

Konzernrichtlinie Datenschutz– Binding Corporate Rules Privacy (BCRP)

Richtlinie zum Schutz der Persönlichkeitsrechte im
Umgang mit personenbezogenen Daten in der
Deutschen Telekom Gruppe

Version 3.0 (final)

vom 29.12.2023

Öffentlich



Connecting
your world.

Impressum

HerausgeberTelekom

Deutsche Telekom AG
Group Privacy
Friedrich-Ebert-Allee 140, 53113 Bonn

Dateiname	Dokumentennummer	Dokumentenbezeichnung
Konzernrichtlinie Datenschutz_BCRP	2.9	Konzernrichtlinie Datenschutz (BCRP)
Version	Stand	Status
3.0	29.12.2023I	
Autor*in	Inhaltlich geprüft von	Freigegeben von
Dr. Jörg Friedrichs	Jan Lichtenberg, Strategy & Steering	Dr. Claus-Dieter Ulmer, Group Privacy Officer
Bonn, 27.10.2023	Bonn, 30.10.2023	Bonn, 31.10.2023

Kurzinfo

Regelung zum Umgang mit personenbezogenen Daten im Konzern

Änderungshistorie

Version	Stand	Bearbeiter*in	Änderungen/Kommentar
2.2	20.01.2013	Sonja Klauck	Überarbeitete Version des Privacy Code of Conducts deutsche Version 2.1
2.3	08.02.2013	Dr. Claus-Dieter Ulmer	Komplette Überarbeitung
2.4	14.02.2013	Dr. Claus-Dieter Ulmer	Datenweitergabe und Haftung
2.5	21.03.2013	Marcus Schmitz Dr. Claus-Dieter Ulmer	Überarbeitung mit den Anmerkungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
2.6	09.04.2013	Daniel Hoff	Überarbeitung mit den Anmerkungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
2.7	05.12.2013	Daniel Hoff Marcus Schmitz	Überarbeitung mit den Anmerkungen der Österreichischen Aufsichtsbehörde
2.8	19.02.2019	Dr. Jörg Friedrichs Christina Kreft-Spallek	Anpassung an die Datenschutz-Grundverordnung auf der Grundlage des WP 256 rev.01
3.0	29.12.2023	Dr. Jörg Friedrichs	Anpassung an Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)

Achtung:

Ein Ausdruck dieser Konzernrichtlinie könnte bereits veraltet sein. Bitte überprüfen Sie stets in der Richtliniendatenbank der Deutschen Telekom (<http://richtlinien.telekom.de>) ob es sich um die aktuelle Version der Konzernrichtlinie handelt.

Inhaltsverzeichnis

Präambel.....	6
Teil 1 Geltungsbereich	7
§ 1 Rechtsnatur der Konzernrichtlinie Datenschutz.....	7
§ 2 Anwendungsbereich	7
§ 3 Verhältnis zu anderen Rechtsvorschriften.....	7
§ 4 Beendigung und Kündigung	8
TEIL 2 GRUNDSÄTZE	9
Abschnitt 1 Transparenz der Datenverarbeitung	9
§ 5 Informationspflicht	9
§ 6 Inhalt und Gestaltung der Information	9
§ 7 Verfügbarkeit von Informationen.....	9
§ 8 Verzeichnis aller Kategorien von Verarbeitungstätigkeiten.....	9
Abschnitt 2 Zulässigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten	10
§ 9 Grundsatz	10
§ 10 Rechtmäßigkeit der Verarbeitung personenbezogener Daten	10
§ 11 Einwilligung des Betroffenen	10
§ 12 Automatisierte Einzelentscheidungen einschließlich Profiling	11
§ 13 Die Verarbeitung personenbezogener Daten für Direktmarketingzwecke.....	11
§ 14 Besondere Kategorien personenbezogener Daten	11
§ 15 Datenminimierung, Datenvermeidung, Speicherbegrenzung, Anonymisierung und Pseudonymisierung	11
§ 16 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.....	11
§ 17 Koppelungsverbot.....	12
Abschnitt 3 Übermittlung personenbezogener Daten	13
§ 18 Arten und Zwecke der Übermittlung von personenbezogenen Daten	13
§ 19 Übermittlung von Daten einschließlich Weiterübermittlung.....	13
§ 20 Pflichten des Empfängers im Falle des Zugangs von Behörden zu den Daten.....	13

§ 21 Datenverarbeitung im Auftrag	15
Abschnitt 4 Datenqualität und Datensicherheit.....	16
§ 22 Datenqualität	16
§ 23 Datensicherheit - Technische und organisatorische Maßnahmen – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.....	16
Teil 3 Rechte des Betroffenen.....	17
§ 24 Auskunftsrecht	17
§ 25 Widerspruchsrecht, Recht auf Löschung oder Einschränkung der Verarbeitung und Recht auf Berichtigung	17
§ 26 Recht auf Klärung, Stellungnahme und Abhilfe.....	17
§ 27 Frage- und Beschwerderecht	18
§ 28 Ausübung der Rechte des Betroffenen.....	18
§ 29 Textfassung der Konzernrichtlinie.....	18
Teil 4 Datenschutzorganisation	19
§ 30 Verantwortung für die Datenverarbeitung	19
§ 31 Datenschutzbeauftragte	19
§ 32 Konzerndatenschutzbeauftragter.....	19
§ 33 Informationspflicht bei Verstößen oder bei Änderungen der für ein Unternehmen geltenden Gesetze und Gepflogenheiten.....	20
§ 34 Überprüfungen des Datenschutzniveaus	20
§ 35 Datenschutz-Folgenabschätzung	21
§ 36 Mitarbeiterverpflichtung und Schulung	21
§ 37 Zusammenarbeit mit Aufsichtsbehörden.....	21
§ 38 Zuständige Stellen für Kontakte und Anfragen.....	21
Teil 5 Haftung	22
§ 39 Anwendungsbereich der Haftungsregelungen	22
§ 40 Haftungsschuldner	22
§ 41 Beweislast.....	22
§ 42 Drittbegünstigung für Betroffene.....	23
§ 43 Gerichtsstand.....	23
§ 44 Außergerichtliche Schlichtung	23
Teil 6 Schlussbestimmungen.....	24
§ 45 Überprüfung und Überarbeitung dieser Konzernrichtlinie	24
§ 46 Ansprechpartner- und Unternehmensliste	24
§ 47 Verfahrensrecht / Salvatorische Klausel.....	24

