Datenschutzbericht 2008.

Über diesen Bericht.

Im vorliegenden Datenschutzbericht sind die wesentlichen Ereignisse und die Schwerpunktaktivitäten des Jahres 2008 aus Sicht des Konzerndatenschutzes dargestellt. Dieser Bericht ist der erste seiner Art, den die Deutsche Telekom veröffentlicht.

Bei der Aufarbeitung der Datenschutzvorfälle im Jahr 2008 hat sich die Deutsche Telekom verpflichtet, jährlich einen Bericht zum Stand des Datenschutzes zu veröffentlichen. Der Jahresdatenschutzbericht dient der Erfüllung der Berichtspflicht des Datenschutzbeauftragten gegenüber dem Gesamtvorstand der Deutschen Telekom AG und ihrem Aufsichtsrat. Er dokumentiert, wie der Konzern datenschutzrechtliche Anforderungen im täglichen Geschäft umgesetzt hat. Der Vorstand der Deutschen Telekom und der Datenschutzbeauftragte wollen damit der Öffentlichkeit signalisieren, dass die Deutsche Telekom beim Datenschutz auf Transparenz setzt.

Aufgrund des Redaktionsschlusses am 25. März 2009 sind einige Verfahren zu Datenschutzvorfällen aus dem Jahr 2008 noch im Status der „laufenden Ermittlungen". Daher kann der Konzern zu den Vorfällen hier nicht umfangreicher informieren, als dies bisher schon geschehen ist.

Zur Struktur des Berichts: Das erste Kapitel enthält einen Überblick über die wichtigsten datenschutzrelevanten Ereignisse im Jahr 2008. Im Anschluss werden die operativen Schwerpunkte des Konzerndatenschutzes aus dem vergangenen Jahr dargestellt. Nach Fazit und Ausblick findet sich im Anhang eine Darstellung der Organisation des Konzerndatenschutzes sowie der Rahmenbedingungen des betrieblichen Handelns. Abschließend ist die Leitlinie des Datenschutzes der Deutschen Telekom, der „Privacy Code of Conduct", aufgeführt.

Inhalt.

Geleitwort des Vorstands.

Dr. Manfred Balz
Vorstand Datenschutz,
Recht und Compliance

Liebe Leserinnen und Leser,

am 15. Dezember 2008 hat sich das „Volkszählungsurteil“ des Bundesverfassungsgerichts zum 25. Mal gejährt. In diesem Urteil wurde erstmalig das Recht auf informationelle Selbstbestimmung als Ableitung des allgemeinen Persönlichkeitsrechts und der Menschenwürde anerkannt. Als das Gericht das Urteil im Jahr 1983 verkündete, war das Leben der Bürgerinnen und Bürger weniger digitalisiert, als es jetzt im Zeitalter des Web 2.0 der Fall ist. Viele Nutzer geben heute in privaten Foren oft mehr Informationen preis, als damals vom Staat erhoben werden sollten. Zudem hinterlassen Menschen heute aufgrund der Nutzung moderner Kommunikationsmittel und der digitalen Speicherung von Geschäftsprozessen präzisere Spuren, als es damals vorstellbar war. Kundendaten sind eine begehrte Ware geworden, die zu kriminellen Handlungen verleitet, wie es die Datendiebstähle bei der Deutschen Telekom 2008 gezeigt haben. Aber auch die Anhäufung von Daten, die Möglichkeit diese zu analysieren und Informationen über Personen zu gewinnen, weckt Begehrlichkeiten.

Bei der Deutschen Telekom wurden in den Jahren 2005 und 2006 Verbindungsdaten unter anderem von Aufsichtsräten, Betriebsräten, Gewerkschaftsvertretern und Journalisten illegal ausgewertet. Diese Tat zeigt, wie schutzbedürftig die informationelle Selbstbestimmung ist – nicht nur gegenüber staatlichen Übergriffen, sondern auch gegenüber Missbrauch in Unternehmen.

Die Deutsche Telekom misst seit 2008 dem Datenschutz eine grundlegend neue Bedeutung bei. Das zeigt sich auch an dem neuen Vorstandsressort Datenschutz, Recht und Compliance. In einem Unternehmen wie der Deutschen Telekom, das täglich mit großen Mengen personenbezogener Daten umgeht, ist der Schutz dieser Daten eine eminent wichtige Aufgabe für alle – vom Mitarbeiter mit direktem Kundenkontakt bis zum Top-Management.

Datenschutz wandelt sich nicht nur bei der Deutschen Telekom, er stellt unsere ganze Gesellschaft im Zeitalter von Internet und Digitalisierung ständig vor neue Aufgaben. In Deutschland wird 2009 das Bundesdatenschutzgesetz novelliert. Wir begrüßen dieses Vorhaben. Zudem haben Vorfälle im Jahr 2009 das Thema Arbeitnehmerdatenschutz in den Fokus gerückt. Hier geht es um transparente Regelungen für den Einsatz von betrieblichen Datensammlungen und Analysemethoden sowie zur privaten Nutzung von Telekommunikationseinrichtungen.

Der sorgsame Umgang mit personenbezogenen Daten und das darauf aufbauende Vertrauen der Kunden sind für unser Geschäft unentbehrlich. Nach den Vorfällen, die im vergangenen Jahr die öffentliche Diskussion bestimmt haben, setzt der Konzern alles daran, verlorengegangenes Vertrauen zurückzugewinnen. Die Veröffentlichung dieses Berichts soll dazu beitragen.

Ihr

Dr. Manfred Balz
Vorstand Datenschutz, Recht und Compliance

Einleitung des Datenschutzbeauftragten: Vertrauensräume schaffen!

Das Jahr 2008 stellte für den Datenschutz bei der Deutschen Telekom nicht nur eine außergewöhnliche Belastungsprobe dar, sondern es markierte auch einen wichtigen Wendepunkt. Kaum ein Unternehmen in Deutschland hat bisher so anhaltend mit Datenschutzthemen in der Öffentlichkeit gestanden wie wir. Das Jahr 2008 hat deshalb wie kein anderes Jahr in der Geschichte des Konzerns dazu geführt, dass Datenschutz im Unternehmen umfassender verstanden wird.

Es geht nicht mehr nur um den optimalen Einsatz von technischen Systemen und die Konzeption und Umsetzung von datenschutzkonformen Arbeitsabläufen und Prozessen. Im Konzern Deutsche Telekom sind an allen relevanten Stellen Maßnahmen angelaufen, die den Datenschutz nicht nur operativ verbessern, sondern im Unternehmen eine Kultur etablieren, die den Datenschutz nachhaltig stärkt. Ein hoher Standard bei technischen Sicherungssystemen sowie rechtskonforme Prozesse und Abläufe sind die Basis für einen funktionierenden Datenschutz. Darüber hinaus muss aber im Management des Konzerns der Schutz der Daten als Teil des unternehmerischen Handels fest verankert sein und in der täglichen Arbeit von allen Mitarbeiterinnen und Mitarbeitern gelebt werden. Auch die Einrichtung des neuen Vorstandsressorts Datenschutz, Recht und Compliance zeigt die Bedeutung, die der Konzern dieser Aufgabe jetzt einräumt.

Der Schutz von Daten ist eine immer neue Herausforderung angesichts technischer Neuerungen und Entwicklungen und operativer Anforderungen. Im Interesse eines kundenorientierten Services müssen etwa Kundendaten an vielen dezentralen Kundenkontaktstellen und zu jeder Zeit verfügbar sein. Das ist eine von vielen Herausforderungen für den Datenschutz, die mit der steigenden Komplexität von Unternehmensstrukturen einhergehen. Neue Geschäftsmodelle, die zum Beispiel umfassende Dienste aus dem Internet heraus anbieten, führen zwangsläufig dazu, dass künftig immer größere Mengen persönlicher Informationen über Einzelpersonen oder Personengruppen an zentralen Speicherplätzen verfügbar sind. Diese Herausforderungen müssen bereits in der Konzeptionsphase von Produkten bedacht und durch den Datenschutz begleitet werden. Beim Blick auf den Nutzen für die Kunden darf der Blick auf ihre Rechte nicht verloren gehen. Das Leitbild der Datenschutzorganisation im Konzern richtet sich an dem Grundsatz aus:

„Vertrauensräume schaffen!“

Der Deutschen Telekom ist von verschiedenen Seiten ein guter Standard beim Datenschutz und gesetzeskonformes Vorgehen bescheinigt worden. Das Jahr 2008 hat aber gezeigt, dass ein Unternehmen wie die Deutsche Telekom nicht nur technische und prozessuale Standards erfüllen muss. Sämtliche Dienstleistungen und Produkte im Kerngeschäft der Deutschen Telekom basieren auf der Verarbeitung von personenbezogenen Daten unserer Kunden. Anders als bei anderen Industriezweigen und Branchen ist die Verarbeitung und die Übermittlung von Daten für die Deutsche Telekom entscheidender Bestandteil des operativen Geschäfts. Die Fähigkeit, diese Daten zu schützen, ist für die Deutsche Telekom damit existenziell.

Ihr

Dr. Claus Dieter Ulmer
Konzerndatenschutzbeauftragter Deutsche Telekom AG

„Ein hoher Standard bei technischen Sicherungssystemen sowie rechtskonforme Prozesse und Abläufe sind die Basis für einen funktionierenden Datenschutz. Darüber hinaus muss aber im Management des Konzerns der Schutz der Daten als Teil des unternehmerischen Handels fest verankert sein und in der täglichen Arbeit von allen Mitarbeiterinnen und Mitarbeitern gelebt werden."

Dr. Claus Dieter Ulmer
Konzerndatenschutzbeauftragter

Datenschutzrelevante Ereignisse 2008.

Datenschutzvorfälle 2008.

Die Deutsche Telekom sah sich 2008 mit Vorfällen konfrontiert, die weitreichende Bedeutung im Hinblick auf das Vertrauen der Kunden und damit die Wahrnehmung der Deutschen Telekom in der Öffentlichkeit und bei ihren Kunden hatten. Die Vorfälle waren teils strafrechtlicher Natur und betrafen den sehr sensiblen und vom Fernmeldegeheimnis geschützten Bereich der persönlichen Kommunikation. Teilweise wurde in 2008 auch aufgedeckt, dass es in vergangenen Jahren schwere Verstöße gegen den Datenschutz gegeben hat (Datenklau) oder es nicht autorisierte Zugriffe auf Datensysteme des Unternehmens gab. Die Vorfälle lassen sich grob in drei Kategorien untergliedern:

- Datenmissbrauch im Zusammenhang mit der Bespitzelung des Aufsichtsrats und von Medienvertretern,
- Diebstahl von Daten aus Datenbanken des Konzerns durch Mitarbeiter oder externe Dienstleister und
- nicht autorisierter Zugriff auf Datenbestände der Deutschen Telekom.

Dieser Bericht greift die wichtigsten Vorfälle auf. Eine vollständige und aktuelle Übersicht der Datenschutzvorfälle, die Gegenstand von staatsanwaltschaftlichen Ermittlungen sind, steht im Statusreport Datenschutz, der im Internet unter www.telekom.com/datenschutz abrufbar ist.

1. Datenmissbrauch im Zusammenhang mit der Bespitzelung des Aufsichtsrats und von Medienvertretern.
Nach derzeitigen Erkenntnissen ist es 2005 und 2006 zu Fällen von missbräuchlicher Nutzung von Verbindungsdaten gekommen. Der Vorstand der Deutschen Telekom hat am 14. Mai 2008 Strafanzeige bei der Staatsanwaltschaft Bonn gestellt, nachdem Ende April dem Unternehmen Hinweise auf deutlich umfangreichere Verletzungen des Datenschutzes vorlagen und nicht mehr von einem Einzelfall ausgegangen werden konnte. Die Ermittlungen der Staatsanwaltschaft Bonn und das vom Unternehmen übergebene Material haben gezeigt, dass Mitarbeiter des Konzerns die Verbindungsdaten von Aufsichtsratmitgliedern, Betriebsräten, Vorständen, Gewerkschaftern und Journalisten aus den Datenbanken ausgelesen und zur Auswertung an einen externen Dienstleister geliefert haben. Wer dieses Vorgehen beauftragt hat und wie der Tathergang im Detail erfolgte, ist Gegenstand der staatsanwaltschaftlichen Ermittlungen. Ende 2008 hat die Staatsanwaltschaft Bonn einen Verdächtigen in Untersuchungshaft genommen. Die Ermittlungen zu diesem Vorfall dauerten bei Redaktionsschluss dieses Berichts noch an.

2. Diebstahl von Daten aus Datenbanken des Konzerns durch Mitarbeiter oder Dienstleister.
Im März 2007 registrierte T-Home im Rahmen routinemäßiger Kontrollen eine auffällig hohe Auslastung bei einem kundendatenverarbeitenden System. Die Massenabrufe stellten sich bei weiteren Überprüfungen als illegale Zugriffe heraus. Mit unberechtigt erlangten Zugangskennungen erfolgte vermutlich im Zeitraum von Ende 2006 bis März 2007 ein Zugriff auf etwa eine halbe Million Kundendatensätze von T-Home. Die möglicherweise betroffenen Kundendaten enthielten Anschriften und Festnetz-Telefonnummern sowie teilweise auch E-Mail-Adressen. Die Deutsche Telekom hat Strafanzeige bei der Staatsanwaltschaft Berlin erstattet, die Ermittlungen dauerten bei Redaktionsschluss dieses Berichts noch an. Die identifizierten Zugangskennungen wurden umgehend gesperrt. Die Vergabe der Zugangskennungen hat die Deutsche Telekom grundlegend überarbeitet und strenger gefasst.

