Datenschutz im Konzern

Leitlinie (Code of Conduct)

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

2010 / 04

Consulting
DETECON

We make ICT strategies work

Inhalt

Präambel

- (1) Der Schutz personenbezogener Daten von Kunden, Vertriebspartnern, Mitarbeitern und Aktionären ist aufgrund der zunehmenden Vernetzung der Informations- und Kommunikationssysteme ein weltweit maßgebliches Anliegen aller Unternehmen im Konzern Deutsche Telekom.
- (2) Wesentliches Ziel dieser Leitlinie ist es daher, im Konzern Deutsche Telekom ein weltweit einheitliches und hohes Datenschutzniveau zu schaffen. Insbesondere muss bei Länder übergreifenden Datenflüssen gewährleistet sein, dass personenbezogene Daten beim Empfänger entsprechend den datenschutzrechtlichen Grundsätzen verarbeitet werden, die für die übermittelnde Stelle gelten.
- (3) 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.
- (4) In vielen Bereichen wird die Deutsche Telekom Gruppe aus Sicht ihrer Kunden als eine Einheit wahrgenommen. Es ist deshalb das gemeinsame Anliegen der Unternehmen der Deutschen Telekom Gruppe, durch die Umsetzung dieser Leitlinie einen wichtigen Beitrag zum gemeinsamen unternehmerischen Erfolg zu leisten und den Anspruch der Deutschen Telekom Gruppe als Anbieter qualitativ hochwertiger Produkte und Dienstleistungen zu unterstützen.

1 Erster Teil / Geltungsbereich

§ 1 Rechtsnatur des Code of Conduct

Dieser Code of Conduct ist eine Richtlinie, die für die gesamte Deutsche Telekom Gruppe bindend ist und mit Verabschiedung und Veröffentlichung durch die jeweilige Unternehmensleitung in Kraft tritt. Sie gilt für den Umgang mit allen personenbezogenen Daten natürlicher Personen, insbesondere Daten von Kunden, Aktionären, Mitarbeitern und sonstigen Dritten sowie Vertrags- oder Geschäftspartnern.

§ 2 Anzuwendende Rechtsvorschriften

- (1) Die nachfolgenden Prinzipien sollen ein gleichmäßig hohes Datenschutzniveau in der gesamten Deutsche Telekom Gruppe gewährleisten. Sie ersetzen jedoch nicht die notwendige, ggf. gesetzliche Legitimation, die dem jeweiligen Umgang mit personenbezogenen Daten zu Grunde liegen muss. Für einzelne Unternehmen bestehende Verpflichtungen und Regelungen zur Verarbeitung und Nutzung personenbezogener Daten, die über die nachfolgenden Grundsätze hinausgehen bzw. zusätzliche Beschränkungen für die Verarbeitung und Nutzung personenbezogener Daten enthalten, bleiben von diesem Code of Conduct unberührt. Unabhängig davon, sind sich die Unternehmen dahingehend einig, dass die für die einzelnen Unternehmen geltenden Gesetze diese nicht an der Erfüllung ihrer Verpflichtungen aus diesem Code of Conduct hindern.
- (2) Für die in Europa erhobenen Daten richtet sich die Verarbeitung – auch bei einer Übermittlung ins Ausland – nach den gesetzlichen Regelungen des Staates, in dem die Daten erhoben wurden.
- (3) Die Erhebung von personenbezogenen Daten und deren Übermittlung an staatliche Stellen erfolgen – soweit nicht im Rahmen einer üblichen Kundenvertragsbeziehung - entsprechend den zwingenden gesetzlichen Regelungen eines Landes.
- (4) Dieser Code of Conduct unterliegt im übrigen dem Recht der Bundesrepublik Deutschland.

§ 3 Kündigung

Die Beendigung oder Kündigung des Code of Conduct - ungeachtet des Zeitpunkts, der Umstände und der Gründe dafür – befreit die Unternehmen nicht von den Verpflichtungen und/oder Regelungen dieses Code of Conduct betreffend die Verarbeitung bereits übermittelter Daten.