§ 48 Öffentliche Bekanntmachung	24
Teil 7 Definitionen und Begriffe.....	25
Liste der Unternehmen, die die Konzernrichtlinie Datenschutz verbindlich eingeführt haben	27

Präambel

- (1) Der Schutz personenbezogener Daten von Kunden, Mitarbeitern und anderen Personen, die mit der Deutschen Telekom Gruppe in Verbindung stehen, ist ein maßgebliches Ziel aller Unternehmen der Deutsche Telekom Gruppe.
- (2) Die Unternehmen der Deutschen Telekom Gruppe sind sich bewusst, dass der Erfolg der Deutschen Telekom im Ganzen nicht nur von der globalen Vernetzung von Informationsflüssen, sondern vor allem auch vom vertrauensvollen und sicheren Umgang mit personenbezogenen Daten abhängt.
- (3) In vielen Bereichen wird die Deutsche Telekom Gruppe aus Sicht ihrer Kunden und der Öffentlichkeit als eine Einheit wahrgenommen. Es ist deshalb das gemeinsame Anliegen der Unternehmen der Deutschen Telekom Gruppe, durch die Umsetzung dieser Konzernrichtlinie einen wichtigen Beitrag zum gemeinsamen unternehmerischen Erfolg zu leisten und den Anspruch der Deutschen Telekom Gruppe als Anbieter qualitativ hochwertiger und zukunftsweisender Produkte und Dienstleistungen zu unterstützen.
- (4) Mit dieser Konzernrichtlinie schafft die Deutschen Telekom Gruppe ein weltweit einheitliches und hohes Datenschutzniveau. Sowohl für die unternehmensinterne, wie auch die unternehmensübergreifende Datenverarbeitung und sowohl für die nationale, wie die internationale Datenübermittlung. Personenbezogene Daten müssen in der Deutschen Telekom Gruppe beim Empfänger von Daten entsprechend den datenschutzrechtlichen Grundsätzen verarbeitet werden, die für die übermittelnde Stelle gelten.

Hinweis:

Bei der Umsetzung dieser Konzernrichtlinie durch Einzelregelungen in den Unternehmen sind die jeweils bestehenden kollektivrechtlichen Regelungen und Beteiligungsrechte der zuständigen Arbeitnehmervertretungen zu beachten.

Teil 1

Geltungsbereich

§ 1 Rechtsnatur der Konzernrichtlinie Datenschutz

Die Konzernrichtlinie Datenschutz ist eine bindende Konzernrichtlinie für die Verarbeitung personenbezogener Daten (entsprechend den Recommendations 1/2022 des Europäischen Datenschutzausschusses). Sie gilt für alle Unternehmen der Deutschen Telekom Gruppe, welche sie rechtsverbindlich in Kraft gesetzt haben.

§ 2 Anwendungsbereich

Die Konzernrichtlinie Datenschutz gilt für alle Arten der Verarbeitung von personenbezogenen Daten in der Deutschen Telekom Gruppe, unabhängig vom Ort ihrer Erhebung. Personenbezogene Daten werden in der Deutschen Telekom Gruppe insbesondere zu folgenden Zwecken verarbeitet:

- a) 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 Deutsche Telekom Gruppe oder Dritte den Beschäftigten darüber hinaus anbieten.
- b) Zur Anbahnung, Durchführung und Abwicklung von Kundenverträgen im Geschäftskundenbereich und im Privatkundenmarkt sowie zur Werbung und Marktforschung, um Kunden und interessierte Dritte über die Produkte und Leistungen der Deutschen Telekom Gruppe oder Dritter bedarfsgerecht informieren zu können.
- c) Zur Anbahnung, Durchführung von Verträgen mit Dienstleistern der Deutschen Telekom Gruppe im Rahmen der Erbringung von Dienstleistungen für die Deutsche Telekom Gruppe.
- d) Zum ordnungsgemäßen Umgang mit sonstigen Dritten, insbesondere Aktionären, Gesellschaftern oder Besuchern, sowie zur Erfüllung zwingender gesetzlicher Vorschriften.

Die Verarbeitung der Daten findet im Rahmen der derzeitigen und zukünftigen Geschäftszwecke der Unternehmen der Deutschen Telekom Gruppe statt, das sind unter anderem Telekommunikation, digitale Services für den Privat- und Geschäftskundenmarkt, IT-Services einschließlich Rechenzentrumsdienstleistungen und Beratungsleistungen.

§ 3 Verhältnis zu anderen Rechtsvorschriften

- (1) Die Bestimmungen der Konzernrichtlinie Datenschutz sollen ein einheitlich hohes Datenschutzniveau in der gesamten Deutsche Telekom Gruppe gewährleisten. Für einzelne Unternehmen bestehende rechtliche Verpflichtungen und Regelungen zur Verarbeitung 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.
- (2) Für die im Europäischen Wirtschaftsraum erhobenen Daten richten sich die Anforderungen an die datenschutzkonforme Verarbeitung der Daten grundsätzlich und unabhängig vom Ort der Verarbeitung nach den gesetzlichen Regelungen des Staates, in dem die Daten erhoben wurden, mindestens jedoch nach den Anforderungen in dieser Konzernrichtlinie Datenschutz.
- (3) 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.
- (4) Sollte ein Unternehmen feststellen, dass wesentliche Teile dieser Konzernrichtlinie landesgesetzlichen Datenschutzbestimmungen widersprechen und dies der Einhaltung der Konzernrichtlinie entgegensteht, ist der Konzerndatenschutzbeauftragte der Deutschen Telekom

Gruppe 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 Deutsche Telekom Gruppe 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 Verarbeitung bereits übermittelter Daten. Jeder weitere Datentransfer von oder zu diesem Unternehmen kann nur stattfinden, wenn andere geeignete Garantien gemäß den Anforderungen des Europäischen Rechts eingehalten werden.

TEIL 2

GRUNDSÄTZE

Abschnitt 1

Transparenz der Datenverarbeitung

§ 5 Informationspflicht

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

§ 6 Inhalt und Gestaltung der Information

- (1) Das Unternehmen stellt den Betroffenen in geeigneter Weise folgende allgemeine Informationen zur Verfügung:
 - a) über die Identität des für die Verarbeitung Verantwortlichen sowie dessen Kontaktadresse;
 - b) die Kontaktdaten des Datenschutzbeauftragten;
 - c) über die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen; sowie die Rechtsgrundlage für die Verarbeitung und wie lange die Daten gespeichert werden,
 - d) bei Übermittlung personenbezogener Daten an Dritte, an wen und in welchem Umfang sowie zu welchem Zweck diese Übermittlung erfolgt;
 - e) über die Rechte, die sie im Zusammenhang mit der Verarbeitung der Daten haben.
- (2) Unabhängig vom gewählten Medium sollen die Informationen den Betroffenen auf eine eindeutige und leicht verständliche Weise gegeben werden.