Ende April 2006 erhielt die Deutsche Telekom einen Hinweis, dass 17 Mio. Kundendaten von T-Mobile Deutschland zum Verkauf angeboten werden. Es handelte sich um Kundendaten von T-Mobile Deutschland mit Namen, Anschrift, Mobilfunknummern und teilweise Geburtsdatum sowie in geringem Umfang auch E-Mail-Adressen, die vor April 2006 gestohlen worden waren. Bankverbindungsdaten waren in den Datensätzen nicht enthalten. Mitte Mai 2006 erstattete die Deutsche Telekom Strafanzeige bei der Staatsanwaltschaft Köln gegen den Anbieter der Kundendaten. Im Verlauf der behördlichen Ermittlungen wurden Datenträger mit 17 Mio. Kundendaten sichergestellt. Der Fall wurde im Oktober 2008 vom Magazin „Der Spiegel“ aufgegriffen und publik gemacht. Inzwischen ermittelt die Staatsanwaltschaft Bonn. Die Ermittlungen dauerten bei Redaktionsschluss dieses Berichts noch an.

T-Mobile Deutschland hat die Kunden Ende 2008 über eine Rechnungsbeilage darüber informiert, dass sie ihre mögliche Betroffenheit vom Konzerndatenschutz prüfen lassen können. Diese Information hatten auch die Call-Center für Kundengespräche. Die der Deutschen Telekom überlassenen Datensätze werden gesondert und speziell gesichert gespeichert. Ein Zugriff darauf findet nur bei konkreten Anfragen und nach dem Vier-Augen-Prinzip statt.

Auf eine direkte Information an die in den Datensätzen enthaltenen Adressen hat die Deutsche Telekom wegen des Alters der Datensätze verzichtet. Es war nach mehr als zweieinhalb Jahren nicht mehr sichergestellt, dass die Daten noch aktuell sind und die Information die Betroffenen erreicht.

Im Sommer 2008 wurden einem Vertriebspartner der Deutschen Telekom 70 000 Kundendaten zum Kauf angeboten. Dieser informierte daraufhin die Deutsche Telekom. Ein Testkauf von einigen wenigen Proben bestätigte den Verdacht, dass es sich um Daten von T-Home handelt. Die entwendeten Kundendaten von T-Home enthalten Anschrift, Telefonnummer und Vertragsdaten. Informationen über Bankverbindungen sind in den Datensätzen nicht enthalten. Derzeit liegen keine weiteren Informationen vor, die es ermöglichen, potentiell betroffene Kunden zu benachrichtigen. Die Deutsche Telekom erstattete im Juli 2008 Strafanzeige bei der Staatsanwaltschaft München. Die Ermittlungen der Staatsanwaltschaft dauerten bei Redaktionsschluss dieses Berichts noch an.

Im November 2008 erhielt ein Vertriebspartner per Mail ein Angebot zum Erwerb von vorgeblich 80 000 DSL-Kundendatensätzen der Deutschen Telekom, deren Verträge zur Verlängerung anstünden. Der Vertriebspartner informierte daraufhin umgehend die Deutsche Telekom. Nach Rücksprache mit der Deutschen Telekom forderte der Vertriebspartner vom unbekannten Anbieter Testdatensätze an. Eine Lieferung erfolgte nicht. Die Deutsche Telekom erstattete am 28. November Strafanzeige gegen unbekannt bei der Staatsanwaltschaft Bonn. Die Ermittlungen der Strafverfolgungsbehörde dauerten bei Redaktionsschluss dieses Berichts noch an.

3. Nicht autorisierter Zugriff auf Datenbestände der Deutschen Telekom.
Im September 2007 erhielt die Deutsche Telekom Hinweise darauf, dass eine Zeit- und Leiharbeitskraft eines Call-Centers in Bremerhaven Zugangskennungen zu einer Datenplattform ausgespäht hatte. Dem Hinweisgeber zufolge hatte die Zeit- und Leiharbeitskraft diese Kennungen im Sommer 2007 missbräuchlich in einem eigenen privaten „Hinterhof-Call-Center“ eingesetzt, um Kunden zu werben. Bei den Kundendatensätzen handelt es sich um Telefonnummern und Adressen von Festnetz-Kunden. Über den Gesamtumfang der Daten liegen der Deutschen Telekom derzeit keine Erkenntnisse vor. Von einem Journalisten, der den Vorgang recherchierte und hierüber berichtete, erhielt das Unternehmen rund 50 Kundendatensätze. Diese Daten enthielten teilweise auch Kontonummern. Die betroffenen Kunden wurden umgehend informiert. Die im Rahmen der internen Untersuchungen festgestellten Mängel im Umgang mit Zugangskennungen wurden unverzüglich beseitigt. Bereits vor Kenntniserlangung des Missbrauchs waren im August 2007 aus anderem Anlass technische Sicherheitslücken geschlossen worden. Im konkreten Fall erstattete die Deutsche Telekom im August 2008 Strafanzeige bei der Staatsanwaltschaft Bremen. Die Ermittlungen der Staatsanwaltschaft Bremen dauerten bei Redaktionsschluss noch an.

Im Rahmen der Regelauswertung von Datenbankzugriffen auf eine Kundendatenbank wurden über Missbrauchserkennungssysteme bei drei Partner-Shops auffällig hohe Abrufzahlen pro Stunde festgestellt, die nicht im Verhältnis zur Kundenfrequenz standen. Alle drei Shops wurden vom selben Partner betrieben. Die hohe Zahl von Kundenbeschwerden über zwar gebuchte, von den Kunden aber nicht erteilte Aufträge, sowie die durchgeführten Einzelanalysen bestätigten den Verdacht auf Provisionsbetrug. Dem Betreiber der drei Shops wurde umgehend der Vertrag gekündigt, zwei der Shops wurden von neuen Partnern übernommen. Die Deutsche Telekom hat Schadensersatz gegen den Betreiber geltend gemacht und am 12. Dezember 2008 bei der zuständigen Staatsanwaltschaft Strafanzeige gegen ihn erstattet.

Aufarbeitung der Vorfälle.

Die Wahrnehmung der Bedeutung des Datenschutzes hat wegen dieser Vorfälle – aber auch anderer Vorfälle in anderen Unternehmen in Deutschland – sowohl in der Gesellschaft, als auch im Konzern sehr stark zugenommen. Die Deutsche Telekom unternimmt intensive Anstrengungen, das allgemeine Datenschutz- und Datensicherheitsniveau weiter zu verbessern, sodass ein höchstmöglicher Schutz personenbezogener Daten sowohl im Rahmen des regelgerecht praktizierten Geschäftsbetriebs als auch beim Einsatz krimineller Energie (Missbrauch) gewährleistet ist.

Der Konzerndatenschutz hat bei allen Vorfällen unmittelbar eigene Prüfungen eingeleitet und sich konstruktiv gestaltend an den eingerichteten Krisenteams und Sofortmaßnahmen beteiligt. So sind etwa auf Betreiben des Konzerndatenschutzbeauftragten vorsorglich Zugänge zu den Datenbanksystemen der Deutschen Telekom umgehend gesperrt worden. Festgestellte Mängel, beispielsweise beim Umgang mit Zugangskennungen, hat die Deutsche Telekom sofort beseitigt.

Aus Anlass der Datenschutzvorfälle hat sich der Konzernvorstand entschlossen, nicht nur die bekannt gewordenen Einzelfälle aufzuarbeiten, sondern eine umfassende Neubetrachtung der Situation zu Datenschutz und Datensicherheit im Konzern vorzunehmen. Deshalb hat die Deutsche Telekom über die Auditierung bestimmter Systeme oder Prozesse hinaus die gesamte Systemarchitektur und ganze Geschäftsmodelle einer intensiven Prüfung unterzogen.

Klares Ziel ist es, das Risiko von Vorfällen auf das geringstmögliche Maß zu reduzieren und vergleichbare Vorfälle in Zukunft mit größtmöglicher Verlässlichkeit zu unterbinden.

Operative Maßnahmen und Zertifizierung.

Die vom Konzern im Zusammenhang mit den Datenschutzvorfällen ergriffenen Maßnahmen hat der Vorstandsvorsitzende der Deutschen Telekom im Oktober 2008 im Rahmen der Datenschutz- und Datensicherheitsinitiative der Öffentlichkeit vorgestellt. Die Schwerpunkte liegen vor allem auf der Erhöhung der Transparenz und der Umsetzung von technisch-operativen Anpassungen, die die Datensicherheit umgehend verbessern.

Die Maßnahmen im Einzelnen:

- Der Datenschutzbeauftragte veröffentlicht jährlich einen Lagebericht, den er dem Bundesbeauftragten für Datenschutz sowie dem Aufsichtsrat vorlegt.
- Die Deutsche Telekom hat eine freiwillige Datenschutz-Zertifizierung ihrer Kundensysteme angestoßen. Beauftragt ist eine anerkannte Prüfstelle – der TÜV-IT Nord. Darüber hinaus hat die Deutsche Telekom zusätzlich zu ihren eigenen Untersuchungen ein zertifiziertes Unternehmen damit beauftragt, die Systeme systematisch auf Schwachstellen zu prüfen.
- Als erstes Unternehmen der Branche in Deutschland berichtet die Deutsche Telekom auf einer speziellen Internetseite über aktuelle kritische Datenschutzvorgänge. Um Ermittlungen nicht zu gefährden, werden die Fälle in Absprache mit den zuständigen Behörden veröffentlicht.
- Betroffene Kunden werden informiert, sobald ein konkreter Missbrauch bekannt wird.
- Die Zugriffsmöglichkeiten externer Vertriebspartner und der eigenen Mitarbeiter auf die Systeme wurden eingeschränkt. Eine PIN/TAN-Nutzung für sensible Datenbanken, die den unbefugten Zugriff von externen Rechnern auf Systeme verhindert, ist installiert.
- Die Benutzerkennungen laufen künftig in kürzeren Abständen ab und müssen erneuert werden. Zusätzlich weitet die Deutsche Telekom die Nutzung von festen IP-Adressen aus, sodass Mitarbeiter und Vertriebspartner nur von bestimmten Rechnern auf die Systeme zugreifen können.
- Die Schwellenwerte für Missbrauchserkennung sind noch sensibler eingestellt und der Automatisierungsgrad erhöht worden. Es wird automatisch früher Alarm geschlagen, wenn Schwellenwerte überschritten und ungewöhnlich viele Zugriffe registriert werden.
- Zugriffe auf Kundendaten werden konzernweit einheitlich erfasst und in kürzeren Abständen als bisher auf Unregelmäßigkeiten überprüft.
- Zum Schutz der Daten von besonders gefährdeten Personen erarbeitet die Deutsche Telekom zusammen mit dem Bundeskriminalamt und der Polizei ein spezielles Konzept.
- Die Sensibilität der Mitarbeiter für das Thema Datenschutz und Datensicherheit wurde weiter erhöht. Die Deutsche Telekom hat die bereits durchgeführten Schulungen und jährlichen Datenschutzaudits intensiviert.

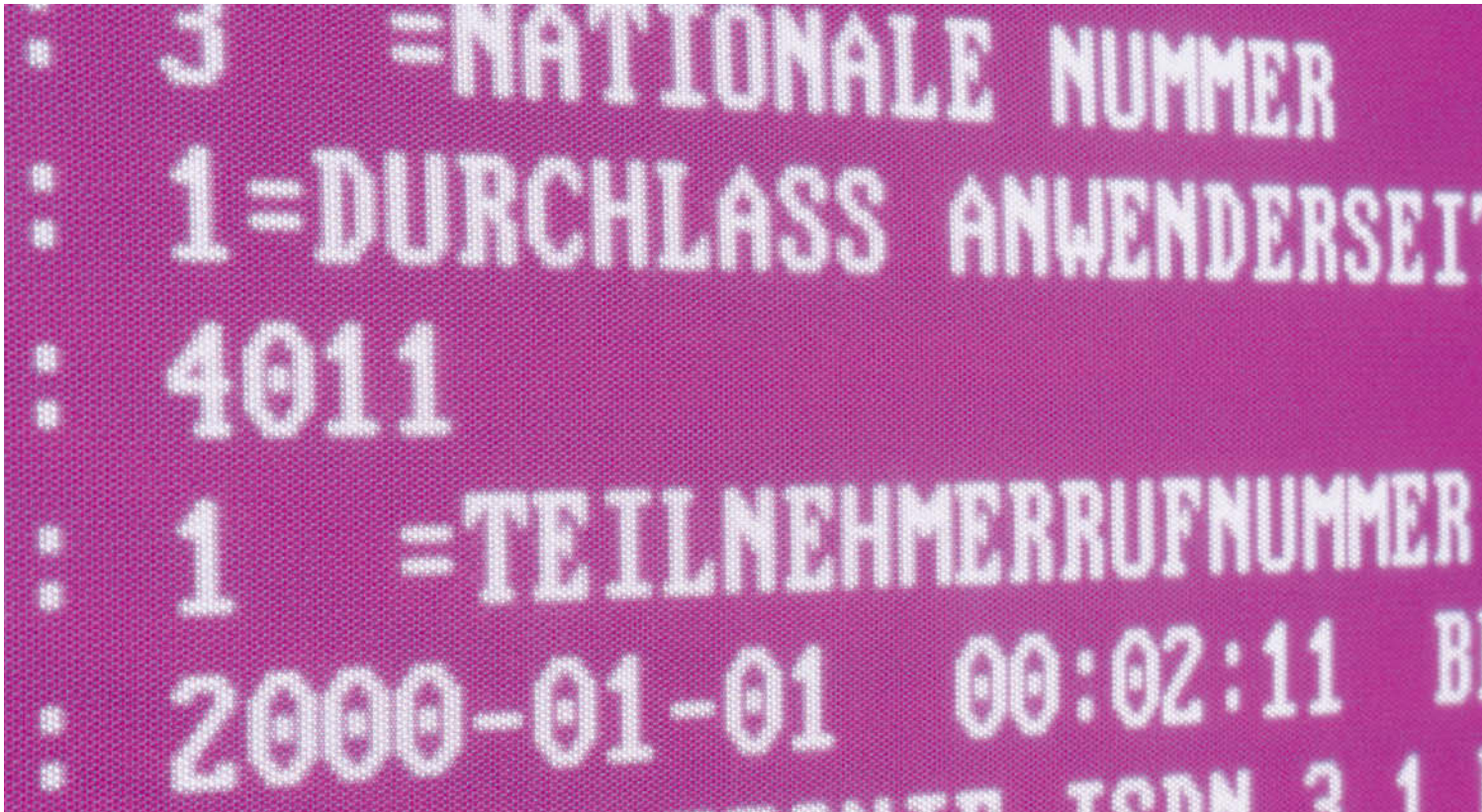
Die Umsetzung der angekündigten Maßnahmen ist inzwischen weitgehend erfolgt. Externe Dienstleister haben u. a. über 180 technische Sicherheitsaudits an Systemen durchgeführt. Besonders kritische Systeme wurden und werden einem kombinierten Datensicherheits- und Datenschutzaudit unterzogen. Im Dezember 2008 hat die Deutsche Telekom beispielsweise zusätzlich zu den Sicherheitsaudits den TÜV-IT Nord damit beauftragt, die Verarbeitungssysteme für Verkehrsdaten im Festnetzbereich im Rahmen eines gesonderten Datenschutzaudits zu prüfen. Der Zertifizierungsprozess liegt im Rahmen der Meilensteinplanungen und wird im Laufe des ersten Halbjahres 2009 abgeschlossen. Hierzu wird die Öffentlichkeit gesondert informiert.