2 Zweiter Teil / Grundsätze

2.1 Artikel 1: Transparenz der Datenverarbeitung

§ 4 Informationspflicht

Die Betroffenen müssen über den Umgang mit ihren personenbezogenen Daten in geeigneter Art und Weise leicht zugänglich informiert werden, zum Beispiel durch Einstellung der Privacy Policy und dieses Code of Conduct in das Internet.

§ 5 Inhalt und Gestaltung der Information

- (1) Die Betroffenen sind über folgende Punkte ausreichend zu informieren:
  - a) die Identität des für die Verarbeitung Verantwortlichen sowie dessen Kontaktadresse.
  - b) den beabsichtigten Umfang und Zweck der Datenerhebung, -verarbeitung und/oder Nutzung. Aus der Information sollte hervorgehen, welche Daten warum und zu welchem Zweck wie lange gespeichert und/oder verarbeitet/genutzt werden.
  - c) bei Weitergabe personenbezogener Daten an Dritte, an wen und in welchem Umfang sowie zu welchem Zweck diese Weitergabe erfolgt.
  - d) über die Art und Weise der Datenverarbeitung und/oder Nutzung, insbesondere auch dann, wenn die Verarbeitung oder Nutzung im Ausland erfolgen soll.
  - e) über ihre gesetzlichen Rechte (siehe Artikel 7).
- (2) Unabhängig vom gewählten Medium sollten diese Informationen den Betroffenen auf eine eindeutige und leicht verständliche Weise gegeben werden.

§ 6 Verfügbarkeit von Informationen

Den Betroffenen müssen die Informationen bei der erstmaligen Erhebung der Daten sowie danach stets bei Bedarf zur Verfügung stehen.

§ 7 Einwilligung

- (1) Sofern die Erhebung, Verarbeitung oder Nutzung der Daten nicht für Zwecke der Vertragsanbahnung oder –erfüllung erforderlich sind oder keine gesetzliche Erlaubnis vorliegt, ist spätestens bei Beginn der Erhebung, Verarbeitung oder Nutzung der Daten die Einwilligung des Betroffenen einzuholen.
- (2) Ergänzend zu den Informationspflichten aus den oben genannten Punkten, ist bei der Einwilligung folgendes zu beachten:
  - a) Inhalt: Die Einwilligung muss ausdrücklich erfolgen, freiwillig sein und auf einer informierten Grundlage beruhen, welche dem Betroffenen insbesondere die Reichweite der Einwilligung, aber auch die Folgen einer Nichteinwilligung aufzeigt. Die Formulierung von Einwilligungserklärungen muss hinreichend bestimmt sein und den Betroffenen über sein jederzeitiges Widerrufsrecht informieren.
  - b) Formvorschriften: Die Einholung der Einwilligung muss in einer den Umständen angemessenen Form (in der Regel schriftlich oder elektronisch) erfolgen. 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.

2.2 Artikel 2: Zweckbindung

§ 8 Grundsatz

Personenbezogene Daten dürfen nur für diejenigen Zwecke verwendet werden, für die sie ursprünglich erhoben wurden.

§ 9 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.

2.3 Artikel 3: Besondere Datenverarbeitungsfälle

§ 10 Direktmarketing

- (1) Die Betroffenen werden darüber in Kenntnis gesetzt, dass sie jederzeit der Verwendung ihrer personenbezogenen Daten für Zwecke des Direktmarketings widersprechen können. Sie werden ferner über die Art, den Inhalt und den Zeitraum, innerhalb dessen ihre Daten für die Zwecke des Direktmarketings möglicherweise verwendet werden, unterrichtet.

  (2) Die Betroffenen werden über ihr Recht informiert, Widerspruch einzulegen, wann immer sie Werbemittel im Rahmen des Direktmarketing erhalten. Ferner erhalten die Betroffenen angemessene Möglichkeiten zur Ausübung ihres Widerspruchsrechts im Hinblick auf derartige Werbemittel, insbesondere erhalten sie Informationen über die Stelle, bei der der Widerspruch einzulegen ist.