§ 7 Verfügbarkeit von Informationen

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

§ 8 Verzeichnis aller Kategorien von Verarbeitungstätigkeiten

Die Unternehmen führen ein Verzeichnis aller Kategorien der von ihnen ausgeübten Verarbeitungstätigkeiten. Das Verzeichnis enthält folgende Angaben:

- a) den Namen und die Kontaktdaten des Unternehmens, des Vertreters sowie des Datenschutzbeauftragten;
- b) eine Beschreibung der Kategorien der Verarbeitungen und der Verarbeitungszwecke;
- c) die Kategorien von Empfängern und Dritten, an die die Daten offengelegt oder übermittelt werden;
- d) die Namen der Drittländer sowie die Dokumentation geeigneter Garantien, falls diese Konzernrichtlinie nicht zur Anwendung kommt;
- e) wenn möglich die Löschfristen und
- f) wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Abschnitt 2

Zulässigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten

§ 9 Grundsatz

- (1) Personenbezogene Daten dürfen nur nach Maßgabe der nachfolgenden Bestimmungen und nicht zu Zwecken verarbeitet werden, die mit denen, für die sie ursprünglich erhoben wurden, unvereinbar sind.
- (2) Die Verarbeitung von bereits erhobenen Daten für andere Zwecke ist nur dann zulässig, wenn dafür die Zulässigkeitsvoraussetzungen nach Maßgabe der folgenden Bestimmungen vorliegen (Zweckbindung).

§ 10 Rechtmäßigkeit der Verarbeitung personenbezogener Daten

Die Verarbeitung 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 Verarbeitung seiner Daten eingewilligt;
- c) die Verarbeitung 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 Verarbeitung der Daten ist für die Erfüllung einer gesetzlichen bzw. rechtlichen Verpflichtung erforderlich, der das Unternehmen unterliegt;
- e) die Verarbeitung der Daten ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;
- f) die Verarbeitung 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 überwiegt.

§ 11 Einwilligung des Betroffenen

Die Einwilligung des Betroffenen gemäß § 10 lit. b) 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.

§ 12 Automatisierte Einzelentscheidungen einschließlich Profiling

- (1) Entscheidungen, die einzelne Aspekte einer Person bewerten (Profiling) und für die Betroffenen möglicherweise rechtliche Folgen nach sich ziehen oder sie erheblich beeinträchtigen können, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung 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.
- (2) 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.

§ 13 Die Verarbeitung personenbezogener Daten für Direktmarketingzwecke

Bei der Verarbeitung von Daten für Direktmarketingzwecke sind die Betroffenen

- a) über die Art und Weise der Verarbeitung ihrer Daten für Zwecke des Direktmarketings zu unterrichten;
- b) darüber in Kenntnis zu setzen, dass sie jederzeit der Verarbeitung ihrer personenbezogenen Daten für Zwecke des Direktmarketings widersprechen können und
- c) in die Lage zu versetzen, ihr Widerspruchsrecht angemessen ausüben zu können, insbesondere müssen die Betroffenen Informationen über das Unternehmen, bei dem der Widerspruch einzulegen ist, erhalten.

§ 14 Besondere Kategorien personenbezogener Daten

- (1) Die Verarbeitung besonderer Kategorien von personenbezogenen Daten (vgl. Teil 7) ist nur zulässig, wenn sie einer gesetzlichen Regelung unterliegen oder die vorherige ausdrückliche 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 Verarbeitung aufgrund einzelstaatlichen Rechts nicht untersagt ist.
- (2) Vor Beginn einer solchen Verarbeitung 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 Verarbeitung der Daten berücksichtigt werden.

§ 15 Datenminimierung, Datenvermeidung, Speicherbegrenzung, Anonymisierung und Pseudonymisierung

- (1) Personenbezogene Daten müssen unter Berücksichtigung der Zweckbestimmung ihrer Verarbeitung angemessen und erheblich sein und dürfen den erforderlichen Umfang nicht übersteigen (Datenminimierung). Daten dürfen im Rahmen einer bestimmten Anwendung nur dann verarbeitet werden, wenn dies erforderlich ist (Datenvermeidung). Sie müssen in einer Form gespeichert werden, die die Identifizierung des Betroffenen nur solange ermöglicht, wie es für die Verarbeitungszwecke erforderlich ist (Speicherbegrenzung).
- (2) 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.

§ 16 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung von im Europäischen Wirtschaftsraum erhobener personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln

aufgrund von § 10 dieser Konzernrichtlinie darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

§ 17 Koppelungsverbot

Die Inanspruchnahme von Dienstleistungen oder der Erhalt von Produkten und/oder Dienstleistungen dürfen nicht davon abhängig gemacht werden, dass der Betroffene in die Verarbeitung 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.

Abschnitt 3

Übermittlung personenbezogener Daten

§ 18 Arten und Zwecke der Übermittlung von personenbezogenen Daten

- (1) Personenbezogene Daten können derart weitergegeben werden, dass die empfangende Stelle über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet oder dass sie die Daten nur nach Weisung und Maßgabe der weitergebenden Stelle verarbeiten darf.
- (2) Die Übermittlung von personenbezogenen Daten erfolgt ausschließlich zu den zulässigen Zwecken gemäß § 10 dieser Konzernrichtlinie im Rahmen der geschäftsgegenständlichen Ausrichtung der Unternehmen, ihrer rechtlichen Verpflichtungen oder von Einwilligungen der betroffenen Personen.
- (3) Personenbezogenen Daten dürfen nur übermittelt werden, wenn angemessene Datenschutz- und Datensicherheitsanforderungen mit dem Empfänger vereinbart sind.