Zusätzlich hat die Deutsche Telekom mehrere hundert operative Einzelmaßnahmen zur Erhöhung des Datenschutz- und Datensicherheitsniveaus umgesetzt bzw. angestoßen. Dazu gehört der Schutz der Kundendaten durch die Verschärfung der Zugangsvoraussetzungen. Die Anforderungen zur technischen Gestaltung der Systeme, die die Kundendaten verarbeiten, wurden erhöht. Zudem hat der Konzern Systeme abgeschaltet, wenn durch technische Verbesserungen nicht der geforderte erhöhte Sicherheitsstandard erreicht werden konnte. Die längerfristigen Maßnahmen sind in das operative Geschäft übergeleitet und werden in der Umsetzung überwacht.

Von großer Bedeutung sind in diesem Zusammenhang auch die personellen und strukturellen Neuerungen bei der Deutschen Telekom. Aufgrund der Datenschutzvorfälle wird derzeit etwa eine weitere Abteilung im Bereich Konzerndatenschutz eingerichtet, die sich zusätzlich zu den bereits bestehenden und standardisierten Vorabkontrollen für alle Systeme speziell um die Erhöhung der Kontrolldichte bei den nachgelagerten Auditierungen befassen wird. Der Fokus wird dabei nicht nur auf den IT-Systemen liegen, sondern auch auf der Kontrolle von Prozessen und Geschäftsmodellen.

Eine wichtige organisatorische Änderung zur Umsetzung der Versprechen an die Öffentlichkeit und die Kunden ist zudem die Implementierung des neuen Vorstandsressorts.

Höchstmöglicher Schutz personenbezogener Daten im täglichen Geschäftsbetrieb ist das Ziel des Datenschutzes. Anforderungen an technische Systeme wurden dazu erhöht.



Vorstand für Datenschutz, Recht und Compliance.

Das neue Vorstandsressort – Datenschutz, Recht und Compliance – wurde im Oktober 2008 eingerichtet, und der Aufsichtsrat hat Dr. Manfred Balz zum verantwortlichen Vorstand für das neue Ressort bestellt. Damit sind Datenschutz und Datensicherheit auf oberster Managementebene verankert. Das hebt die Themen auf eine deutlich höhere Wahrnehmungsstufe und gewährleistet, dass sie zukünftig noch intensiver vorangetrieben werden.

Der neue Vorstand hat unmittelbar nach seiner Bestellung ein Zehn-Punkte-Programm zur weiteren Stärkung von Datenschutz und Datensicherheit im Konzern initiiert. Dazu wird an gesonderter Stelle vom Vorstand berichtet werden. Der Konzerndatenschutzbeauftragte begrüßt dieses Programm als einen integralen Bestandteil der Neuausrichtung des Konzerns zum Thema Datenschutz.

Externe Expertise.

Die Deutsche Telekom nutzt umfangreiche externe Expertise, um den Datenschutz und die Datensicherheit im Unternehmen weiter zu optimieren. Im Oktober 2008 hat der Vorstand die Einrichtung eines Datenschutzbeirats angekündigt. Im Februar 2009 kam der Datenschutzbeirat zu seiner ersten Sitzung in Berlin zusammen. Das Gremium soll den Austausch mit führenden Datenschutzexperten und Persönlichkeiten aus Politik, Lehre, Wirtschaft und unabhängigen Organisationen über Geschäftmodelle, Prozesse und den Umgang mit Daten im Konzern fördern. Es berät den Telekom-Vorstand in datenschutzrelevanten Themen.

Im Mai 2008 hat die Deutsche Telekom den Vorsitzenden Richter am Bundesgerichtshof a. D., Dr. Gerhard Schäfer, als Sachverständigen für die Aufklärung der Vorwürfe zum Datenmissbrauch gewonnen. Als unabhängiger Experte prüft Dr. Schäfer alle relevanten Datensicherheitsaspekte der Vorwürfe und wird – soweit erforderlich – in seinem Abschlussbericht dem Vorstand der Deutschen Telekom entsprechende Vorschläge zur Verbesserung des Datensicherheitskonzepts für den Konzern machen.

Ebenso hat der Vorstand im Zusammenhang mit den Bespitzelungsvorwürfen die Kanzlei Oppenhoff zur Aufklärung des Sachverhalts eingeschaltet. Das Gutachten liegt dem Aufsichtsrat und dem Vorstand bereits vor. Die in Bezug auf den Datenschutz empfohlenen Maßnahmen setzt der Konzerndatenschutz derzeit gemeinsam mit den operativ verantwortlichen Stellen um.

Zusammenarbeit mit Aufsichtsbehörden.

Im Mittelpunkt der Zusammenarbeit des Datenschutzbeauftragten mit den Aufsichtsbehörden standen die Information, Unterstützung und die Begleitung umfangreicher Kontrollen im Zusammenhang mit den Datenschutzvorfällen. Der Schwerpunkt der Kontrollbesuche des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit war die Verarbeitung von Verkehrsdaten in verschiedenen Systemen.

Die Deutsche Telekom führt mit den zuständigen Referaten und der Behördenleitung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kontinuierlich Gespräche zu aktuellen Fragen des Datenschutzes sowie den im Konzern ergriffenen Maßnahmen. Durch die frühzeitige Einbindung der Aufsichtsbehörden in kritische Datenschutzvorgänge will der Konzern vor allem die Transparenz erhöhen.

Auch mit Vertretern der Bundesnetzagentur hat die Deutsche Telekom aktuelle Entwicklungen und die ergriffenen Maßnahmen zu Datenschutz und Datensicherheit eingehend erörtert.

Kundenkommunikation.

Zusätzlich zu den bereits etablierten Informationswegen hat die Deutsche Telekom ihre Kunden vor allem über das Internet über Datenschutz und die Verarbeitung von personenbezogenen Daten informiert. Die Kunden finden dort umfassende Dokumentationen über den Umgang mit ihren persönlichen Daten. Die wesentlichen Maßnahmen zum Datenschutz sowie Informationen über datenschutzkritische Vorfälle werden dort ebenfalls transparent aufgearbeitet.

Interne Kommunikationsmaßnahmen.

Bei den Datenschutzverletzungen im Zusammenhang mit der Bespitzelung von Aufsichtsräten und Journalisten hat sich gezeigt, dass nicht nur technische Systeme, Software und Kontrollen beim Datenschutz bedacht werden müssen. Darüber hinaus muss auch eine Unternehmenskultur entstehen, in der der Datenschutz eine bedeutendere Stellung hat. Deshalb hat der Bereich Datenschutz die Sensibilisierung der Mitarbeiter verstärkt. Zusätzlich zu Schulungen, der turnusgemäßen Neuverpflichtung der Mitarbeiter auf den Datenschutz und zahlreichen Informations- und Kommunikationsangeboten, wurde gemeinsam mit den Bereichen Konzernsicherheit und der Unternehmenskommunikation eine umfangreiche Sensibilisierungskampagne gestartet. Die Kampagne setzt auf eine starke symbolträchtige Bildersprache und nutzt Symbole wie „das rohe Ei“, das für die Sensibilität der Kundendaten steht. Die Mitarbeiter erfahren so erneut die Bedeutung des Datenschutzes und der Datensicherheit für den Konzern.

Anfragen.

Die Zahl der Kundenanfragen ist seit den Datenschutzvorfällen stark angestiegen: 2007 gab es etwa 600 Anfragen, 2008 rund 1 400. Auch die Eingaben und Anfragen der Aufsichtsbehörden haben zugenommen. Der Datenschutz hat die Beantwortung dieser Anfragen sowohl gegenüber den Kunden, der Presse als auch gegenüber den Aufsichtsbehörden fachlich-kommunikativ begleitet. Die Mitarbeiter im Vertrieb wurden gezielt darin unterstützt, vertrauensvoll mit Kundendaten umzugehen.

Gesetzliche Rahmenbedingungen.

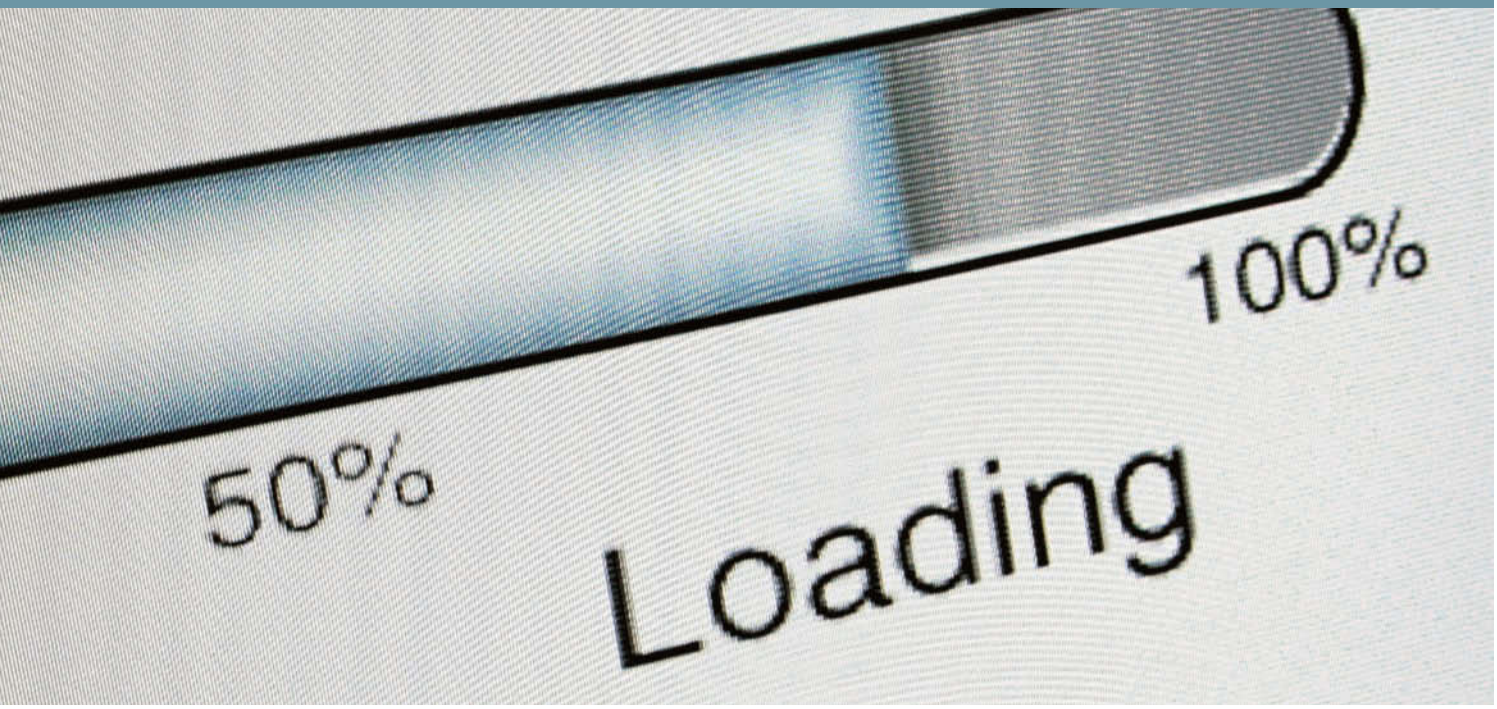
Neue Gesetze bzw. Gesetzesvorhaben hatten maßgeblichen Einfluss auf das Thema Datenschutz bei der Deutschen Telekom. Zu nennen sind vor allem die Vorratsdatenspeicherung und die Beauskunftungspflicht gegenüber den Rechteinhabern nach Änderung des Urheberrechtsgesetzes. Ferner gehört dazu die derzeit geplante, mehrstufige Novellierung des Bundesdatenschutzgesetzes.

