der Weitergabe von personenbezogenen Daten

Personenbezogene Daten können derart weitergegeben werden, dass die empfangende Stelle für die erhaltenen Daten eigenverantwortlich ist (Übermittlung), oder dass sie die Daten nur nach Weisung und Maßgabe der weitergebenden Stelle verwenden darf (Auftragsdatenvereinbarung).

Die Weitergabe von personenbezogenen Daten erfolgt ausschließlich zu den zulässigen Zwecken gemäß dieser Konzernrichtlinie im Rahmen der geschäftsgegenständlichen Ausrichtung der Unternehmen, ihrer rechtlichen Verpflichtungen oder den Einwilligungen der betroffenen Personen.

2. Übermittlung von Daten

a. Wenn ein Unternehmen Daten an Stellen übermittelt, die ihren Sitz in einem Drittland haben oder die grenzüberschreitenden Datentransfer ausüben, muss sichergestellt werden, dass diese Daten in rechtmäßiger Art und Weise übertragen werden. Vor der Übertragung müssen angemessene Datenschutz- und Datensicherheitsanforderungen mit dem Empfänger vereinbart werden. Personenbezogene Daten, insbesondere die in der EU bzw. EWR erhobenen, dürfen an Stellen außerhalb der Europäischen Union zudem nur übermittelt werden, wenn das angemessene Datenschutzniveau durch diese Konzernrichtlinie Datenschutz oder durch andere angemessene Maßnahmen sichergestellt wurde. Dies können die EU-Standardvertragsklauseln oder vertragliche Individualvereinbarungen sein, die den Anforderungen aus dem europäischen Recht genügen.
b. Auf Grundlage der Vorgaben der Telio Group sowie der allgemein anerkannten technischen und organisatorischen Standards, müssen angemessene technische und organisatorische Maßnahmen getroffen werden, um den Schutz der personenbezogenen Daten auch während ihrer Übermittlung an eine andere Stelle sicherzustellen.

3. Datenverarbeitung im Auftrag

a. Wird eine andere Stelle (Auftragnehmer) im Auftrag eines Unternehmens (Auftraggeber) nach dessen Weisung und für dessen Zwecke tätig, so ist neben den zu erbringenden Dienstleistungen im Vertrag auch auf die Verpflichtungen des Auftragnehmers als Auftragsdatenverarbeiter Bezug zu nehmen. In diesen Verpflichtungen werden die Anweisungen des Auftraggebers bezüglich der Art und Weise der Verarbeitung der personenbezogenen Daten, dem Zweck der Verarbeitung und den erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten festgelegt.
b. Ohne die vorherige Zustimmung des Auftraggebers darf der Auftragnehmer die ihm zur Auftragserfüllung überlassenen personenbezogenen Daten nicht für eigene oder fremde Zwecke verwenden. Die Einbindung von Unterauftragnehmern durch den Auftragnehmer zur Erfüllung der vertraglichen Verpflichtungen bedarf der vorherigen Information des

Auftraggebers. Der Auftraggeber hat ein Widerspruchsrecht gegen die Beauftragung von Unterauftragnehmern. Bei der zulässigen Einbindung von Unterauftragnehmern hat der Auftragnehmer den Unterauftragnehmer auf die Vereinbarungen, die zwischen dem Auftragnehmer und dem Auftraggeber getroffen wurden, entsprechend zu verpflichten.

c. Die Auftragnehmer sind von den Unternehmen nach ihrer Fähigkeit, die oben genannten Anforderungen zu erfüllen, auszuwählen.

VI. Datenqualität und Datensicherheit

1. Datenqualität

a. Personenbezogene Daten müssen korrekt sein und sind soweit erforderlich auf dem jeweils aktuellen Stand zu halten (Datenqualität).
b. Unter Beachtung des Verwendungszwecks der Daten sind angemessene Maßnahmen dafür zu treffen, dass unrichtige oder unvollständige Daten gelöscht, gesperrt oder gegebenenfalls berichtigt werden.

2. Datensicherheit - Technische und organisatorische Maßnahmen

Für die Unternehmensprozesse, IT-Systeme und Plattformen in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, müssen die Unternehmen zum Schutz der Daten angemessene technische und organisatorische Maßnahmen treffen.

Zu diesen Maßnahmen gehören:

a. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
b. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
c. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
d. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Kontrolle der Weitergabe),
e. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

f. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Kontrolle des Auftragnehmers),
g. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
h. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungsgebot).

VII. Rechte des Betroffenen

1. Auskunftsrecht

Jeder Betroffene kann gegenüber jeder verantwortlichen Stelle, das seine Daten verwendet, jederzeit Auskunft verlangen über:

a. die zu seiner Person gespeicherten Daten, inklusive ihrer Herkunft und Empfänger,
b. den Zweck der Verwendung der Daten,
c. die Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, insbesondere soweit es sich um eine Übermittlung ins Ausland handelt,
d. die Regelungen dieser Konzernrichtlinie Datenschutz.