§ 19 Übermittlung von Daten einschließlich Weiterübermittlung

- (1) Personenbezogene Daten, insbesondere die im Europäischen Wirtschaftsraum erhobenen, dürfen an Stellen außerhalb des Europäischen Wirtschaftsraums nur übermittelt werden, wenn das angemessene Datenschutzniveau durch diese Konzernrichtlinie Datenschutz oder durch andere geeignete Garantien sichergestellt wurde und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe im Sinne des Teil 5 dieser Konzernrichtlinie Datenschutz zur Verfügung stehen. Dies können die EU-Standardvertragsklauseln oder vertragliche Individualvereinbarungen sein, die den Anforderungen aus dem europäischen Recht genügen.
- (2) Dazu gehört, dass diese Konzernrichtlinie Datenschutz nach einem Transfer Impact Assessment nur dann als Übermittlungsinstrument verwendet wird, wenn ein Unternehmen festgestellt hat, dass die für die Verarbeitung personenbezogener Daten durch den Empfänger geltenden Rechtsvorschriften und Gepflogenheiten im Drittland den Empfänger nicht an der Einhaltung der Verpflichtungen aus dieser Konzernrichtlinie Datenschutz hindern. Diese Überprüfung hat ebenfalls die Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, zu berücksichtigen. Dies gilt für alle personenbezogenen Daten, die an Unternehmen außerhalb des Europäischen Wirtschaftsraums übermittelt werden, und für Weiterübermittlungen von Unternehmen in Drittländern an Unternehmen im selben oder einem anderen Drittland.
- (3) Ein Unternehmen, das personenbezogene Daten übermittelt, muss die Übermittlung aussetzen, wenn es der Ansicht ist, dass die Konzernrichtlinie Datenschutz nicht eingehalten werden kann, oder wenn es von der zuständigen Aufsichtsbehörde dazu aufgefordert wird. Das Unternehmen muss die Übermittlung beenden, wenn die Einhaltung der Binding Corporate Rules Privacy nicht innerhalb eines Monats nach der Aussetzung wiederhergestellt wird. In diesem Fall sind personenbezogene Daten, die vor der Beendigung übermittelt wurden, und etwaige Kopien davon nach Wahl des Unternehmens, das die personenbezogenen Daten übermittelt, an dieses zurückzugeben oder vollständig zu löschen.
- (4) Auf Grundlage der Vorgaben der Deutschen Telekom Gruppe 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.

§ 20 Pflichten des Empfängers im Falle des Zugangs von Behörden zu den Daten

- (1) Der Empfänger erklärt sich damit einverstanden, das übermittelnde Unternehmen unverzüglich zu benachrichtigen,

- a) wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß dieser Konzernrichtlinie Datenschutz übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder
 - b) wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß dieser Konzernrichtlinie Datenschutz übermittelt wurden; diese Benachrichtigung muss alle dem Empfänger verfügbaren Informationen enthalten.
- (2) Ist es dem Empfänger gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, das übermittelnde Unternehmen zu benachrichtigen, so erklärt sich der Empfänger einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Empfänger verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des übermittelnden Unternehmens nachweisen zu können.
 - (3) Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Empfänger bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.).
 - (4) Der Empfänger erklärt sich damit einverstanden, die Informationen gemäß den Absätzen 1 bis 3 während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.
 - (5) Die Absätze 1 bis 3 gelten unbeschadet der Pflicht des Empfängers, das übermittelnde Unternehmen unverzüglich zu informieren, wenn er diese Konzernrichtlinie Datenschutz nicht einhalten kann.
 - (6) Der Empfänger erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Empfänger mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Empfänger einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der weiteren Pflichten des Empfängers aus dieser Konzernrichtlinie Datenschutz.
 - (7) Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung.
 - (8) Der Datenimporteur erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

§ 21 Datenverarbeitung im Auftrag¹

- (1) Wird eine andere Stelle (Auftragsverarbeiter) im Auftrag eines Unternehmens (Verantwortlicher) nach dessen Weisung und für dessen Zwecke tätig, so ist neben den zu erbringenden Dienstleistungen im Vertrag auch auf die Verpflichtungen des Auftragsverarbeiters Bezug zu nehmen. In diesen Verpflichtungen werden die Anweisungen des Verantwortlichen 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.
- (2) Ohne die vorherige Zustimmung des Verantwortlichen darf der Auftragsverarbeiter die ihm zur Auftragserfüllung überlassenen personenbezogenen Daten nicht für eigene oder fremde Zwecke verarbeiten. Die Einbindung von Unterauftragnehmern durch den Auftragsverarbeiter zur Erfüllung der vertraglichen Verpflichtungen bedarf der vorherigen Information des Verantwortlichen. Der Verantwortliche hat ein Widerspruchsrecht gegen die Beauftragung von Unterauftragsverarbeitern. Bei der zulässigen Einbindung von Unterauftragsverarbeitern hat der Auftragsverarbeiter den Unterauftragsverarbeitern auf die Vereinbarungen, die zwischen dem Auftragsverarbeiter und dem Verantwortlichen getroffen wurden, entsprechend zu verpflichten.
- (3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, nachdem ihm ein Datenschutzverstoß oder konkrete Anhaltspunkte für einen Verstoß gegen Datenschutzbestimmungen, insbesondere auch dieser Konzernrichtlinie Datenschutz, bekannt werden.
- (4) Die Auftragsverarbeiter sind von den Unternehmen nach ihrer Fähigkeit, die oben genannten Anforderungen zu erfüllen, auszuwählen.

¹ Dieser § ist keine Regelung im Sinne des Arbeitspapiers 195 der Artikel 29 Arbeitsgruppe der Europäischen Kommission.

Abschnitt 4

Datenqualität und Datensicherheit

§ 22 Datenqualität

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

§ 23 Datensicherheit - Technische und organisatorische Maßnahmen – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

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, die regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert werden.

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 (Zugriffskontrolle), und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (z.B. durch Verschlüsselung);
- 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 Auftragsverarbeiters);
- 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);

Teil 3

Rechte des Betroffenen

§ 24 Auskunftsrecht

- (1) Jeder Betroffene kann gegenüber jedem Unternehmen, das seine Daten verarbeitet, jederzeit Auskunft verlangen über:
 - a) die zu seiner Person gespeicherten Daten, inklusive ihrer Herkunft und Empfänger;
 - b) den Zweck der Verarbeitung der Daten;
 - c) die Empfänger, an die seine Daten übermittelt werden bzw. wurden, insbesondere soweit es sich um eine Übermittlung in ein Drittland handelt;
 - d) die Regelungen dieser Konzernrichtlinie Datenschutz.
- (2) Die Auskunft ist dem Betroffenen in angemessener Frist in verständlicher Form zu erteilen. Sie erfolgt in der Regel schriftlich oder elektronisch. Der Betroffene ist spätestens innerhalb eines Monats über den Stand der Bearbeitung zu informieren. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und Anzahl der Anfragen erforderlich ist, wobei der Betroffene hierüber entsprechend zu informieren ist. Die Information über die Regelungen dieser Konzernrichtlinie Datenschutz kann durch Überlassen einer Textfassung der Konzernrichtlinie erfolgen.
- (3) Die Unternehmen können für die anlässlich einer Auskunftserteilung zur Verfügung gestellten weiteren Kopien der Daten nur dann eine Gebühr verlangen, wenn und soweit dies nach Maßgabe des jeweiligen Landesrechts zulässig ist.