Vor allem für die Einführung des Datenschutzauditgesetzes hat sich die Deutsche Telekom eingesetzt. Bereits zu Beginn des Jahres 2008 hat der Konzern einen Meinungsaustausch zwischen Politik und Aufsichtsbehörden initiiert. Der Konzerndatenschutz hatte den damaligen Entwurfsstand kritisch diskutiert und die grundsätzliche Bedeutung der Einführung eines für alle Beteiligten verlässlichen Verfahrens zur Auditierung in Datenschutzfragen dargestellt.

Auf europäischer Ebene wurden rechtliche Entwicklungen wie beispielsweise die e-Privacy Direktive (Richtlinie zu Privatsphäre und elektronischer Kommunikation), weiter vorangetrieben und von Verbänden und der Deutschen Telekom aktiv begleitet. Im Rahmen der europäischen Aktivitäten zur Datenschutzstandardisierung beteiligt sich die Deutsche Telekom an der Erarbeitung von Vorschlägen für Datenschutzauditierung und für Management Best Practices des europäischen Normungsinstituts CEN.

Eine interne Kampagne soll die Sensibilität für das Thema Datenschutz steigern. Datenschutz geht alle Mitarbeiter an.

Wesentliche Aktivitäten des Konzerndatenschutzes.



Umsetzung gesetzlicher und unternehmensinterner Maßnahmen.

Implementierung Vorratsdatenspeicherung.

Vorgaben.
Zum 1. Januar 2008 sind die Verpflichtungen zur Vorratsdatenspeicherung für den Bereich der Telekommunikation in Kraft getreten. Das Gesetzgebungsverfahren für die gesetzlichen Neuregelungen in den §§ 111, 113a und 113b TKG ist erst Ende Dezember 2007 beendet worden. Bis dahin war unklar, ob und wie die Vorratsdatenspeicherung in Kraft treten wird.

Nachdem der Konzerndatenschutz 2007 gemeinsam mit den anderen beteiligten Bereichen des Konzerns das Gesetzgebungsverfahren intensiv begleitet und Planungsprojekte in allen relevanten Gesellschaften der Deutschen Telekom initiiert hatte, stand 2008 die Umsetzung der gesetzlichen Verpflichtungen an.

Für die Festnetz- und Mobilfunktelefonie hatte der Gesetzgeber keinerlei Übergangsfrist vorgesehen, lediglich die Ordnungswidrigkeitentatbestände für die Nichtumsetzung waren bis zum Jahresende 2008 ausgesetzt. Andere aufsichtsrechtliche Maßnahmen – etwa wegen einer verzögerten Umsetzung – blieben möglich.

Aufgrund der vorherigen Information und Vorbereitung der operativ Verantwortlichen haben die Arbeiten für die Umsetzung auf Grundlage der vom Konzerndatenschutz entwickelten Implementierungsvorgaben zügig begonnen.

Das neue Gesetz zur Vorratsdatenspeicherung lässt in einigen Bereichen klare Regelungen vermissen und unterliegt daher der Interpretation. So bestehen z. B. im Bereich der öffentlichen Fernsprecher oder öffentlichen WLAN-Hotspots Speicherpflichten, aber nicht immer Pflichten zur Registrierung der Nutzer. Die sich daraus ergebenden Fragestellungen wurden intern bewertet und dokumentiert und mit den zuständigen Aufsichtsbehörden im Sinne einer tragbaren, datenschutzkonformen Lösung abgestimmt.

Eine besondere Herausforderung stellte die Umsetzung der im Jahr 2008 ergangenen Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung dar. Mit der Eilentscheidung im April 2008 wurden die gesetzlichen Vorgaben zur Vorratsdatenspeicherung modifiziert, d. h. eingeschränkt, in Randbereichen aber auch erweitert. Vorratsdaten zu nicht schwerwiegenden Straftaten dürfen derzeit nicht an die Strafverfolgungsbehörden übermittelt werden, müssen jedoch bis zu einer endgültigen Entscheidung des Bundesverfassungsgerichts gespeichert werden – auch über die gesetzliche Vorgabe der Speicherung von 180 Tagen hinaus.

Parallel dazu hat die Deutsche Telekom die zweite Stufe der Vorratsdatenspeicherung vorbereitet. Zum Jahreswechsel 2008/2009 war sicherzustellen, dass entsprechend den gesetzlichen Vorgaben zukünftig auch Internet-, E-Mail- und Voice-over-IP-Daten auf Vorrat gespeichert werden können.

Stand der Umsetzung.
T-Mobile speichert den überwiegenden Teil der Vorratsdaten seit Jahresbeginn 2008. Für Daten, die bisher nicht in Abrechnungssystemen gespeichert wurden, hat das Unternehmen die technischen Voraussetzungen entwickelt und die technische Realisierung im dritten und vierten Quartal 2008 umgesetzt.

T-Systems hat mehrere tausend Produkte auf Vorratsdatenspeicherungsrelevanz geprüft. Besondere Herausforderungen ergaben sich bei T-Systems aus der Internationalität und der Individualität einzelner Systeme.

T-Home begann mit der Umsetzung der Vorratsdatenspeicherung im Sommer 2008 für den Festnetzbereich. Internet- und E-Mail-Daten werden seit dem 1. Januar 2009 gespeichert.

Die Deutsche Telekom speichert gemäß Gesetz damit folgende Daten über einen Zeitraum von längstens 185 Tagen:

- **Festnetz:** Rufnummern des Anrufenden und des angerufenen Anschlusses, Beginn und Ende der Verbindung (Verbindungsdaten)
- **Mobilfunk:** Rufnummer des Anrufenden und des angerufenen Anschlusses, Beginn und Ende der Verbindung, die Bezeichnung der durch die beteiligten Anschlüsse genutzten Funkzellen, bei SMS und MMS Zeitpunkt des Versendens und des Empfangs
- **Internet-Telefonie:** IP-Adresse des anrufenden und des angerufenen Anschlusses
- **E-Mail:** Postfachkennung des Absenders und jedes Empfängers der Nachricht, IP-Adresse des Absenders, Datum und Uhrzeit der Versendung unter Angabe der Zeitzone
- **Internetzugangsdienste:** Dynamische IP-Adresse des Nutzers, die eindeutige Anschlusskennung, über die der Zugang erfolgt, Beginn und Ende der Nutzung unter der zugewiesenen IP-Adresse nach Datum, Uhrzeit und Zeitzone

Die Speicherung erfolgt in Hochsicherheitsrechenzentren, die besonderen Sicherheitsaudits unterzogen werden. Weitere Auditmaßnahmen überprüfen den datenschutzgerechten Zugriff auf die Daten. Ausschließlich besonders ermächtigtes Personal hat Zugriff auf Vorratsdaten und zwar nur dann, wenn ein staatliches Auskunftsersuchen vorliegt. Für interne Zwecke oder Zwecke Dritter dürfen die Vorratsdaten in keinem Fall verwendet werden. In dem Bereich, der die Vorratsdaten beauskunftet, hat der Konzerndatenschutz ein Datenschutzaudit durchgeführt. Das Ergebnis war positiv, die festgestellten Optimierungspotentiale hat der Bereich umgesetzt.

Im Jahr 2009 steht die Entscheidung des Bundesverfassungsgerichts zur Zulässigkeit der Vorratsdatenspeicherung an.

Datenschutzgrundkonzeption – Konzernsicherheit.
Im Jahr 2008 wurde die Datenschutz-Compliance im Bereich der Konzernsicherheit optimiert. Im Zentrum dieser Maßnahmen stand die Datenschutzgrundkonzeption Konzernsicherheit. Kernprinzip ist die zweifelsfreie Umsetzung des datenschutzrechtlichen Grundsatzes, dass personenbezogene Daten nur im Einklang mit Rechtsvorschriften verarbeitet werden dürfen. Diese Maßnahmen sind eine Reaktion auf die Vorgänge, die sich im Zusammenhang mit der Bespitzelung von Aufsichtsräten und Journalisten ereignet haben. Dabei haben sich nach dem derzeitigen Stand der Ermittlungen Teile der Konzernsicherheit massiv über Regelungen zum Datenschutz im Konzern hinweggesetzt und im Namen und mit Mitteln des Unternehmens Persönlichkeitsrechte von Dritten verletzt. Die Deutsche Telekom hat die Kontrollen und die Organisation so verändert, dass datenschutzrechtliche Grundsätze jetzt nicht mehr durch einzelne Personen umgangen werden können.

Zusätzlich wurden folgende Maßnahmen definiert und implementiert:

- Überprüfung aller Ermittlungsprozesse auf Datenschutzanforderungen
- Definition von Datenschutzprüfpunkten in den Prozessen
- Erstellung einer Datenschutzprüfcheckliste und Integration in die Ermittlungsprozesse
- Erstellung eines Datenschutzleitfadens für Ermittlungen: Datenschutzgrundkonzeption Konzernsicherheit
- Erstellung eines Meldebogens für die Konzernsicherheit bei internen Ermittlungen und Einbindung in die Ermittlungsprozesse (Vier-Augen-Prinzip)
- Klare Vorgaben zu erlaubten und nicht erlaubten Ermittlungsmaßnahmen im Bereich der Verkehrsdaten (Black/White-List)
- Durchführung intensiver Datenschutzschulungen für Ermittler
- Durchführung von Sensibilisierungskampagnen in der Konzernsicherheit

Diese neu gestaltete Datenschutzgrundkonzeption stellt den datenschutzrechtlich zulässigen Rahmen für Ermittlungstätigkeiten dar und dient damit der Durchsetzung des datenschutzrechtlichen Verbots mit Erlaubnisvorbehalt. Die allgemeinverbindlichen und grundsätzlichen Regeln zum Umgang mit personenbezogenen Daten sind für die Mitarbeiter der Konzernsicherheit transparent und verständlich dargestellt. Zur Sicherstellung der Nachhaltigkeit werden auch die Schulungen für den Bereich Konzernsicherheit kontinuierlich fortgesetzt.

Ziel für das Jahr 2009 ist es, die mit dem Konzept eingeführten Maßnahmen zu überprüfen und ggf. zu verbessern. Die Datenschutzgrundkonzeption wird deshalb auch in diesem Jahr fortgeschrieben. Besondere Maßnahmen sind darüber hinaus im Bereich der Verkehrsdatenzugriffe der Konzernsicherheit geplant.

Richtlinien und Leitfäden.

Neben dem oben erwähnten Leitfaden für datenschutzkonforme Ermittlungen hat der Datenschutz weitere Richtlinien entwickelt. So wurden die Anforderungen an die Passwortkomplexität weiter überarbeitet und systematisiert. Ferner fand eine Prüfung aller Datenarten statt, die im Konzern erhoben und verarbeitet werden. Sämtliche Datenarten wurden in einer Richtlinie erfasst, kategorisiert und entsprechend ihren Datenschutz- und Sicherheitsbedürfnissen bewertet. Dadurch wird u. a. erreicht, dass die technischen Datenschutz- und Datensicherheitsanforderungen an IT-Systeme optimiert werden können.

Zusätzlich zu dem bereits bestehenden Leitfaden hat der Konzerndatenschutz u. a. praxisgerechte Checklisten für die Zulässigkeit der Verarbeitung von personenbezogenen Daten im Ausland erstellt und in die Unternehmensprozesse implementiert. Des Weiteren erarbeitet der Konzerndatenschutz eine spezielle Prozessübersicht zum Datenschutz, die 2009 abgeschlossen werden soll.

Basisdatenschutzaudit 2008.

Seit 1997 führt die Deutsche Telekom jährlich ein Basisdatenschutzaudit bis auf Mitarbeiterebene im Rahmen einer Selbstauskunft mit anschließenden Stichprobenkontrollen durch. Das Audit hat sich als effektives Instrument herausgestellt, um Schwachstellen aufzudecken und Handlungsnotwendigkeiten auf allen Managementebenen zu erkennen. 2008 nahmen auf nationaler Ebene 93 932 Mitarbeiter am Basisdatenschutzaudit teil, 80 275 IT-Systeme, wie z. B. Personal Computer, wurden auditiert. Durch die jährliche Abfrage werden die Mitarbeiter regelmäßig für aktuelle und grundsätzliche Datenschutzfragen sensibilisiert. Durch die Selbstauskunft des Managements erreicht das Basisdatenschutzaudit eine Verbindlichkeit, die über diejenige von reinen Richtlinienvorgaben weit hinausgeht. Auch auf internationaler Ebene hat die Deutsche Telekom ein Datenschutzaudit durchgeführt, das seit 2006 in den internationalen Beteiligungsgesellschaften angewendet wird.

Grundlagen des Basisdatenschutzaudits.
Das Basisdatenschutzaudit erfasst die zentralen Datenschutzanforderungen des Bundesdatenschutzgesetzes, des Telekommunikationsgesetzes und des konzernweiten Privacy Code of Conduct der Deutschen Telekom (siehe Anhang). Die Fragebögen beziehen sich auf die wesentlichen Prozesse, welche die Einhaltung dieser Anforderungen und deren Umsetzung in den einzelnen Konzerneinheiten sowie deren Einhaltung vor Ort auf Mitarbeiterebene sicherstellen. Auf Ebene der Unternehmensleitung sind vor allem die Themen Datenschutzorganisation, Einbeziehung des Datenschutzbeauftragten in die wesentlichen Prozesse der Produkt- und Anwendungsentwicklung und die Prozesse zur Gewährleistung der Betroffenenrechte (Auskunft, Berichtigung, Löschung personenbezogener Daten) Gegenstand des Audits. Auf Team-/Mitarbeiterebene stehen die Verpflichtung und Schulung von Mitarbeitern sowie die Einhaltung von grundlegenden technischen Datenschutzanforderungen (z. B. Verschlüsselungsmöglichkeiten) im Vordergrund. Die Selbstauskünfte der Mitarbeiter prüfen die Datenschutzbeauftragten in Stichproben auf ihre Richtigkeit.