  (3) Besondere gesetzliche Vorschriften gemäß § 2 Abs. 1 S. 2 dieses Code of Conduct, die die Nutzung personenbezogener Daten von der Einwilligung des Betroffenen abhängig machen, gelten vorrangig.

§ 11 Automatisierte Einzelentscheidungen

- (1) 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 Verarbeitung 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 unverzüglich über das Ergebnis der automatisierten Entscheidung zu informieren, und es ist ihm die Möglichkeit zur Stellungnahme innerhalb angemessener Frist zu geben. Seine Stellungnahme ist angemessen zu berücksichtigen, bevor eine endgültige Entscheidung getroffen wird.

§ 12 Besondere Arten personenbezogener Daten

(1) Der Umgang mit besonderen Arten von personenbezogenen Daten ist nur zulässig, wenn eine ausdrückliche gesetzliche Genehmigung oder die vorherige Einwilligung des Betroffenen vorliegt. Er kann auch erfolgen, wenn die Verarbeitung erforderlich ist, um den Rechten und Pflichten der verantwortlichen Stelle auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist.

(2) Vor Beginn einer solchen Erhebung, Verarbeitung oder Nutzung ist der Bereich Datenschutz des betreffenden Unternehmens ordnungsgemäß schriftlich zu Rate zu ziehen, sofern dies erforderlich ist. Insbesondere sollten Art, Umfang, Zweck, das Erfordernis und die Rechtsgrundlage der Verwendung der Daten berücksichtigt werden.

2.4 Artikel 4: Datenqualität, Datensparsamkeit und Datenvermeidung

§ 13 Datenqualität

- (1) Personenbezogene Daten müssen jederzeit korrekt sein und sind, falls erforderlich, auf dem jeweils aktuellen Stand zu halten (Datenqualität).
- (2) Unter Beachtung des Erhebungs-, Verarbeitungs- oder Nutzungszwecks der Daten sind angemessene Maßnahmen dafür zu treffen, dass unrichtige oder unvollständige Daten gelöscht oder gegebenenfalls berichtigt werden.

§ 14 Datensparsamkeit, Datenvermeidung, Anonymisierung und Pseudonymisierung

- (1) 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).
- (2) Wo möglich und wirtschaftlich zumutbar, sind Verfahren zur Löschung der Identifikationsmerkmale der Betroffenen (Anonymisierung) bzw. zur Ersetzung der Identifikationsmerkmale durch andere Kennzeichen (Pseudonymisierung) einzusetzen. Anonymisierung und Pseudonymisierung haben so zu erfolgen, dass die tatsächliche Identität des Betroffenen nicht oder nur mit unverhältnismäßigem Aufwand wieder festgestellt werden kann.

§ 15 Profilbildungen, statistische Auswertungen

- (1) Durch organisatorische und technische Maßnahmen, die dem aktuellen Stand angewandter Konzeptionen bzw. der angewandten Technik entsprechen, ist sicherzustellen, dass Profilbildungen (z.B. Bewegungsprofile, Benutzerprofile, Konsumprofile) ausgeschlossen sind, soweit sie nicht ausdrücklich gesetzlich erlaubt sind oder der Betroffene eingewilligt hat.
- (2) Rein statistische Auswertungen oder Untersuchungen auf der Basis anonymisierter oder pseudonymisierter Daten bleiben davon unberührt.

§ 16 Datenarchivierung

Bei der Erstellung von Datenarchivierungskonzepten muss den Grundsätzen der Datenverarbeitung, insbesondere der Datensparsamkeit und der Datenvermeidung Rechnung getragen werden. Ohne ausdrückliche Einwilligung des Betroffenen hat die Archivierung von personenbezogenen Daten zu unterbleiben, soweit sie nicht betrieblich notwendig oder gesetzlich erforderlich ist.