§ 25 Widerspruchsrecht, Recht auf Löschung oder Einschränkung der Verarbeitung und Recht auf Berichtigung

- (1) Der Betroffene kann der Verarbeitung seiner Daten jederzeit widersprechen, wenn sie nicht zu gesetzlich zwingenden Zwecken verwendet werden.
- (2) Das Widerspruchsrecht gilt auch für den Fall, dass der Betroffene zuvor seine Einwilligung zur Verarbeitung seiner Daten gegeben hatte.
- (3) Berechtigten Ersuchen zur Löschung oder Einschränkung der Verarbeitung von Daten ist unverzüglich nachzukommen. Ein solches Ersuchen ist insbesondere dann berechtigt, wenn die rechtliche Grundlage für die Verarbeitung der Daten weggefallen ist. Gesetzliche Aufbewahrungsfristen sind zu beachten.
- (4) Der Betroffene kann vom Unternehmen jederzeit die Berichtigung der zu seiner Person gespeicherten Daten verlangen, sofern diese unvollständig und/oder unrichtig sind.
- (5) Bei Geschäftsmodellen, bei denen der Widerspruch oder die Löschung dazu führt, dass vertragliche Pflichten nicht erfüllt werden können, ist der Betroffene darüber zu informieren.

§ 26 Recht auf Klärung, Stellungnahme und Abhilfe

- (1) Macht ein Betroffener eine Verletzung seiner Rechte durch unzulässige Verarbeitung 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 Übermittlung von Daten an Unternehmen außerhalb des Europäischen Wirtschaftsraums hat das im Europäischen Wirtschaftsraums ansässige Unternehmen den Sachverhalt aufzuklären und den Beweis zu erbringen, dass der Empfänger 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.

- (2) Der Betroffene kann gegenüber der Konzernholding der Deutschen Telekom Gruppe jederzeit Beschwerde einreichen, wenn der Verdacht besteht, dass ein Unternehmen der Deutschen Telekom Gruppe seine personenbezogenen Daten nicht gemäß den Gesetzen oder den Bestimmungen dieser Konzernrichtlinie verarbeitet. Der begründeten Beschwerde wird innerhalb eines angemessenen Zeitraums abgeholfen und der Betroffene innerhalb eines Monats über den Stand der Bearbeitung entsprechend informiert. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und Anzahl der Anfragen erforderlich ist, wobei der Betroffene hierüber entsprechend zu informieren ist.
- (3) Sind von einer Beschwerde mehrere Unternehmen betroffen, koordiniert der Datenschutzbeauftragte des Unternehmens mit der größten Sachnähe die gesamte einschlägige Korrespondenz mit dem Betroffenen. Der Konzerndatenschutzbeauftragte hat ein jederzeitiges Eintritts- und Übernahmerecht.
- (4) Meldungen zu einem Datenschutzvorfall müssen in geeigneter Weise (z.B. über ein Funktionspostfach des Datenschutzbereiches oder Nennung eines direkten Ansprechpartners im Internet) erfolgen können.
- (5) Der Datenschutzbeauftragte des betroffenen Unternehmens hat den Konzerndatenschutzbeauftragten über einen Datenschutzvorfall anhand der dafür vorgesehenen Meldeprozesse unverzüglich zu informieren und eine Dokumentation des Datenschutzvorfalls, die den Aufsichtsbehörden auf Anfrage zur Verfügung gestellt werden kann, zu gewährleisten.
- (6) Betroffene können im Falle einer Verletzung ihrer Rechte oder im Schadensfall etwaige Ansprüche gemäß den Bestimmungen in Teil 5 dieser Konzernrichtlinie geltend machen.

§ 27 Frage- und Beschwerderecht

Jeder Betroffene hat das Recht, sich jederzeit mit Fragen und Beschwerden zur Anwendung dieser Konzernrichtlinie an den oder die Datenschutzbeauftragten der Unternehmen zu wenden, das oder die seine personenbezogenen Daten verarbeitet. 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.

§ 28 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.

§ 29 Textfassung der Konzernrichtlinie

Die aktuelle Version der Konzernrichtlinie Datenschutz und die Liste der Unternehmen, die die Konzernrichtlinie Datenschutz verbindlich eingeführt haben, werden auf www.telekom.com veröffentlicht.

Teil 4

Datenschutzorganisation

§ 30 Verantwortung für die Datenverarbeitung

Die Unternehmen sind verpflichtet, die Einhaltung der gesetzlichen Datenschutzbestimmungen und dieser Konzernrichtlinie Datenschutz sicherzustellen und dies jederzeit nachweisen zu können.

§ 31 Datenschutzbeauftragte

- (1) In den Unternehmen ist ein unabhängiger Datenschutzbeauftragter zu bestellen. Dieser hat die Aufgabe, die Beratung der verschiedenen Organisationseinheiten in diesem Unternehmen 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.
- (2) Vor der Bestellung oder der Abberufung eines Datenschutzbeauftragten ist der Konzerndatenschutzbeauftragte vom Unternehmen zu konsultieren.
- (3) Das Unternehmen stellt sicher, dass die Aufgaben und Pflichten des Datenschutzbeauftragten nicht zu einem Interessenkonflikt führen.
- (4) Das Unternehmen stellt sicher, dass der Datenschutzbeauftragte die erforderlichen Kompetenzen zur rechtlichen, technischen und organisatorischen Bewertung von datenschutzrelevanten Maßnahmen hat.
- (5) Der Datenschutzbeauftragte ist für die Ausübung seiner Aufgaben vom Unternehmen mit angemessenen finanziellen und personellen Mitteln auszustatten.
- (6) Dem Datenschutzbeauftragten des Unternehmens ist ein direktes Berichtsrecht an die Unternehmensleitung einzuräumen. Er ist organisatorisch an die Unternehmensleitung anzubinden.
- (7) Die Umsetzung der Vorgaben des Konzerndatenschutzbeauftragten und der Datenschutzstrategie der Deutschen Telekom Gruppe obliegt dem Datenschutzbeauftragten des jeweiligen Unternehmens.
- (8) 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.