Vorteile des Basisdatenschutzaudits.
Das jährliche Basisdatenschutzaudit soll nachhaltig die Sensibilität und das Datenschutzbewusstsein bei den Mitarbeitern des Konzerns fördern. Der Grad der Compliance mit gesetzlichen und unternehmensinternen Anforderungen wird auf allen Konzernebenen transparent. Das Management erhält einen Überblick über den allgemeinen Stand des Datenschutzniveaus im Konzern, kann mögliche Defizite abstellen und damit das Datenschutzniveau im Unternehmen kontinuierlich erhöhen. Die Ergebnisse sowie die Fragestellungen werden jährlich einem detaillierten Monitoring unterzogen und bei Bedarf angepasst und weiterentwickelt.

Internationales Datenschutzaudit.
Das internationale Datenschutzaudit basiert auf den Vorgaben unseres Privacy Code of Conduct, durch dessen weltweite Implementierung die Weiterentwicklung international anerkannter Standards und die Sicherstellung eines angemessenen Datenschutzniveaus gewährleistet werden kann. Berücksichtigung finden dabei immer die jeweiligen nationalen Vorgaben und Lösungen zum Schutz des Persönlichkeitsrechts.

Im Herbst 2008 hat die Deutsche Telekom das dritte internationale Datenschutzaudit durchgeführt. Im Rahmen einer Selbstauskunft beantworteten die Datenschutzbeauftragten von internationalen Tochtergesellschaften Fragen zur Organisation und zum Vorgehen beim Datenschutz in ihren Landesgesellschaften. Es nahmen 21 Tochtergesellschaften aus 16 Ländern teil. Als regelungsbedürftige Ergebnisse wurden u. a. die teils mangelnde Einbeziehung der Datenschutzbeauftragten in die Anwendungs- und Produktentwicklungsprozesse sowie die ebenfalls teilweise nicht ausreichend vorhandenen Verschlüsselungsmöglichkeiten von vertraulichen Informationen festgestellt.

Die Teilnehmer des Audits erhielten ihr Ergebnis zusammen mit einer Schwachstellenanalyse und Verbesserungsvorschlägen. Die Umsetzung wird durch unterstützende Maßnahmen wie International Privacy Circles, Schulungsunterlagen sowie Informations- und Kontrollbesuche vor Ort begleitet.

Interne Sicherheitstests.
Bei übergreifenden Systemprüfungen wurden im Jahr 2008 über 200 Sicherheitstests durchgeführt. Diese erfolgten zusammen mit anderen Bereichen des Unternehmens bspw. mit den auf IT-Sicherheit spezialisierten Kollegen der Konzernsicherheit.

Es erfolgten umfangreiche Penetrationstests auf den Service-, Authentisierungs- und Kommunikationsplattformen sowie auf den Zugangsplattformen für Kunden. Ebenfalls wurden die Systeme überprüft, die Kundendaten führen, und entsprechende Audits bei Outsourcing-Partnern unterstützt.

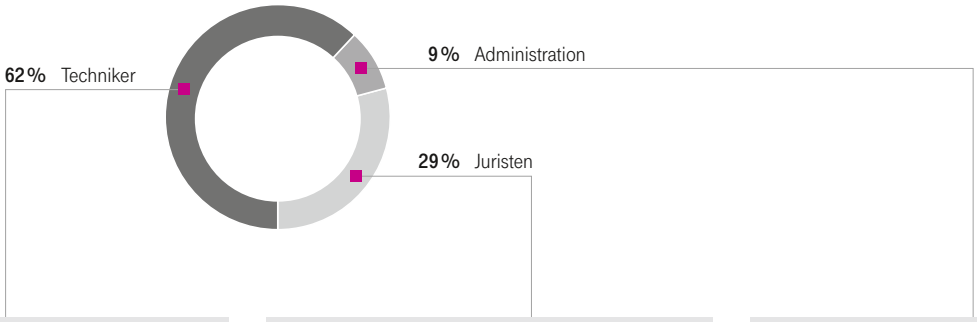
Die Netzwerkaudits zielten auf die Netzplattformen, Netzelemente und auch auf die netznahen Applikationen. Hinzu kamen die Überprüfung der physikalischen Infrastruktur mit Zutrittsschutz und Brandschutz sowie die Überprüfung der Sicherheitsprozesse und deren Anwendung und Umsetzung.

Folgende Verbesserungen resultierten aus den Sicherheitstests:

- Durch Analyse und Bewertung von mehr als 400 Anwendungen wurden die Systeme bewertet, die Kundendaten führen (inklusive Risikoabschätzung).
- Das Risiko für unautorisierte Zugriffe auf Plattformen und Applikationen wurde minimiert.
- Die Zahl der vorhandenen Accounts wurde durch Löschung von Zugängen signifikant reduziert.
- Die unautorisierte Veränderung von Zugriffsrechten wurde unterbunden.
- Vorhandene Trivial-Passwörter wurden identifiziert und den verschärften Passwortregeln angepasst.

Mit diesen Maßnahmen wurde die Datensicherheit und damit der Datenschutz erheblich verbessert.

Kompetenzen und Aufgaben im Konzerndatenschutz.



Technik/Sachbearbeitung

- Beratung bei Projekten und Prozessen
- Prüfung und Freigabe von Datenschutzkonzepten
- Technische Kontrollen (Audits)

Recht

- Vertragsgestaltung und -prüfung
- Konzeption von Richtlinien
- Begleitung bei der Entwicklung von Geschäftsmodellen

Assistenz

- Unterstützung bei Schulungen
- Steuerung der Koordinatoren
- Reporting

Kommunikationsmaßnahmen.

Datenschutz umfasst auch die Interaktion mit den Kunden, um insbesondere bei Vorfällen das Gefährdungspotential umgehend zu minimieren.

Kundenkommunikation.

Nach Bekanntwerden der Datenschutzvorfälle Mitte 2008 hat die Deutsche Telekom ihre Maßnahmen für Datenschutz- und Datensicherheit mit Hilfe umfassender Berichterstattungen und Spezialreports im Internet dargestellt. In umfangreichen Frage- und Antwort-Zusammenstellungen mit Bezug zum Schutz und zur Sicherheit der Kundendaten konnte und kann sich die Öffentlichkeit informieren.

Insbesondere werden kritische Datenschutzvorfälle und der Stand der Aufarbeitungen dargestellt. Diese Übersicht wird bei Erforderlichkeit unmittelbar aktualisiert und sorgt somit für weitgehende Transparenz nach außen. Die Berichterstattung via Internet wurde 2008 durch Anschreiben an Kunden ergänzt, die möglicherweise von Datenmissbrauch betroffen waren. Anfragen können die Kunden weiterhin an die E-Mail Adresse datenschutz@telekom.de richten.

Die Kommunikation von Datenschutzvorfällen ist eine Forderung, die in den Änderungsvorschlägen zum Bundesdatenschutzgesetz enthalten ist und die vom Konzerndatenschutz und der Deutschen Telekom begrüßt wird.

Interne Kommunikationsmaßnahmen.

Die Zusammenarbeit mit dem konzerninternen Arbeitgeberverband und mit den Arbeitnehmervertretungen war 2008 aufgrund der Datenschutzvorfälle, die Aufsichtsrat und Arbeitnehmervertreter betrafen, von besonderer Bedeutung. So wurden zu verschiedenen Zeitpunkten die Aktivitäten und Maßnahmen des Konzerns im Zusammenhang mit den Datenschutzvorwürfen mit dem Konzernbetriebsrat diskutiert und bewertet.

Der Konzerndatenschutz nimmt regelmäßig an den Arbeitssitzungen der Arbeitgeber- und Arbeitnehmervertretungen teil und unterstützt die Diskussionen durch seine neutrale Expertise. Als zentrale Anlaufstelle für Mitarbeiteranfragen zum Datenschutz sorgt der Konzerndatenschutz dafür, dass Anregungen und Vorschläge aufgenommen werden.

Darüber hinaus ist die Sensibilisierung der Mitarbeiter ein wichtiger Teil der Arbeit des Konzerndatenschutzes. Regelmäßig wird über aktuelle Datenschutzthemen im Intranet der Deutschen Telekom und im Datenschutznewsletter informiert. Grundlageninformationen, wie das Datenschutzhandbuch, Arbeitshilfen und Schulungen, wurden erweitert und zum Abruf sowohl auf nationaler als auch auf internationaler Ebene zur Verfügung gestellt. Eine Richtlinendatenbank ermöglicht zudem den Zugriff auf alle wichtigen Regelungen.

Zusätzlich zu den regelmäßigen Datenschutz-Basisschulungen und zur Verpflichtung auf das Daten- und Fernmeldegeheimnis stehen Online-Arbeitshilfen und Online-Schulungen, Dokumentationen sowie Datenschutzvorträge für alle Mitarbeiter zur Verfügung. Ergänzt wird dies durch ein umfangreiches Angebot an Präsenzschulungen zu verschiedenen Schwerpunkten wie z. B. die Themen Kundendatenschutz, Personaldatenschutz und Datenschutz in Call-Centern.

2008 hat der Konzerndatenschutz gemeinsam mit der Konzernsicherheit und der Unternehmenskommunikation eine Sensibilisierungskampagne zum Thema „Kundendatenschutz und Kundendatensicherheit“ durchgeführt. Im November 2008 startete zudem die Maßnahmeninitiative „Schutz von Kundendaten geht alle an!“

Die Maßnahme wurde durch Plakate, Postkarten sowie Artikel und Experten-Interviews im Intranet unterstützt. Hilfsmittel wie Merkblätter und Chartsätze sind weitere Bestandteile der internen Kommunikation. Darüber hinaus visualisieren Filme die Themenschwerpunkte in entsprechenden Situationen mit einer integrierten Hilfestellung.

Die Deutsche Telekom beteiligt sich auch an den Veranstaltungen zum Europäischen Datenschutztag, den die Europäische Union jeweils am 28. Januar eines Jahres begeht. So hat der Konzerndatenschutz am 28. Januar 2008 zu einem internationalen Ideenwettbewerb „Datenschutz ohne Grenzen“ aufgerufen. Mitarbeiter haben in einem Bild oder Photo, einem Spruch oder einem Symbol ausgedrückt, wie ihre Vorstellung von Datenschutz ist. Die Anzahl der Einsendungen hat die Erwartungen mit mehr als 600 Einsendungen übertroffen. Die besten Vorschläge wurden prämiert und in konzernweiten Plakatkampagnen zur Steigerung der Aufmerksamkeit für den Schutz von personenbezogenen Daten eingesetzt. Die Gewinnerin, eine Mitarbeiterin von T-Mobile USA, wurde vom Vorstandsvorsitzenden in die Service-Zentrale der Deutschen Telekom nach Bonn eingeladen.

Internationale Koordinierung.

Die zunehmende Internationalisierung der Deutschen Telekom erfordert auch eine tragfähige Strategie zum internationalen Datenschutz. Schließlich müssen auch länderübergreifende Anforderungen an Datenschutzlösungen berücksichtigt werden. Durch die internationale Ausrichtung werden aus organisatorischen Gründen oder wegen grenzüberschreitender Kundenprojekte innerhalb des Konzerns zunehmend Daten austauscht. Der Konzerndatenschutzbeauftragte und seine Organisation unterstützen das internationale Geschäft der Deutschen Telekom und bauen hierzu auf eine kontinuierliche Kommunikation und Information sowie den Prozess der regelmäßigen Selbstauskunft durch Auditierung.

International Privacy Circles.
Einmal pro Jahr finden die Internationalen Privacy Circles für die internationalen Einheiten der Deutschen Telekom für die Region Europa/Afrika, North/South America und Asia/Pacific statt. Sie sind etablierter Bestandteil des Roll-outs und der effektiven Betreuung des Privacy Code of Conducts (siehe Anhang) der Deutschen Telekom.

Die Datenschutzvorfälle in Deutschland boten eine Grundlage für einen übergreifenden und intensiven Austausch mit den Beteiligungsgesellschaften der Deutschen Telekom. Fragen zum internationalen Datenschutzstandard im Unternehmen bei Kundenmanagementsystemen, Betrugsprävention und -aufklärung wurden diskutiert. Der Austausch über Fragen zu Kundeninformationen bei Datenschutzvorfällen („notification procedures") gab weitere Einblicke in den Umgang mit personenbezogenen Daten und Missbrauchsvorfällen im internationalen Vergleich.

Gestaltungsmöglichkeiten der internationalen Zusammenarbeit wurden behandelt. So wird die enge Begleitung des internationalen Datenschutzaudits durch Stichprobenkontrollen, sog. „spotchecks", und Beratungen vor Ort unterstützt und weiter intensiviert. Beschlossen wurde auch die Erstellung von internationalen Anforderungskonzepten zum Datenschutz. Über Datenschutzleitlinien und gemeinsame Positionspapiere (sog. „papers of common understanding") werden einheitliche Standards und Vorgehensweisen auf internationaler Ebene im Umgang mit personenbezogenen Daten etabliert.

Kundendatenverarbeitung.