2.5 Artikel 5: Beschränkung der Weitergabe

§ 17 Weitergabe von Daten an Dritte

- (1) Die Weitergabe von personenbezogenen Daten an einen Dritten bedarf einer rechtlichen Grundlage. Diese kann sich auch aus der Erfüllung einer vertraglichen Verpflichtung gegenüber dem Betroffenen oder aus seiner Einwilligung ergeben.
- (2) Absatz 1 gilt nicht, soweit nationale Vorschriften, insbesondere aus Gründen der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit sowie der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten, bestehen, die die Weitergabe von personenbezogenen Daten zu diesen Zwecken ausdrücklich vorsehen.

§ 18 Verantwortlichkeit

- (1) Bei der Weitergabe von Daten an Dritte, die nicht öffentliche Stellen sind, stellt das Unternehmen, das die personenbezogenen Daten ursprünglich erhoben hat, sicher, dass diese rechtmäßig verarbeitet oder genutzt werden. Dementsprechend müssen bereits vor der Weitergabe von Daten mit dem Empfänger angemessene Datenschutz- und Datensicherheitsmaßnahmen erörtert und vereinbart werden. Soweit Vereinbarungen mit Stellen in Ländern ohne angemessenes Datenschutzniveau geschlossen werden, sind ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte zu gewährleisten.
- (2) Auf Grundlage der allgemein anerkannten Standards müssen angemessene technische und organisatorische Maßnahmen getroffen werden, um die Integrität und Sicherheit der Daten während ihrer Übermittlung an einen Dritten sicherzustellen.

§ 19 Datenverarbeitung im Auftrag

- (1) Wird ein Subunternehmer im Auftrag eines Unternehmens tätig, so ist neben den zu erbringenden Dienstleistungen im Vertrag auch auf die Verpflichtungen des Subunternehmers als Auftragsdatenverarbeiter Bezug zu nehmen. In diesen Verpflichtungen werden die Anweisungen des Unternehmens (der verantwortlichen Stelle) 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 geregelt. § 18 Abs. 1 S. 3 dieses Code of Conduct gilt entsprechend.
- (2) Ohne die vorherige Zustimmung der verantwortlichen Stelle darf der Auftragnehmer die personen-bezogenen Daten nicht für eigene oder fremde Zwecke verwenden. Im letzten Fall müssen die oben genannten Regelungen auch mit dem (den) Subunternehmer(n) vereinbart werden.
- (3) Die Subunternehmer sind nach ihrer Fähigkeit, die oben genannten Anforderungen zu erfüllen, auszuwählen.

2.6 Artikel 6: Datenschutz-Organisation und Datensicherheit

§ 20 Datenschutzbeauftragte

- (1) In den Unternehmen ist ein unabhängiger Datenschutzbeauftragter zu benennen, dessen Aufgabe es ist, die Beratung der verschiedenen Organisationseinheiten über die gesetzlichen und/oder konzerninternen Vorgaben bzw. die Grundsätze des Datenschutzes sicherzustellen.
- (2) Der Datenschutzbeauftragte ist bei der Entwicklung neuer Produkte und Dienste frühzeitig zu beteiligen, um sicherzustellen, dass sie mit den im vorliegenden Code of Conduct festgelegten Grundsätzen im Einklang sind.

§ 21 Überprüfungen des Datenschutzniveaus

Überprüfungen des Datenschutzniveaus (z.B. durch Datenschutzaudits) sollten in regelmäßigen Abständen durchgeführt werden, um die Wirksamkeit und den Erfolg der eingeführten technischen und organisatorischen Maßnahmen zum Schutz der Daten zu überprüfen. Datenschutzaudits können intern durch den Datenschutzbeauftragten oder andere mit Prüfungsauftrag ausgestattete Organisationseinheiten, oder – in Abstimmung mit dem Datenschutzbeauftragten - durch einen unabhängigen, externen Dritten durchgeführt werden. Grundlage für die Feststellung des Datenschutzniveaus sind die für die jeweilige Organisationseinheit geltenden gesetzlichen und unternehmenspolitischen Vorgaben sowie die Anforderungen aus dieser Leitlinie.