§ 32 Konzerndatenschutzbeauftragter

- (1) Der Konzerndatenschutzbeauftragte koordiniert die Zusammenarbeit und Abstimmung zu allen wichtigen Fragen des Datenschutzes in der Deutschen Telekom Gruppe. Er informiert bei Bedarf den Vorstand der Konzernholding der Deutschen Telekom Gruppe zu den aktuellen Entwicklungen oder formuliert Empfehlungen.
- (2) Es obliegt dem Konzerndatenschutzbeauftragten die Datenschutzpolitik der Deutschen Telekom Gruppe zu entwickeln und fortzuschreiben. Die Datenschutzbeauftragten der Unternehmen werden dabei angemessen eingebunden. Sie entwickeln die Datenschutzpolitik für ihr Unternehmen im Einklang mit der Datenschutzpolitik der Gruppe. Ein gemeinsamer Austausch zwischen dem Konzerndatenschutzbeauftragten und den Datenschutzbeauftragten der Länder findet jährlich im Rahmen von Präsenzveranstaltungen statt.

§ 33 Informationspflicht bei Verstößen oder bei Änderungen der für ein Unternehmen geltenden Gesetze und Gepflogenheiten

Die Datenschutzbeauftragten sind vom betroffenen Unternehmen unverzüglich über Verstöße oder konkrete Anhaltspunkte für einen Verstoß gegen Datenschutzbestimmungen, insbesondere auch dieser Konzernrichtlinie Datenschutz, zu informieren. Bei Vorfällen mit möglicher Öffentlichkeitswirkung, mit Relevanz für mehr als ein Unternehmen oder mit einem möglichen Schadenseintritt von über 500.000 EUR informiert der Datenschutzbeauftragte unverzüglich auch den Konzerndatenschutzbeauftragten. Der Konzerndatenschutzbeauftragte ist stets zu informieren, wenn die zuständige Aufsichtsbehörde gegen das Unternehmen ein Bußgeld verhängt hat.

Die Datenschutzbeauftragten der Unternehmen informieren den Konzerndatenschutzbeauftragten ferner, wenn die für ein Unternehmen geltenden Gesetze oder Gepflogenheiten sich wesentlich nachteilig im Sinne dieser Konzernrichtlinie ändern.

Der Verantwortliche benachrichtigt betroffene Personen unverzüglich, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

§ 34 Überprüfungen des Datenschutzniveaus

- (1) 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 Datenschutzbeauftragten der Unternehmen oder Reports. Der jährliche Kontrollplan berücksichtigt die Risiken, die mit den Verarbeitungstätigkeiten verbunden sind, die unter diese Konzernrichtlinie Datenschutz fallen. Die Kontrollen des Konzerndatenschutzbeauftragten werden durch interne oder externe Auditoren durchgeführt. Darüber hinaus können regelmäßige Self-Assessment Verfahren in der Deutschen Telekom Gruppe durchgeführt und vom Konzerndatenschutzbeauftragten koordiniert werden.
- (2) Die Ergebnisse wesentlicher Kontrollen und die dazu vereinbarten Maßnahmen werden dem Vorstand der Holding der Deutschen Telekom Gruppe mitgeteilt. Die zuständige Datenaufsichtsbehörde kann auf Nachfrage eine Kopie des Kontrollergebnisses erhalten. Zudem kann die für das Unternehmen zuständige Aufsichtsbehörde auch eine Kontrollmaßnahme anstoßen. Diese Kontrollmaßnahmen werden von den Unternehmen bestmöglich unterstützt und die daraus abgeleiteten Maßnahmen werden umgesetzt.
- (3) Werden im Rahmen einer Kontrolle Schwachstellen festgestellt, sind diese durch entsprechende Maßnahmen durch das Unternehmen zu beheben. Der Konzerndatenschutzbeauftragte verfolgt die Umsetzung der Maßnahmen. Sollten diese ohne ausreichende Begründung nicht umgesetzt werden, bewertet der Konzerndatenschutzbeauftragte die Auswirkungen auf den Datenschutz und leitet die notwendigen Konsequenzen und gegebenenfalls eine Eskalation ein.
- (4) Die Datenschutzbeauftragten der Unternehmen oder andere mit einem Prüfungsauftrag ausgestattete Organisationseinheiten prüfen zusätzlich auf die Einhaltung der Belange des Datenschutzes auf Grundlage von eigenen, schriftlich zu dokumentierenden Auditierungsplanungen. Datenschutzbeauftragte sind nicht für die Prüfung der Einhaltung dieser Konzernrichtlinie Datenschutz zuständig, wenn diese Prüfung zu einem Interessenkonflikt führen kann.
- (5) Sofern keine gesetzlichen Beschränkungen bestehen, sind der Konzerndatenschutzbeauftragte bei allen Unternehmen und die Datenschutzbeauftragten, jeweils für ihr Unternehmen, befugt die ordnungsgemäße Verarbeitung von personenbezogenen Daten zu überprüfen. Dazu gewähren die Unternehmen umfassend Zutritt und Einsicht zu den Informationen, die der Konzerndatenschutzbeauftragte und die Datenschutzbeauftragten zur Aufklärung und Bewertung eines Sachverhalts für notwendig erachten. Der Konzerndatenschutzbeauftragte und die Datenschutzbeauftragten können in diesem Zusammenhang Weisungen erteilen.

- (6) Die Datenschutzbeauftragten der Unternehmen bedienen sich im Rahmen ihrer Prüfaufgabe nach Möglichkeit konzernweit gleichartiger Verfahren, z.B. in Form von gemeinsamen Datenschutzaudits. Diese Verfahren können vom Konzerndatenschutzbeauftragten zur Verfügung gestellt werden.

§ 35 Datenschutz-Folgenabschätzung

Die Unternehmen führen für die Verarbeitung personenbezogener Daten eine strukturierte und dokumentierte Datenschutz-Folgenabschätzung durch. Die Konzernholding stellt einen zentral verfügbaren Prozess namens Privacy and Security Assessment (PSA) zur Verfügung, der in seiner aktuellen Fassung einheitlich in allen Unternehmen implementiert werden muss. Abweichungen von der Nutzung des PSA-Prozesses können in Abstimmung und bei vorheriger Zustimmung des Konzerndatenschutzbeauftragten vorgenommen werden, wenn Unternehmen besonders klein oder ohne eine wesentliche eigene Datenverarbeitung sind.