Durchführung von Audits bei externen Call-Centern.
Die Deutsche Telekom nutzt externe Vertriebspartner u. a. auch zur Abwicklung von Kundenaufträgen, -beschwerden und -fragen als Call-Center für den Kundenservice. Für diese Aufgaben müssen die Vertriebspartner Zugriff auf die IT-Anwendungen erhalten, die auch von internen Call-Centern für dieselben Zwecke genutzt werden. Dabei werden personenbezogene Daten im Auftrag der Deutschen Telekom verarbeitet. § 11 Bundesdatenschutzgesetz schreibt vor, dass dieser Auftrag schriftlich zu erteilen ist und der Auftragnehmer sorgfältig ausgewählt werden muss. Der Auftraggeber hat sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes zu überzeugen. Der Konzerndatenschutz hat deshalb in 2008 in mehreren Fällen Vor-Ort-Überprüfungen bei Vertriebspartnern durchgeführt. Bei den überprüften Vertriebspartnern wurden keine wesentlichen Mängel aus datenschutzrechtlicher Sicht festgestellt. Der Konzerndatenschutz hat den Vertriebspartnern im Anschluss einen Auditbericht übermittelt, in dem die festgestellten Nachbesserungsbedarfe aufgezeigt und Maßnahmen zur Mängelbeseitigung vereinbart wurden. Die Erfüllung der Anforderungen hat der Konzerndatenschutz gemonitort.

In Bereichen, die Kundendaten verarbeiten, hat der Konzerndatenschutz die Kontrollen und Audits verstärkt.

Im Rahmen einer anlassbezogenen Prüfung von Unregelmäßigkeiten, die durch ein installiertes Missbrauchskontrollsystem erkannt wurden, sind bei einem Vertriebspartner Mängel im Umgang mit den Kundendaten festgestellt worden. Der Konzerndatenschutz der Deutschen Telekom hat in diesem Fall mit dem Datenschutzbeauftragten des Vertriebspartners Kontakt aufgenommen, um die Mängelbeseitigung unmittelbar anzustoßen und zu begleiten. Im Zusammenhang mit diesen Überprüfungen ist der Konzerndatenschutz auf weitere Prozesse bei Handelspartnern im Shop-Geschäft gestoßen, die möglicherweise ebenfalls mängelbehaftet sind und die derzeit weiter überprüft werden.

Kooperationsverträge DTKS (Deutsche Telekom Kundenservice).
Die Kooperationsverträge zu Vertrieb und Service zwischen T-Mobile und DTKS (Deutsche Telekom Kundenservice) einerseits und zwischen Deutscher Telekom AG und DTKS andererseits wurden 2008 insgesamt überarbeitet und neu vereinbart. Dem Kooperationsmodell, nach dem die DTKS einen Teil der Kundenbetreuungsaufgaben für den Konzern wahrnimmt, liegt das Konzept der Auftragsdatenverarbeitung zugrunde, das auch für die Legaleinheiten innerhalb des Konzerns gilt. Der Konzerndatenschutz war bereits in die Entwicklung der Erstverträge einbezogen und hat nun auch die Erstellung der neuen Verträge betreut. Eine besondere Schwierigkeit liegt darin, dass die DTKS einerseits als Auftragsdatenverarbeiter weisungsgebunden ist und sich an detaillierte Vorgaben der Auftraggeber halten muss, sie andererseits jedoch das Selbstverständnis hat, in gewissen Grenzen eigenständig und eigenverantwortlich zu agieren. Der Konzerndatenschutz hat den beteiligten Fachseiten die Bedeutung der datenschutzrechtlichen Rahmenbedingungen erläutert und deren Akzeptanz erreicht.

Arbeitsplatzsicherheit – Minimierung potentieller Risiken.
Die Möglichkeit, umfangreiche Datensätze unauffällig per Mail von einem Arbeitsplatzrechner zu versenden, wurde durch eine Größenbeschränkung der Anhänge auf zehn MByte erschwert. In Ergänzung hierzu wird gegenwärtig bei vertriebsnahen Funktionen die Sperrung der USB-Schnittstelle für den Anschluss von Massenspeichergeräten (Sticks, externe Festplatten) umgesetzt. Auf CD/DVD-Brenner wird kein schreibender Zugriff mehr möglich sein.

Mit der derzeit laufenden Umrüstung auf Terminalsysteme (sog. „Thin-Clients“), ohne die Möglichkeit einer lokalen Datenspeicherung, bei den Telekom Shops und im Servicebereich wird die Gefahr von Massendatenkopien maßgeblich verringert.

Zur weiteren Reduzierung potentieller Risiken hat die Deutsche Telekom auch die Administrationsrechte für die Arbeitsplatzsysteme der Mitarbeiterinnen und Mitarbeiter eingeschränkt. Die Rechte werden nur noch nach einem speziellen Freigabeprozess vergeben. Das Verfahren wird gegenwärtig getestet und anschließend sukzessive von den Organisationseinheiten übernommen.

Die sichere Datenlöschung bei Alt-Geräten wird durch eine lückenlose Nachweiskette sichergestellt; Kernelemente des Prozesses sind bereits eingeführt.

Konzernweite Einwilligungserklärung.
Die betriebliche Regelung zur Konzerneinwilligungsklausel für die Deutsche Telekom wurde aktualisiert. Mit der aktiven Abgabe dieser Einwilligungsklausel erlaubt der Kunde dem Konzern seine Vertragsdaten innerhalb des Konzerns für Beratungs-, Werbungs- und Marktforschungszwecke zu verwenden.

Die vereinbarte betriebliche Regelung umfasst und beschreibt die Prozesse zur Einholung und Erfassung der Konzerneinwilligungsklausel in allen relevanten IT-Systemen, insbesondere die sichere Dokumentation eingeholter Einwilligungen. Bei Call-Centern, die keine ausreichende Dokumentation zum Nachweis darstellen können, ist deren Einholung außer Kraft gesetzt.

Datenschutzkonforme Löschung von Kundendaten.
Datenschutzrechtlich geprüft wurde die Einhaltung der gesetzlichen Speicherfristen und Löschfristen von Kundendaten bei den wichtigsten IT-Verfahren und -Systemen der Deutsche Telekom AG und T-Mobile Deutschland. Insgesamt war das Ergebnis zufriedenstellend. Die entsprechenden Anpassungsbedarfe wurden an die verantwortlichen Stellen adressiert. Die Umsetzung wird vom Konzerndatenschutz überwacht.

Neue Verträge für Vertrieb und Handel.
Für den Vertrieb und Handel hat die Deutsche Telekom ein komplett überarbeitetes Paket an Musterverträgen entwickelt. Die bisherigen Muster haben nicht mehr den aktuellen Anforderungen der sehr unterschiedlichen Vertriebsmodelle entsprochen. Die neuen Verträge basieren auf einem Baukastensystem: Der Hauptvermarktungsvertrag, der die wesentlichen Rechte und Pflichten des jeweiligen Händlers enthält, wird bei Bedarf um eine oder mehrere Zusatzvereinbarungen ergänzt, die jeweils bestimmte Vermarktungsformen bzw. -kanäle regeln. Ziel ist der Austausch aller derzeit mit T-Mobile und T-Home bestehenden Händlerverträge, sodass jeder Händler künftig nur noch einen Vertrag bzw. ein Vertragspaket mit der Deutschen Telekom Gruppe unterhält. Der Konzerndatenschutz hat an der Entwicklung des Vertragspakets mitgewirkt und insbesondere eine vollständig überarbeitete und an die neue Vertragssystematik angepasste Datenschutzvereinbarung bereitgestellt. Das neue Vertragspaket wird sukzessive an die Händler ausgeliefert.

Künftiges Verfahren zur Prüfung von Kundenlisten.
Bei den Systemüberprüfungen im Zusammenhang mit den Datenschutzvorfällen wurde festgestellt, dass aus verschiedenen Systemen Listen mit Kundendaten generiert wurden, die auf einem nicht datenschutzkonformen Weg ausgetauscht wurden. Gemeinsam mit den Bereichen Qualitätsmanagement von T-Home und T-Mobile sowie der Konzernsicherheit wurde deshalb ein Verfahren zur Prüfung von Kundenlisten, also dem Export von Daten aus Systemen in Listenform, entwickelt. Die bereits vorhandenen Listen wurden überprüft und wo erforderlich datenschutzkonform ausgestaltet.

Das neue Verfahren zur Listenprüfung ermöglicht es den operativ verantwortlichen Stellen, die Nutzung von Kundendaten selbst einzustufen und zu dokumentieren. Der Konzerndatenschutz und die Konzernsicherheit stehen zur Absicherung der Datenschutz- und Datensicherheitsaspekte beratend zur Verfügung.

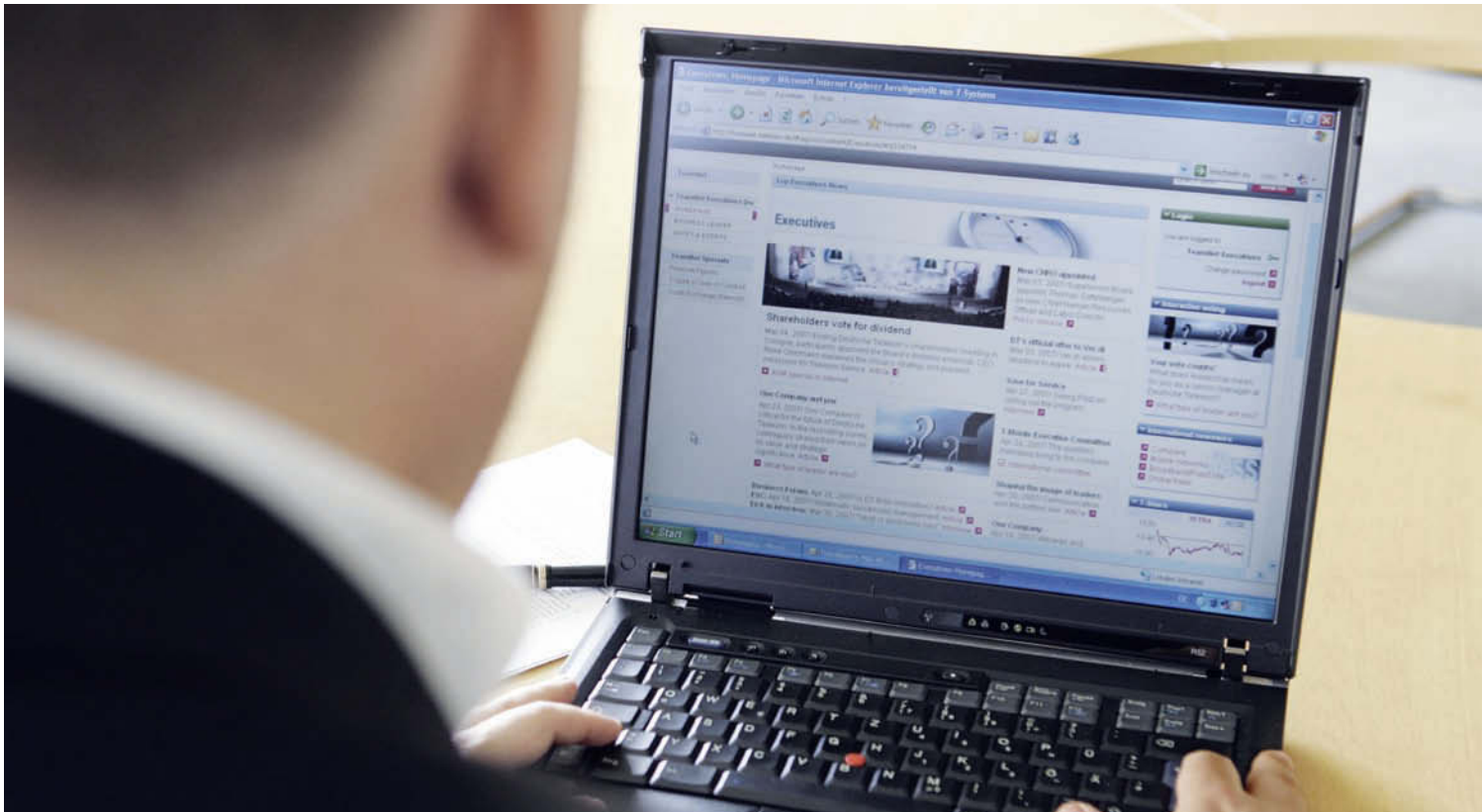
Listen mit Kundendaten sind sowohl intern als auch extern in allen Geschäftsbereichen zur Aufgabenerledigung notwendig: beispielsweise für die Vorbereitung von Marketingkampagnen, den Einsatz von Servicetechnikern aber auch beim Einsatz von externen Vertriebspartnern zur Kundenansprache im Auftrag der Deutschen Telekom. Letzteres insbesondere dann, wenn den Vertriebspartnern z. B. nur thematisch abgegrenzte Daten zur Verfügung stehen sollen.

Betriebliche Regelung „Legitimation“.
Nachdem die uneinheitliche Handhabung der Kundenlegitimation bei den Konzerntöchtern im Rahmen eines Kontrollbesuchs festgestellt worden war, wurde gemeinsam mit den verantwortlichen Abteilungen eine einheitliche betriebliche Regelung zur „Legitimation“ erstellt. Diese regelt, wie sich ein Kunde gegenüber der Deutschen Telekom beim Call-Center oder am Point of Sales als Neu- oder Bestandskunde identifizieren muss, um z. B. einen Auftrag zu erteilen, Änderungen an einem bestehenden Anschluss vorzunehmen oder Informationen zur Rechnung zu erhalten.