§ 22 Technische, organisatorische und mitarbeiterbezogene Maßnahmen

Angemessene Geheimhaltungsverpflichtungen sind mit den Mitarbeitern bei der Aufnahme der Tätigkeit im Unternehmen schriftlich zu vereinbaren. Darüber hinaus müssen für die Unternehmensprozesse und IT-Systeme beim Umgang mit personenbezogenen Daten angemessene technische und organisatorische Maßnahmen ergriffen 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, 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)

2.7 Artikel 7: Rechte von Betroffenen

§ 23 Frage- und Beschwerderecht

Jeder Betroffene hat das Recht, sich jederzeit mit Fragen und Beschwerden bezüglich der Anwendung dieses Code of Conduct an den Datenschutzbereich des jeweils zuständigen Unternehmens zu wenden. Soweit nachfolgend nicht anders bestimmt, sind zuständig im Sinne dieser Regelungen alle Unternehmen, mit denen der Betroffene ein Vertragsverhältnis hat oder bei denen seine personenbezogenen Daten verarbeitet werden. Das Unternehmen, an das sich der Betroffene gewandt hat, sorgt für die Umsetzung der Rechte des Betroffenen bei den anderen zuständigen Unternehmen.

§ 24 Auskunftsrecht

- (1) Jeder Betroffene kann gegenüber dem zuständigen Unternehmen jederzeit Auskunft verlangen über:
  - a) die zu seiner Person gespeicherten Daten, inkl. ihrer Herkunft und Empfänger;
  - b) den Zweck der Verarbeitung oder Nutzung;
  - 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 dieses Code of Conduct
  - (2) Die Auskunft ist dem Betroffenen in angemessener Frist in verständlicher Form zu erteilen. Sie erfolgt in der Regel schriftlich oder elektronisch.
  - (3) Die Unternehmen können für die Auskunftserteilung eine Gebühr verlangen, wenn und soweit dies nach Maßgabe des jeweiligen Landesrechts zulässig ist.

§ 25 Widerspruchsrecht/Recht auf Löschung/Sperrung

- (1) Der Betroffene kann gegenüber dem zuständigen Unternehmen der Verwendung seiner Daten widersprechen, wenn ihm ein Widerspruchsrecht zusteht.
- (2) Das Widerspruchsrecht gilt auch für den Fall, dass der Betroffene zuvor seine Einwilligung zur Verwendung seiner Daten gegeben hatte.
- (3) Berechtigten Ersuchen zur Löschung/Sperrung von Daten ist umgehend 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.

§ 26 Recht auf Berichtigung

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

§ 27 Recht auf Klärung und Stellungnahme

- (1) Macht ein Betroffener eine Verletzung seiner Rechte durch unzulässige Datenverarbeitung, insb. in Form eines Verstoßes gegen diesen Code of Conduct geltend, so haben die zuständigen Unternehmen den Sachverhalt ohne schuldhaftes Zögern aufzuklären. Sie arbeiten dabei eng zusammen und gewähren sich gegenseitig Zugang zu allen für die Sachverhaltsfeststellung erforderlichen Informationen.
- (2) Der zuständige Datenschutzbereich des Unternehmens mit der größten Sachnähe hat die gesamte einschlägige Korrespondenz mit dem Betroffenen zu koordinieren.

§ 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.

2.8 Artikel 8: Prozessmanagement / Zuständigkeiten im Datenschutz

§ 29 Verantwortung für die Datenverarbeitung

- (1) Die Unternehmen sind in ihrer Eigenschaft als verantwortliche Stelle insbesondere gegenüber den Betroffenen verpflichtet, die Einhaltung der Datenschutzbestimmungen und dieses Code of Conduct sicherzustellen.
- (2) Der Datenschutzbeauftragte des jeweiligen Unternehmens ist unverzüglich über Verstöße (auch schon bei Verdacht auf Verstoß) gegen Datenschutzbestimmungen und diesen Code of Conduct zu informieren. Bei Vorfällen mit Relevanz für mehr als ein Unternehmen ist auch der Bereich Konzerndatenschutz zu informieren. Die Datenschutzbeauftragten der Unternehmen informieren den Bereich Konzerndatenschutz ferner, wenn die für ein Unternehmen geltenden Gesetze sich wesentlich nachteilig ändern.
- (3) Die Datenschutzbereiche der einzelnen Unternehmen haben ihre Aktivitäten im Rahmen der Datenschutzpolitik untereinander abzustimmen. Dementsprechend sollen sie sich gegenseitig Unterstützung gewähren und Synergien nutzen.