§ 36 Mitarbeiterverpflichtung und Schulung

- (1) 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.
- (2) 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 Datenschutzbeauftragten des Unternehmens zu dokumentieren und an den Konzerndatenschutzbeauftragten jährlich zu berichten.
- (3) Der Konzerndatenschutzbeauftragte kann Materialien und Prozesse zur Verpflichtung und Schulung der Mitarbeiter der Deutschen Telekom Gruppe zentral zur Verfügung stellen.

§ 37 Zusammenarbeit mit Aufsichtsbehörden

- (1) 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.
- (2) Im Falle einer Änderung der für ein Unternehmen geltenden Gesetze, die auf die hier gegebenen Zusicherungen wesentliche nachteilige Auswirkungen haben können, setzt das Unternehmen die zuständige Aufsichtsbehörde über die Änderung in Kenntnis.
- (3) Alle Streitigkeiten im Zusammenhang mit der Überwachung der Einhaltung dieser Konzernrichtlinie Datenschutz durch die zuständigen Aufsichtsbehörden werden von den Gerichten des Mitgliedstaats der Aufsichtsbehörde gemäß dem Verfahrensrecht dieses Mitgliedstaats entschieden. Die Unternehmen verpflichten sich, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

§ 38 Zuständige Stellen für Kontakte und Anfragen

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

Der Konzerndatenschutzbeauftragte ist über

datenschutz@telekom.de

privacy@telekom.de

Friedrich-Ebert-Allee 140,

53113 Bonn

Teil 5

Haftung

§ 39 Anwendungsbereich der Haftungsregelungen

- (1) Die Konzernrichtlinie Datenschutz gilt für diesen Bereich ausschließlich für die Verarbeitung aller personenbezogenen Daten, auf die die Datenschutz-Grundverordnung 2016/679 Anwendung findet.
- (2) Innerhalb des Europäischen Wirtschaftsraums finden die gesetzlichen Haftungsregelungen der Länder Anwendung, in denen ein Unternehmen seinen Sitz hat. Bei Daten, die nicht unter § 39 Abs. 1 BCRP fallen, finden die gesetzlichen Haftungsregelungen des Landes Anwendung, in dem das Unternehmen seinen Sitz hat, das die Daten erhoben hat, oder wenn keine gesetzliche Regelung besteht, die Allgemeinen Geschäftsbedingungen des Unternehmens, das die Daten erhoben hat.
- (3) Die Zahlung von Strafschadensersatz, wonach ein Unternehmen einem Betroffenen Zahlungen leisten muss, die über den tatsächlich entstandenen Schaden hinausgehen, ist ausdrücklich ausgeschlossen.

§ 40 Haftungsschuldner

- (1) Jede betroffene Person, die durch eine Verletzung der in der Konzernrichtlinie genannten Pflichten durch ein Unternehmen der Deutschen Telekom Gruppe oder durch Empfänger von Daten, an die ein Unternehmen der Deutschen Telekom Gruppe die Daten übermittelt hat, ist berechtigt, von den beteiligten Unternehmen der Deutschen Telekom Gruppe Schadensersatz für den erlittenen Schaden zu verlangen.
- (2) Der Betroffene kann den Schadensersatzanspruch auch gegen die Holdinggesellschaft der Deutschen Telekom Gruppe geltend machen. Leistet die Holdinggesellschaft Schadensersatz, kann sie die Erstattung der Zahlungen von den Unternehmen verlangen, die den Schaden verursacht haben oder einen verursachenden Dritten beauftragt haben.
- (3) Der Betroffene hat den Schadensersatzanspruch zunächst gegen das Unternehmen geltend zu machen, das die Daten übermittelt hat. Fällt das übertragende Unternehmen als Schuldner faktisch oder rechtlich aus, kann der Betroffene seine Ansprüche gegenüber dem empfangenen Unternehmen geltend machen. Das empfangende Unternehmen kann sich seiner Haftung nicht entziehen, indem es sich auf die Verantwortung eines Auftragsverarbeiters für einen Verstoß beruft.
- (4) Der Betroffene hat jederzeit das Recht, sich mit einer Beschwerde an die zuständige Aufsichtsbehörde in dem Mitgliedstaat seines Aufenthaltsorts, seines Arbeitsplatzes oder Orts des mutmaßlichen Verstoßes oder die für die Holdinggesellschaft der Deutschen Telekom Gruppe zuständige Aufsichtsbehörde zu wenden.
- (5) Der Betroffene hat das Recht auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten des Europäischen Wirtschaftsraums, wenn er der Ansicht ist, dass die ihm aufgrund dieser Konzernrichtlinie Datenschutz zustehenden Rechte infolge einer nicht im Einklang mit dieser Konzernrichtlinie stehenden Verarbeitung seiner personenbezogenen Daten verletzt wurden.
- (6) Der Betroffene hat das Recht, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht zu beauftragen, in seinem Namen die vorgenannten Rechte geltend zu machen.

§ 41 Beweislast

Die Beweislast für die ordnungsgemäße Verarbeitung der Daten des Betroffenen tragen die haftenden Unternehmen.

§ 42 Drittbegünstigung für Betroffene

Soweit dem Betroffenen keine unmittelbaren Rechte zustehen, kann er als Drittbegünstigter die Rechte aus den Bestimmungen dieser Konzernrichtlinie gegen die Unternehmen geltend machen, wenn diese im Hinblick auf den Betroffenen ihre Vertragspflichten verletzen.

§ 43 Gerichtsstand

Der Gerichtsstand für die Geltendmachung von Ansprüchen kann nach Wahl des Betroffenen

- a) der für den Betroffenen geltende Gerichtsstand des gewöhnlichen Aufenthaltsortes oder
- b) entweder im Gerichtsstand des Sitzes der Niederlassung oder
- c) im Gerichtsstand der europäischen Zentrale oder des mit dem Datenschutz beauftragten, in der EU ansässigen Unternehmensteils sein.