Die Auskunft ist dem Betroffenen in angemessener Frist in verständlicher Form zu erteilen. Sie erfolgt in der Regel schriftlich oder elektronisch. Die Information über die Regelungen dieser Konzernrichtlinie Datenschutz kann durch Überlassen einer Textfassung der Konzernrichtlinie erfolgen.

Die Unternehmen können für die Auskunftserteilung eine Gebühr verlangen, wenn und soweit dies nach Maßgabe des jeweiligen Landesrechts zulässig ist.

2. Widerspruchsrecht und Recht auf Löschung, Sperrung und Berichtigung

Der Betroffene kann der Verwendung seiner Daten gegenüber der verantwortlichen Stelle jederzeit widersprechen, wenn sie nicht zu gesetzlich zwingenden Zwecken verwendet werden.

Das Widerspruchsrecht gilt auch für den Fall, dass der Betroffene zuvor seine Einwilligung zur Verwendung seiner Daten gegeben hat.

Berechtigten Ersuchen zur Löschung oder Sperrung von Daten ist unverzüglich nachzukommen. Ein solches Ersuchen ist insbesondere dann berechtigt, wenn die rechtliche Grundlage für die Verwendung der Daten weggefallen ist. Falls ein Recht auf Löschung der Daten besteht, eine Löschung aber nicht möglich oder unzumutbar ist, sind die Daten für nicht zulässige Verwendungen zu sperren. Gesetzliche Aufbewahrungsfristen sind zu beachten.

Der Betroffene kann vom Unternehmen jederzeit die Berichtigung der zu seiner Person gespeicherten Daten verlangen, sofern diese unvollständig und/oder unrichtig sind.

Bei Geschäftsmodellen bei denen der Widerspruch oder die Löschung dazu führt, dass vertragliche Pflichten nicht erfüllt werden können, ist der Betroffene darüber zu informieren.

3. Recht auf Klärung, Stellungnahme und Abhilfe

Macht ein Betroffener eine Verletzung seiner Rechte durch unzulässige Verwendung seiner Daten, insbesondere in Form eines nachweislichen Verstoßes gegen diese Konzernrichtlinie geltend, so haben die zuständigen Unternehmen den Sachverhalt ohne schuldhaftes Zögern aufzuklären. Insbesondere bei einer Weitergabe oder Übermittlung von Daten an Unternehmen außerhalb der Europäischen Union hat das in der Europäischen Union ansässige Unternehmen den Sachverhalt aufzuklären und den Beweis zu erbringen, dass die Stelle, die die Daten empfangen hat, nicht gegen diese Konzernrichtlinie verstoßen hat oder verantwortlich für einen entstandenen Schaden ist. Die Unternehmen arbeiten bei der Sachverhaltsfeststellung eng zusammen und gewähren sich gegenseitig Zugang zu allen dafür erforderlichen Informationen.

Der Betroffene kann gegenüber den Unternehmen der Telio Group jederzeit Beschwerde einreichen, wenn der Verdacht besteht, dass ein Unternehmen der Telio Group seine personenbezogenen Daten nicht gemäß den Gesetzen oder den Bestimmungen dieser Konzernrichtlinie verarbeitet. Über die Beschwerde ist der Konzerndatenschutzbeauftragte zu informieren und zur Bearbeitung hinzuzuziehen. Der begründeten Beschwerde wird innerhalb eines angemessenen Zeitraums abgeholfen und der Betroffene entsprechend informiert.

Sind von einer Beschwerde mehrere Unternehmen betroffen, koordiniert der Konzerndatenschutzbeauftragte die gesamte einschlägige Korrespondenz mit dem Betroffenen. Der Konzerndatenschutzbeauftragte hat ein jederzeitiges Eintritts- und Übernahmerecht.

Meldungen zu einem Datenschutzvorfall müssen in geeigneter Weise (z.B. über ein Funktionspostfach des Datenschutzbereiches oder Nennung eines direkten Ansprechpartners im Internet) erfolgen können.

Der Datenschutzkoordinator des betroffenen Unternehmens hat den Konzerndatenschutzbeauftragten über einen Datenschutzvorfall anhand der dafür vorgesehenen Meldeprozesse unverzüglich zu informieren.

4. Frage- und Beschwerderecht

Jeder Betroffene hat das Recht, sich jederzeit mit Fragen und Beschwerden zur Anwendung dieser Konzernrichtlinie an den Konzerndatenschutzbeauftragten der Telio Group zu wenden. Das Unternehmen mit der größten Sachnähe oder das Unternehmen, von dem die Daten des Betroffenen erhoben wurden, sorgt für die Umsetzung der Rechte des Betroffenen bei den anderen zuständigen Unternehmen.