§ 30 Koordinierung durch den Konzerndatenschutzbeauftragten

- (1) Der Konzerndatenschutzbeauftragte koordiniert die Zusammenarbeit und Abstimmung zu allen wichtigen Fragen des Datenschutzes. Als Abstimmungsgremium dient der Datenschutzkoordinierungskreis der Deutsche Telekom Gruppe.
- (2) Es obliegt dem Konzerndatenschutzbeauftragten, die Datenschutzpolitik des Konzerns zu entwickeln und fortzuschreiben. Auch diesbezüglich stimmen sich die Datenschutzbereiche der Unternehmen untereinander ab.

§ 31 Überwachungs- und Beratungspflicht

- (1) Die Überwachung der Einhaltung der nationalen und internationalen Datenschutzvorschriften und dieses Code of Conduct obliegt den Datenschutzbeauftragten der jeweiligen Unternehmen. Diesbezüglich sind alle Bereiche der jeweiligen Unternehmen verpflichtet, den zuständigen Datenschutzbeauftragten über entsprechende Entwicklungen und zukünftige Pläne in Kenntnis zu setzen.
- (2) Sofern keine gesetzlichen Beschränkungen bestehen, sind die zuständigen Datenschutzbeauftragten befugt, vor Ort alle Verarbeitungsverfahren, bei denen personenbezogene Daten zum Einsatz kommen, zu überprüfen.
- (3) Die Datenschutzbereiche der Unternehmen bedienen sich ggf. im Rahmen ihrer Prüfaufgabe konzernweit gleichartiger Verfahren, z.B. in Form von gemeinsamen Datenschutzaudits.

§ 32 Mitarbeiterschulung und –verpflichtung

- (1) Die Mitarbeiter der Unternehmen sind bezüglich der Datenschutzvorschriften und der Anwendung dieses Code of Conduct ausreichend zu schulen.
- (2) Die Unternehmen erstellen unter Beteiligung der zuständigen Datenschutzbereiche entsprechende Schulungsunterlagen.

§ 33 Zusammenarbeit mit Aufsichtsbehörden

(1) Die Unternehmen erklären sich damit einverstanden, auf Anfragen der für sie oder gegebenenfalls für das datenexportierende Unternehmen zuständigen Aufsichtsbehörde innerhalb eines angemessenen Zeitraums sowie in einem zumutbaren Umfang zu antworten und deren Empfehlung zu befolgen.

(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.

2.9 Artikel 9: Begriffe und Definitionen

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.

Betroffener
Jede natürliche Person mit deren personenbezogenen oder personenbeziehbaren Daten in der Deutsche Telekom Gruppe umgegangen wird.

Verantwortliche Stelle
ist das Unternehmen, das über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Konzern Deutsche Telekom/Deutsche Telekom Gruppe
Die Deutsche Telekom AG sowie alle Unternehmen, an denen die Deutsche Telekom AG mittelbar oder unmittelbar zu mehr als 50% beteiligt ist, oder bei denen sie die wirtschaftliche Führung hat.

Verarbeiter von Daten
ist eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet (Datenverarbeitung im Auftrag).

Unternehmen
ist eine Gesellschaft, die sich damit einverstanden erklärt hat, sich an diesen Code of Conduct gebunden zu halten und im Anhang A aufgeführt ist.

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.

Umgang mit personenbezogenen Daten
ist jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie die Erhebung, Aufzeichnung, Organisation, Speicherung, Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination, Verknüpfung, Sperrung, Löschung oder Vernichtung; dies beinhaltet auch die Verarbeitung von personenbezogenen Daten in strukturierten, manuell erstellten Dateien.

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.

Besondere Arten personenbezogener Daten
sind Daten über die rassische oder ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Dritter
ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.