§ 44 Außergerichtliche Schlichtung

- (1) Betroffene, die sich durch eine tatsächliche oder vermutete Verarbeitung von personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt fühlen, können sich an den Datenschutzbeauftragten des betroffenen Unternehmens mit der Bitte um Schlichtung wenden. Dieser hat die Berechtigung der Beschwerde zu überprüfen und den Betroffenen im Hinblick auf seine Rechte zu beraten. Dabei ist er verpflichtet, die Vertraulichkeit von weiteren, vom Beschwerdeführer mitgeteilten personenbezogenen Daten zu wahren, soweit dieser ihn nicht hiervon befreit. Auf Wunsch des Betroffenen kann der Versuch unternommen werden, unter Beteiligung des Betroffenen und des Datenschutzbeauftragten, eine Einigung über die Beschwerde zu erzielen. Eine solche Einigung kann auch eine Empfehlung über einen Ersatz eines durch Verletzung des Persönlichkeitsrechts erlittenen Schadens enthalten. Eine solche Empfehlung – sofern sie einvernehmlich zustande kommt – ist für die beteiligten Unternehmen verbindlich.
- (2) Das Recht sich mit der Beschwerde an die zuständigen Aufsichtsbehörden in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes zu wenden oder eine Klage zu erheben bleiben hiervon unberührt.

Teil 6

Schlussbestimmungen

§ 45 Überprüfung und Überarbeitung dieser Konzernrichtlinie

- (1) Der Konzerndatenschutzbeauftragte überprüft die Konzernrichtlinie Datenschutz in regelmäßigen Abständen, mindestens jedoch einmal jährlich, auf deren Vereinbarkeit mit dem geltenden regulatorischen Umfeld und passt diese bei Bedarf an.
- (2) Wesentliche Änderungen der Konzernrichtlinie, die sich zum Beispiel aus der notwendigen Anpassung an rechtliche Vorgaben ergeben, werden mit der Aufsichtsbehörde abgestimmt. Diese Änderungen gelten nach einer angemessenen Übergangsfrist unmittelbar für alle Unternehmen, die die Konzernrichtlinie Datenschutz gezeichnet haben.
- (3) Der Konzerndatenschutzbeauftragte informiert alle Unternehmen, die die Konzernrichtlinie Datenschutz verbindlich eingeführt haben, über die inhaltlichen Änderungen.
- (4) Die Datenschutzbeauftragten der Unternehmen sind verpflichtet zu überprüfen, ob Änderungen dieser Konzernrichtlinie Datenschutz Auswirkungen auf die Rechtskonformität in ihrem Land haben oder in Kollision mit den landesgesetzlichen Bestimmungen und Gepflogenheiten stehen. Sollte das Unternehmen die Änderungen aus zwingenden gesetzlichen Gründen nicht umsetzen können, ist der Konzerndatenschutzbeauftragte und zuständige Aufsichtsbehörde unverzüglich darüber zu informieren und gegebenenfalls die Konzernrichtlinie Datenschutz für dieses Unternehmen vorübergehend auszusetzen.
- (5) Die Unternehmen, die personenbezogene Daten in Drittländer übermitteln, überwachen laufend und gegebenenfalls in Zusammenarbeit mit den Empfängern die Entwicklungen in den betreffenden Drittländern, die sich auf das bestehende Transfer Impact Assessment und die Einhaltung dieser Konzernrichtlinie Datenschutz auswirken könnten.

§ 46 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 auf Anfrage. Die zuständige Aufsichtsbehörde erhält einmal jährlich eine aktuelle Liste der Unternehmen, die die Konzernrichtlinie verbindlich eingeführt haben.

§ 47 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.

§ 48 Öffentliche Bekanntmachung

Die Unternehmen machen die Informationen zu den Rechten der Betroffenen und die Drittbegünstigungsklausel an geeigneter Stelle der Öffentlichkeit zugänglich, etwa bei den Datenschutzhinweisen im Internet. Die Veröffentlichung erfolgt unverzüglich, nachdem die Konzernrichtlinie für das Unternehmen verbindlich geworden ist.

Teil 7

Definitionen und Begriffe

Anonymisierung

ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Auftragsverarbeiter

sind Unternehmen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten.

Automatisierte Einzelentscheidungen

sind Entscheidungen, die für den Betroffenen rechtliche Folgen nach sich ziehen oder ihn wesentlich beeinträchtigen und sich ausschließlich auf eine automatisierte Verarbeitung von Daten stützen, mit denen bestimmte persönliche Aspekte hinsichtlich des Betroffenen bewertet werden, wie seine berufliche Leistungsfähigkeit, Kreditwürdigkeit, Zuverlässigkeit, Verhalten etc.

Besondere Arten personenbezogener Daten

sind Daten aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit hervorgeht sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung einer Person.

Betroffener

ist jede identifizierte oder identifizierbare natürliche Person mit deren personenbezogenen oder personenbeziehenden Daten in der Deutsche Telekom Gruppe umgegangen wird.

Deutsche Telekom Gruppe

ist die Deutsche Telekom AG sowie alle Unternehmen, an denen die Deutsche Telekom AG mittelbar oder unmittelbar zu mehr als 50% beteiligt ist, oder die vollkonsolidiert sind.

Dritter

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.

Empfänger

ist jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, der personenbezogene Daten preisgegeben werden, und zwar unabhängig davon, ob es sich hierbei um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines einzelnen Untersuchungsauftrags möglicherweise Daten erhalten, gelten jedoch nicht als Empfänger.

Europäischer Wirtschaftsraum

besteht aus den Mitgliedstaaten der Europäischen Union und drei Ländern der Europäischen Freihandelszone (Island, Liechtenstein und Norwegen; ohne die Schweiz).

Konzernholding

Derzeit ist die Konzernholding die Deutsche Telekom AG mit Sitz in Deutschland, Friedrich-Ebert-Allee 140, 53113 Bonn.

Personenbezogene Daten

sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person (Betroffener); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Pseudonymisierung

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.

(Verantwortliche) Stelle

ist jede natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Unternehmen

ist eine Gesellschaft, die dieser Konzernrichtlinie Datenschutz unterliegt. Die Unternehmen sind in einer gesonderten Liste zur Einsicht vorgehalten, die ständig aktualisiert wird. Die Liste kann von jedermann jederzeit eingesehen werden.

Verarbeitung

ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter 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, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Weiterübermittlung

Ist die Übermittlung personenbezogener Daten aus einem Drittland in ein anderes Drittland

Liste der Unternehmen, die die Konzernrichtlinie Datenschutz verbindlich eingeführt haben