5. Ausübung der Rechte des Betroffenen

Betroffene dürfen wegen der Inanspruchnahme der hier beschriebenen Rechte nicht benachteiligt werden. Die Art und Weise der Kommunikation mit dem Betroffenen – z.B. telefonisch, elektronisch oder schriftlich – sollte, soweit dies angemessen ist, dem Wunsch des Betroffenen entsprechen.

6. Textfassung der Konzernrichtlinie

Jedermann bekommt auf Anfrage eine Textfassung dieser Konzernrichtlinie Datenschutz zugesandt.

VIII. Datenschutzorganisation

1. Verantwortung für die Datenverarbeitung

Die Unternehmen sind verpflichtet, die Einhaltung der gesetzlichen Datenschutzbestimmungen und dieser Konzernrichtlinie Datenschutz sicherzustellen.

2. Datenschutzbeauftragte

Es ist ein unabhängiger Konzerndatenschutzbeauftragter zu bestellen. Dieser hat die Aufgabe, die Beratung der verschiedenen Organisationseinheiten der Telio Group über die gesetzlichen sowie unternehmens- und konzerninternen Vorgaben zum Datenschutz und insbesondere diese Konzernrichtlinie Datenschutz sicherzustellen. Der Datenschutzbeauftragte überwacht die Einhaltung der Datenschutzvorschriften durch geeignete Maßnahmen, insbesondere stichprobenartige Kontrollen.

Der Verantwortliche stellt sicher, dass der Datenschutzbeauftragte die erforderlichen Kompetenzen zur rechtlichen, technischen und organisatorischen Bewertung von datenschutzrelevanten Maßnahmen hat.

Der Konzerndatenschutzbeauftragte ist für die Ausübung seiner Aufgaben vom Verantwortlichen mit angemessenen finanziellen und personellen Mitteln auszustatten.

Dem Datenschutzbeauftragten ist ein direktes Berichtsrecht an die Unternehmensleitung einzuräumen. Er ist organisatorisch an die Unternehmensleitung anzubinden.

Die Umsetzung der Vorgaben des Konzerndatenschutzbeauftragten und der Datenschutzstrategie der Telio Group obliegt dem Verantwortlichen.

Alle Bereiche der Unternehmen sind verpflichtet, den Datenschutzbeauftragten alle Entwicklungen zur IT-Infrastruktur, zur Netzinfrastruktur, zu Geschäftsmodellen, Produkten, Personaldatenverarbeitungen sowie den zugehörigen strategischen Planungen zu unterrichten. Der Datenschutzbeauftragte ist bei neuen Entwicklungen frühzeitig zu beteiligen, um sicherzustellen, dass jegliche Datenschutzbelange berücksichtigt und bewertet werden.

Der Konzerndatenschutzbeauftragte koordiniert die Zusammenarbeit und Abstimmung zu allen wichtigen Fragen des Datenschutzes in der Telio Group. Er informiert bei Bedarf den Vorstand zu den aktuellen Entwicklungen oder formuliert Empfehlungen.

Es obliegt dem Konzerndatenschutzbeauftragten den Verantwortlichen bei der Entwicklung der Datenschutzpolitik der Telio Group zu beraten. Das Datenschutzteam wird dabei angemessen eingebunden. Ein gemeinsamer Austausch zwischen dem Konzerndatenschutzbeauftragten und dem Datenschutzteam findet viermal jährlich statt.

3. Informationspflicht bei Verstößen

Der Datenschutzbeauftragte ist vom betroffenen Unternehmen unverzüglich über Verstöße oder konkrete Anhaltspunkte für einen Verstoß gegen Datenschutzbestimmungen, insbesondere auch dieser Konzernrichtlinie Datenschutz, zu informieren. Der Datenschutzkoordinator der Unternehmen informiert den Konzerndatenschutzbeauftragten ferner, wenn die für ein Unternehmen geltenden Gesetze sich wesentlich nachteilig im Sinne dieser Konzernrichtlinie ändern.

4. Überprüfungen des Datenschutzniveaus

Überprüfungen der Einhaltung der Vorgaben dieser Konzernrichtlinie und des sich daraus abzuleitenden Datenschutzniveaus erfolgen durch Kontrollen, die vom Konzerndatenschutzbeauftragten anhand eines jährlichen Kontrollplans durchgeführt werden, sowie durch andere Maßnahmen, wie etwa Kontrollen der Datenschutzkoordinatoren der Unternehmen oder Reports.