Mit der Neuregelung wurde die Legitimationsrichtlinie zugleich den organisatorischen Änderungen im Konzern zur einheitlichen Kundenbetreuung über die Deutsche Telekom Kundenservice Gesellschaft und die Telekom Shop Gesellschaft sowie den damit einhergehenden gesetzlichen Anforderungen angepasst.

Weitergehende Modelle zur Verbesserung der Sicherheit in der Kundenlegitimation werden mit den Fachseiten im Laufe des Jahres 2009 entwickelt.

Bei Arbeitsplatzrechnern in vertriebsnahen Bereichen werden Funktionen eingeschränkt: Sperrung der USB-Schnittstelle für den Anschluss von Massenspeichergeräten, auf CD/DVD-Brenner wird kein schreibender Zugriff ermöglicht.



Kontrollbesuche des Bundesdatenschutzbeauftragten/Anfragen.
Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) hat anlässlich der Datenschutzvorfälle und der Diskussion um Datenschutz und Datensicherheit bei der Deutschen Telekom zahlreiche Kontrollbesuche durchgeführt. Schwerpunkt war die Überprüfung der Verarbeitung von Verkehrsdaten bei T-Home und T-Mobile Deutschland im Rahmen der Billingkette, die von der Rohdatenverarbeitung der reinen technischen Verkehrsdaten bis zur Rechnungsstellung für Endkunden und Provider reicht. Weiterer Schwerpunkt der Prüfungen waren die Missbrauchserkennungssysteme. Die Kontrollbesuche des BfDI wurden über einen Zeitraum von mehreren Monaten an verschiedenen Standorten durchgeführt und vom Konzerndatenschutz organisatorisch begleitet.

Die Prüfungen waren im September 2008 beendet.

Im Februar 2009 wurden im formellen Verfahren zur Stellungnahme an die Bundesnetzagentur Nachbesserungsbedarfe adressiert. Die Deutsche Telekom prüft diese Sachverhalte derzeit und wird dazu innerhalb der gewährten Stellungnahmefrist gegenüber der Bundesnetzagentur Stellung nehmen.

Die Auskunftsverlangen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit stiegen 2008 um etwa 100 auf 280. Abgefragt werden in der Regel Informationen zu Betroffenenbeschwerden, die direkt an die Behörde gerichtet werden. Teilweise wird auch Auskunft zu technischen Gestaltungen von Systemen oder Geschäftsmodellen verlangt, die dann im Einzelnen dargestellt und begründet werden.

Kundenanfragen und Kundenbeschwerden.
Im Jahr 2008 sind die beim Konzerndatenschutz eingegangenen Kundenanfragen und Kundenbeschwerden, insbesondere bedingt durch die Datenschutzvorfälle, signifikant gestiegen von etwa 600 in 2007 auf etwa 1 400 in 2008. Inhaltlicher Schwerpunkt der Kundenanfragen und Kundenbeschwerden waren Auskunftsverlangen zu den gespeicherten Kundendaten, die Frage nach der Sicherheit der gespeicherten personenbezogenen Daten und die Frage nach der individuellen Betroffenheit durch die Datenvorfälle.

Insbesondere zur Frage nach der Betroffenheit vom Datenklau 2006 hatten sich (Stand Redaktionsschluss) 615 Privatkunden gemeldet, die der Konzerndatenschutz entsprechend informiert hat.

Ferner zeigte sich, dass die Kunden sensibler gegenüber der Ansprache durch die von der Deutschen Telekom beauftragten Vertriebspartner waren. So gab es vermehrt Nachfragen, ob etwa die Deutsche Telekom Daten unzulässigerweise an Dritte weitergibt und ob die Vertriebspartner entsprechend autorisiert seien.

Betreuung von Großprojekten, Geschäftskunden und Beteiligungen.

Projektunterstützung.
Die Unterstützung von internen und externen Projekten im Bereich Großkunden der Deutschen Telekom wurde 2008 mit 240 neuen Projekten gegenüber dem Vorjahr 2007 mit 105 Projekte deutlich intensiviert. Neben der operativen Projektarbeit wurden folgende Dokumente für Großkunden und Projektmanager erstellt:

- Leitfaden „Datenschutz im Rahmen von Ausschreibungen im Geschäftskundenvertrieb“
- Kundenbroschüre „Datenschutz im öffentlichen Sektor“
- Informationsleitfaden für Projektleitungen
- Internes Arbeitsdokument „Beratung Healthcare Projekte“

Support Geschäftskundenprojekte.
Der Konzerndatenschutz erbringt für alle Geschäftskundensegmente des Vertriebs kunden- und branchenspezifische Beratungsleistungen im Datenschutz. Die projektspezifischen Anforderungen an datenschutzrechtliche Rahmenbedingungen, Zulässigkeitsvoraussetzungen sowie die angemessenen technischen und organisatorischen Maßnahmen an Lösungen ergeben sich aus dem konkreten Einzelfall.

Im Jahr 2008 wurden etwa 200 Geschäftskundenprojekte des Vertriebs begleitet. Inhaltlich betrafen sie insbesondere folgende Themenkomplexe: PreSale-Aktivitäten, Ausschreibungen, Gestaltung von Leistungen und Verträgen, Gestaltung und Realisierung von Kundenlösungen, Zusammenstellung eines Gesamtkonzepts Datenschutzmaßnahmen und Abstimmung von Lösungen mit der zuständigen Datenschutzaufsichtsbehörde des Kunden.

Beispiel einer Betreuung anhand eines Großkunden der T-Systems.
Ein Kunde mit Stammsitz in Deutschland plante, Daten von einer in der Europäischen Union ansässigen Tochter auf zentrale Ressourcen in Deutschland zu überführen. In diesem Zusammenhang wurden zahlreiche Fragen zur Datenherrschaft und zur Zulässigkeit des grenzüberschreitenden Datenverkehrs aufgeworfen. Bei den Daten handelte es sich um vertriebsrelevante Daten, u. a. zu Endkunden, Produkten und Marketing. Im Ausschreibungsverfahren waren sämtliche betrieblichen Vorgaben des Kunden zum Datenschutz und zur Datensicherheit auf Kompatibilität mit dem innerbetrieblichen Datenschutz des Konzerns Deutsche Telekom zu prüfen und zu bewerten. Der Konzerndatenschutz hat die Verträge analysiert, bewertet und mit der operativ verantwortlichen Stelle Lösungsmöglichkeiten diskutiert. Im Hinblick auf die kompatiblen Lösungsangebote erfolgte der Zuschlag schließlich für T-Systems.

Leistungen für interne Projekte im Konzern Deutsche Telekom.
Der Konzerndatenschutz unterstützt im Rahmen der vorhandenen Kapazitäten alle konzerninternen Fachseiten bei der Realisierung ihrer Dokumentationspflicht in Form von Datenschutzkonzepten im Rahmen der Einführung interner IT-Systeme. Darüber hinaus hat der Bereich einzelne IT- und TK-Lösungen sowie betriebliche Prozesse datenschutzrechtlich auditiert. Insgesamt wurden 36 größere konzerninterne Projekte begleitet, u. a. die Neuentwicklung des Datenschutzkonzepts SAP HR des Konzerns sowie die Integration des SAP HR GK. Innerhalb des Projekts IEI (Integrated Enduser Infrastructure) wurde die Qualitätssicherung bei der Erstellung von Datenschutzkonzepten übernommen.

Interne Vergabe von IT-Dienstleistungen.
Im Zusammenhang mit einer Kundeneskalation wurde bei T-Systems die Überprüfung des internen Beauftragungsprozesses zur Vergabe von IT-Dienstleistungen an Tochterunternehmen von T-Systems in Europa und im außereuropäischen Ausland angestoßen. Im Zentrum der Fragestellung stand und steht von Seiten des Konzerndatenschutzes insbesondere die Art der vertraglichen Legitimation und die datenschutzrechtliche Zulässigkeit der Verlagerung von Diensten. Die Überprüfung erfolgt gemeinsam mit anderen Querschnittsbereichen und unter enger Einbindung der operativ verantwortlichen Stellen. Alle Anwendungen und Verträge werden an einer definierten Anforderungsmatrix gemessen und identifizierter Anpassungsbedarf adressiert. Nicht behebbare Mängel wurden nicht festgestellt. Die Umsetzung wird vom Konzerndatenschutz begleitet. Das Prozessmodell zur internen Beauftragung wird entsprechend weiterentwickelt.

Produktentwicklung.
Im Bereich der Produktentwicklung nehmen wie bei anderen Projekten auch die rechtlichen, technischen und organisatorischen Gestaltungsspielräume im zeitlichen Verlauf eines Projekts ab. Vor diesem Hintergrund ist sowohl aus Sicht des Datenschutzes als auch aus Unternehmenssicht anzustreben, dass die angemessene datenschutzrechtliche Begleitung der Produktentwicklung sichergestellt ist. Dieser Anspruch wird zunehmend über die frühzeitige Einbindung der Datenschutzorganisation im Rahmen der Produktentwicklungsprozesse realisiert.

Die Entwicklung ist ausdrücklich zu begrüßen und soll auch durch den Konzerndatenschutz weiter verstärkt werden. Darüber hinaus profitierte die Begleitung der Produktentwicklung qualitativ von der vorausschauenden Auseinandersetzung mit aufkommenden technologischen Trends, wie z. B. Web 2.0, Tracing- und Trackingtechnologien sowie Fragestellungen zum Datenschutz in serviceorientierten IT-Architekturen.

Kundendaten werden an vielen Stellen und in verschiedenen Formen im Konzern täglich bearbeitet – diese dezentrale Verarbeitung stellt hohe Ansprüche an die Datensicherheit.

Beispiel herausragender Produktentwicklungen, die durch den Konzerndatenschutz begleitet wurden:

Sichere Dienste im Web.
Die Entwicklung bestimmter Services für die Steuerung von Funktionalitäten der Mobilfunk- und Festnetze des Konzerns wurde vorangetrieben. Ziel ist es, über verlässliche und sichere Dienste, die von „jedermann" im Web integriert werden können, universelle Nutzungsmöglichkeiten der Netze zu schaffen. Für den Datenschutz bestand die Herausforderung im Wesentlichen darin, die unterschiedlichen Anforderungen für den Umgang mit personenbezogenen Daten bezogen auf die jeweiligen Dienste zu definieren.

T-Mobile G1.
Bei der datenschutzrechtlichen Begleitung des Mobiltelefons T-Mobile G1 wurde das Ziel verfolgt, eine möglichst klare Trennung zwischen den Diensten von T-Mobile – dem Internet-Access und der Telefonie – und den Google-Diensten herzustellen. Technisch wurde dies insoweit sichergestellt, als dass keine personenbezogenen Daten von T-Mobile an Google übermittelt werden. Somit kann Google beim T-Mobile G1 ausschließlich diejenigen Daten des Kunden erheben, die im Rahmen der Internetnutzung von jedem Internationalen Service Provider erhoben werden können und die der Kunde im Rahmen seines eigenen Vertragsverhältnisses mit Google an Google übergibt. Der Kunde wird bei der Beratung im Verkaufsgespräch sowie über entsprechende Hinweise auf der Produktverpackung darauf hingewiesen, dass er ein gesondertes Vertragsverhältnis mit Google eingehen muss, wenn er ein T-Mobile G1 erwirbt.

Beteiligungsgesellschaften.
2008 wurden zahlreiche vom Konzerndatenschutz betreute Beteiligungsgesellschaften erstmalig in das konzernweite Basisdatenschutzaudit eingebunden. Die zuständigen Ansprechpartner hat der Konzerndatenschutz in die konzernweit gültigen Standards eingewiesen. Der Konzerndatenschutz unterstützte zudem die Schaffung der erforderlichen organisatorischen Rahmenbedingungen und die Durchführung der Maßnahme. Die Auditergebnisse waren die Grundlage für konkrete Maßnahmenpläne und Priorisierungen für das Jahr 2009. Die Umsetzung wird vom Konzerndatenschutz begleitet.

DeTeAssekuranz.
Im Zusammenhang mit der Vertragsgestaltung des internen Versicherungsdienstleisters DeTeAssekuranz mit einem externen Dienstleister wurde wegen Unwägbarkeiten der Dokumentation der bestehenden technisch-organisatorischen Maßnahmen eine Vor-Ort-Kontrolle durchgeführt. Dabei wurden Verbesserungspotentiale identifiziert und kommuniziert. Der Konzerndatenschutz stellte eine Dokumentation der Mindestanforderungen für Produktionsstätten zur Verfügung, die potentiellen Auftragnehmern vorgelegt werden können und die damit die Vertragsgestaltung künftig erleichtert.

Unternehmensverbund SAF – Forderungsmanagement GmbH.
Im Jahr 2008 hat der Konzerndatenschutz sowohl die Prozesse bei der SAF Forderungsmanagement GmbH als auch bei der Accumio Finance Services GmbH, die als Wirtschaftsauskunftei tätig ist, auditiert. Aufgrund von Beschwerden über angebliche Unregelmäßigkeiten lag ein Schwerpunkt der Überprüfungen bei den Prozessen zur Bonitätsprüfung. In diesem Zusammenhang wurden insbesondere die Struktur der Datenspeicherung, die vertraglichen Grundlagen sowie die Berücksichtigung des für die Datenübermittlung notwendigen berechtigten Interesses begutachtet. Auch dem Hinweis auf eine angeblich unterbliebene Benachrichtigung eines Betroffenen durch die Accumio wurde nachgegangen und dabei das gesamte Benachrichtigungsverfahren beleuchtet. Das Audit ergab weder bei der SAF noch bei der Accumio Beanstandungen. Der Konzerndatenschutz hat keinen Prozess und keine Regelung festgestellt, die gegen datenschutzrechtliche Regelungen verstoßen.