Werden im Rahmen einer Kontrolle Schwachstellen festgestellt, sind diese durch entsprechende Maßnahmen durch das Unternehmen zu beheben. Der Konzerndatenschutzbeauftragte begleitet beratend die Umsetzung der Maßnahmen. Sollten diese ohne ausreichende Begründung nicht umgesetzt werden, bewertet der Konzerndatenschutzbeauftragte die Auswirkungen auf den Datenschutz und leitet seine Erkenntnisse an den Verantwortlichen weiter.

Die Datenschutzkoordinatoren der Unternehmen oder andere mit einem Prüfungsauftrag ausgestattete Organisationseinheiten prüfen zusätzlich auf die Einhaltung der Belange des Datenschutzes auf Grundlage von bereitgestellten Checklisten durch den Verantwortlichen, die unter Hinzuziehung des Datenschutzbeauftragten erstellt wurden.

Sofern keine gesetzlichen Beschränkungen bestehen, ist der Konzerndatenschutzbeauftragte bei allen Unternehmen befugt, die ordnungsgemäße Verwendung von personenbezogenen Daten zu überprüfen. Dazu gewähren die Unternehmen umfassend Zutritt und Einsicht zu den Informationen, die der Konzerndatenschutzbeauftragte zur Aufklärung und Bewertung eines Sachverhalts für notwendig erachten. Der Konzerndatenschutzbeauftragte kann in diesem Zusammenhang Weisungen erteilen.

5. Mitarbeiterverpflichtung und Schulung

Die Unternehmen verpflichten ihre Mitarbeiter spätestens bei Aufnahme ihrer Tätigkeit auf das Daten- und Fernmeldegeheimnis. Im Rahmen der Verpflichtung werden die Mitarbeiter ausreichend auf die Belange des Datenschutzes geschult. Dafür richtet das Unternehmen geeignete Prozesse ein und stellt Materialien zur Verfügung.

Die Mitarbeiter werden regelmäßig, mindestens aber alle zwei Jahre auf die Grundlagen im Datenschutz geschult. Die Unternehmen können die Schulungen für die eigenen Mitarbeiter selbst entwickeln und durchführen. Die Durchführung der Schulungen ist vom HR-Verantwortlichen zu dokumentieren und an den Verantwortlichen, sowie den Konzerndatenschutzbeauftragten jährlich zu berichten.

Materialien und Prozesse können zur Verpflichtung und Schulung der Mitarbeiter der Telio Group zentral zur Verfügung gestellt werden.

6. Zusammenarbeit mit Aufsichtsbehörden

Die Unternehmen erklären sich damit einverstanden, mit der für sie oder das Daten übermittelnde Unternehmen zuständigen Aufsichtsbehörde vertrauensvoll zusammenzuarbeiten, insbesondere Anfragen zu beantworten und Empfehlungen aufzunehmen.

7. Zuständige Stellen für Kontakte und Anfragen

Zuständige Stelle für Kontakte und Anfragen zu dieser Konzernrichtlinie sind die Datenschutzkoordinatoren der Unternehmen oder der Konzerndatenschutzbeauftragte. Der Konzerndatenschutzbeauftragte nennt auf Anfrage auch die Kontakte zu den Datenschutzkoordinatoren der Unternehmen.

Der Konzerndatenschutzbeauftragte ist über

Data.Protection.Officer@tel.io

Erreichbar.

IX. Schlussbestimmungen

1. Überprüfung und Überarbeitung dieser Konzernrichtlinie

Der Konzerndatenschutzbeauftragte überprüft die Konzernrichtlinie Datenschutz in regelmäßigen Abständen, mindestens jedoch einmal jährlich, auf deren Vereinbarkeit mit den geltenden Gesetzen und berät bei deren Anpassung durch den Verantwortlichen.

Der Konzerndatenschutzbeauftragte informiert alle Unternehmen, die die Konzernrichtlinie Datenschutz verbindlich eingeführt haben, über die inhaltlichen Änderungen.

2. Ansprechpartner- und Unternehmensliste

Der Konzerndatenschutzbeauftragte führt eine Liste der Unternehmen, die diese Konzernrichtlinie verbindlich eingeführt haben und deren Ansprechpartner. Er hält diese aktuell und informiert Betroffene bzw. die Datenschutzbehörde auf Anfrage.

3. Verfahrensrecht / Salvatorische Klausel

Die Konzernrichtlinie unterliegt in Streitfragen dem Verfahrensrecht der Bundesrepublik Deutschland.

Sollten einzelne Bestimmungen dieser Konzernrichtlinie unwirksam sein oder werden, gelten sie als durch Bestimmungen ersetzt, die dem ursprünglichen Gedanken dieser Konzernrichtlinie und der weggefallenen Bestimmung am nächsten kommt. Im Zweifel gelten in diesen Fällen oder im Fall einer fehlenden Regelung die einschlägigen Regelungen der europäischen Union zum Datenschutz entsprechend.