Mitarbeiterdatenverarbeitung.

Business Partner Prozessmodell – frühzeitige Einbindung des Konzerndatenschutzes sichergestellt.
Im Berichtszeitraum begleitete der Konzerndatenschutz im Personalbereich u. a. das Projekt Business Partner Modell. Ziel ist die Konzeption, Koordination und Implementierung der Reorganisation des gesamten Personalbereichs. Es sollen übergreifende Prozessdefinitionen eingeführt und die Rolle der Ansprechpartner des Personalbereichs für die operativen Einheiten und Competence-Center neu definiert werden. Die HR-Prozesse zur Beibehaltung der Datenschutzkonformität und die Prozesse des Konzerndatenschutzes wurden entsprechend angepasst. Damit ist für alle Personalkernprozesse eine frühzeitige Beteiligung des Konzerndatenschutzes an allen wesentlichen datenschutzrechtlich relevanten Vorhaben sichergestellt.

Datenschutzfreigabe für das neue konzernweite Identitätsmanagement.
Das konzernweite Identitätsmanagement bildet die Prozesse „Identity Management" und „Account Management" ab. Ziele des neuen Managementsystems:

- ein hohes Niveau an korrekten und aktuellen Identitäts- und Accountdaten,
- ein hohes Niveau an Automatisierung und Normierung,
- leistungsfähige, schnelle Prozesse und Datenflüsse sowie
- ein hohes Niveau an Transparenz und Auditierbarkeit.

Dafür benötigt werden:

- standardisierte Identitäts- und Datenquellen,
- standardisierte leistungsfähige Prozesse während des gesamten Benutzerlebenszyklus,
- standardisierte Prozesse für Account-, Objekt- sowie Privilegien- und Rechtebeantragungen,
- standardisierte Prozesse für Freigaben und
- automatisierte Mechanismen zum Verwalten von Accounts, Objekten und Berechtigungen.

Das Identitätsmanagementsystem stellt damit die Basis für alle konzernweiten identitätsbezogenen Daten und Datenänderungen dar. Des Weiteren dient es als elektronisches Nachschlagewerk zu Bestandsinformationen zu Personen oder Angaben zu Organisationen und Organisationseinheiten. Ferner dient es als Zertifikatsablage und zudem vielen Anwendungen als Authentifizierungsplattform und als Datenbasis für die jeweiligen Applikationen.

Das System wurde datenschutzrechtlich eingehend begutachtet, als datenschutzkonform eingestuft und zum Betrieb freigegeben.

Electronic Business Performance Management der Deutschen Telekom Kundenservice GmbH.

Das Projekt „Electronic Business Performance Management“ hat die Entwicklung einer IT-Lösung zur technischen Unterstützung des Qualitätsmonitorings und Business Performance Managements für alle Call-Center und Dienstleister der Deutschen Telekom Kundenservice zum Gegenstand. Ziel ist die Einführung eines objektiven, automatisierten Verfahrens zur Aufzeichnung von Kundenanrufen und für die Bearbeitung von Kundenanliegen. Die Einführung dieses Systems dient der Erkennung von Verbesserungspotenzialen hinsichtlich der Gesamtprozesse und der Betrachtung der Benutzerfreundlichkeit von verwendeten Systemen. Darüber hinaus werden individuelle Fähigkeiten des Kundenberaters festgestellt, um gezielt Schulungen anbieten zu können.

Grundvoraussetzung zur Gesprächsaufzeichnung ist eine mittels Sprachsteuerung eingeholte Einwilligung des Kunden vor dem eigentlichen Gespräch. Bei allen Gesprächen, für die eine Zustimmung vorliegt, werden zusätzliche Aufzeichnungskriterien geprüft. Trifft ein automatisierter „Recording-Service“ die Entscheidung, das Gespräch zu behalten, wird zeitgleich eine Bildschirmaufzeichnung initiiert. Erfolgt während des Gesprächs eine Rück- oder Nachfrage des Agents beim Teamleiter, pausiert die Audioaufzeichnung für die Dauer des Rückfragegesprächs.

Die Speicherung der Daten im System erfolgt ohne direkt erkennbare Struktur oder Bezifferung, sodass für Dritte kein Anhaltspunkt hinsichtlich natürlicher Personen gegeben ist. Die Daten werden in einem systemeigenen Format gespeichert und lassen sich nicht durch Standardprogramme öffnen. Auf den für die Aufzeichnung notwendigen virtuellen Speicherbereich kann nicht zugegriffen werden. Dies gilt auch für Systemadministratoren, Service-Techniker oder vergleichbare Rollen.

Die Analyse der Aufzeichnungen erfolgt aufgrund strukturierter Bewertungsvorlagen. Diese können vom Agent eingesehen werden. Widerspricht der Agent der Bewertung, erfolgt eine zweite, finale Beurteilung. Basis für ein individuelles Trainingspaket ist der im Rahmen der Bewertung festgestellte Schulungsbedarf. Der Agent erhält ein Bündel von Trainingsmaßnahmen, die innerhalb eines bestimmten Zeitraums durchgeführt werden sollen, um die Kompetenz gezielt zu verbessern.

Diese IT-Lösung ermöglicht durch einen Nebenprozess zusätzlich die Aufzeichnung der Konzerneinwilligungsklausel. Der Nachweis der telefonischen Einwilligung zur Konzerneinwilligungsklausel wird mittels Aufzeichnungen entsprechender Gesprächspassagen durch den Agent erbracht. Dabei wird die Audioaufzeichnung mit Kundennummer archiviert. Hierbei erfolgt die Abfrage der Zustimmung unmittelbar durch den Agenten im Gesprächsverlauf. Die Speicherung dieser speziellen Aufzeichnung erfolgt in einem separaten System.

Das System ist aus datenschutzrechtlicher Sicht komplex, weil es u. a. zu einer weiterreichenden Verhaltens- und Leistungskontrolle der Mitarbeiter führen könnte. Aus Datenschutzsicht wurde darauf geachtet, dass durch eine enge Zweckbindung und kurze Speicherfristen sowie begleitende Mitarbeiterinformationen die Persönlichkeitsrechte der Mitarbeiter gewahrt bleiben. Vor der Einführung des Systems wurde eine Gesamtbetriebsvereinbarung, die im einzelnen Rechte und Pflichten der Beteiligten regelt, vereinbart. Zudem wird eine zusätzliche Praxiskontrolle durch den Konzerndatenschutz stattfinden.

Der Gesamtbetriebsrat der Deutschen Telekom Kundenservice GmbH wurde früh eingebunden. Die Verhandlungen wurden mit dem Abschluss einer Gesamtbetriebsvereinbarung erfolgreich beendet.

Das System wird außerdem der zuständigen Aufsichtsbehörde in Nordrhein-Westfalen vorgestellt.

Fazit und Ausblick 2009.

2008 war ein außerordentliches Jahr für den Datenschutz bei der Deutschen Telekom. Auch wenn der Konzern durch Datenmissbrauch und -diebstahl sowie nicht autorisierte Zugriffe auf Kundendaten negativ in die Schlagzeilen geraten ist, so haben diese Vorfälle doch dazu beigetragen, dass der Datenschutz im Unternehmen heute eine deutlich größere Bedeutung hat. Die Krise eröffnete für die Deutsche Telekom zudem die Chance, beim Thema Datenschutz in Zukunft Standards zu setzen. Und diese Chance wird genutzt.

Kaum ein anderes Unternehmen hat den Datenschutz auf Vorstandsebene verankert. Kaum ein anderes Unternehmen gewährleistet in diesem Maße Transparenz. Kaum ein anderes Unternehmen hat so viele operative und strategische Maßnahmen ergriffen, um den Datenschutz nachhaltig zu stützen.

Auch 2009 geht es vorrangig darum, das Vertrauen der Kunden und der Öffentlichkeit zurückzugewinnen. Die bereits angestoßenen Maßnahmen werden deshalb ohne Einschränkung weitergeführt.

In strategischer Hinsicht ist die Einrichtung des neuen Vorstandsressorts Datenschutz, Recht und Compliance eine konsequente Reaktion auf die Datenschutzvorfälle. Durch die Verankerung des Datenschutzes im neuen Vorstandsressort Datenschutz, Recht und Compliance werden alle Maßnahmen des Konzerndatenschutzes auf höchster Ebene effektiv gebündelt. Dieser Ansatz wird 2009 intensiviert.

In operativer Hinsicht legt der Konzerndatenschutz seine Schwerpunkte 2009 vor allem auf die Erhöhung der Kontrolldichte in datenschutzrelevanten Bereichen sowie auf eine weitere Standardisierung der datenschutzspezifischen Anforderungen an Produkt- und IT-Entwicklungen. Dies wird auch durch die neue Abteilung im Konzerndatenschutz ermöglicht, die sich ausschließlich mit diesen Themen befasst.

Die ersten Monate des Jahres 2009 haben bereits gezeigt, dass der Aspekt des Arbeitnehmerdatenschutzes eine größere Rolle spielen wird. Unternehmen können etwa mit modernen Auswertungsprogrammen und der entsprechenden Buchungssoftware große Datenmengen des internen Rechnungsverkehrs schnell auf mögliche Unregelmäßigkeiten überprüfen.

Das berechtigte Interesse der Unternehmen, Korruption, Betrug und Veruntreuung wirksam zu bekämpfen, darf aber nicht dazu führen, dass Daten von Mitarbeitern wahllos und ins Blaue hinein ausgewertet werden. Die Beschäftigen müssen wissen, wofür Daten ausgewertet werden, wie die Auswertung erfolgen soll und welche Daten betroffen sind. Es reicht nicht, dass Betrug und Untreue mit rechtskonformen Mitteln bekämpft werden. Die Mitarbeiter müssen von der Verhältnismäßigkeit der Mittel überzeugt sein. Dafür wird die Deutsche Telekom die nötigen Voraussetzungen schaffen.

Die neuen Gesetzesinitiativen zum Arbeitnehmerdatenschutz, die derzeit diskutiert werden, werden von der Deutschen Telekom auf dem Weg zu einem transparenten und rechtssicheren Arbeitnehmerdatenschutz unterstützt.

Mit der zunehmenden Nutzung von sozialen Netzwerken rückt der persönliche Datenschutz stärker ins Blickfeld. In sozialen Netzwerken und durch neue Nutzungsformen von Medien im Mobilfunk stellen Privatpersonen im Netz freiwillig immer mehr Daten zur Verfügung, die bei entsprechender Auswertung detaillierte Personenprofile ermöglichen. Für die Bereitstellung dieser Informationen sind die Nutzer zwar primär selbst verantwortlich. Die Deutsche Telekom sieht sich in diesem Bereich jedoch als verantwortungsbewusster Partner für den Kunden. Daher hat es sich der Konzern zum Ziel gesetzt, durch eine offensive Informationspolitik die Medienkompetenz der Nutzer in einem durch die vielfältigen Kommunikationsmedien bestimmten Leben zu stärken. So sollen 2009 insbesondere junge Nutzer mit verschiedenen Maßnahmen für die Gefährdungspotentiale dieser Entwicklung sensibilisiert werden. Ziel ist es, die Medienkompetenz der Nutzer zu stärken, um so zu einem verantwortungsvollen Umgang mit internetbasierten Netzwerken beizutragen. Darüber hinaus will die Deutsche Telekom aber auch konkrete technische und organisatorische Entwicklungen unterstützen. So untersucht der Konzerndatenschutz derzeit gemeinsam mit den Entwicklungsbereichen des Konzerns (Deutsche Telekom Laboratories), wie sich Nutzer in verschiedenen sozialen Netzwerken bewegen können und dabei ihre Reputation (Verlässlichkeit, Solvenz), die sie sich in einzelnen Netzwerken erarbeitet haben, mitnehmen können, ohne dass sie dabei ihre persönlichen Daten preisgeben müssen (anonymous cross community reputation).

Auch andere, neu aufkommende gesellschaftliche und technische Entwicklungen veranlassen den Konzerndatenschutz, sich weiter und intensiver auch auf innovativer Ebene zu engagieren. Diese Entwicklungen bieten weitere Möglichkeiten der Nutzung von personenbezogenen Daten vor allem für Angebote im Bereich des täglichen Lebens. Projekte wie „De-Mail“ als Kommunikationsmittel, das den sicheren Austausch rechtsgültiger elektronischer Dokumente zwischen Bürgern, Behörden und Unternehmen über das Internet ermöglichen soll und „e-Metering“ als Möglichkeit zur optimierten elektronischen Fernauslese von Energiezählern werden Eingang in die Alltagswelt finden und bedürfen der sensiblen datenschutzrechtlichen Beratung, Begleitung und Betreuung.

Sicher wird das Thema Datenschutz im Fokus der Öffentlichkeit bleiben: Die zunehmende Digitalisierung weiterer Bereiche des privaten, beruflichen und gesellschaftlichen Lebens birgt die Gefahren der Manipulation, des Diebstahls und des Missbrauchs persönlicher Daten. Die Deutsche Telekom hat aufgrund ihres Geschäftsmodells eine besondere Verantwortung. Und die Deutsche Telekom ist fest entschlossen, beim Thema Datenschutz eine Vorreiterrolle zu übernehmen.

Bonn, den 25. März 2009

Dr. Claus-Dieter Ulmer

Anhang.

Anhang 1
Organisation des Konzerndatenschutzes.

Der Konzerndatenschutz betreut unter Leitung des Konzerndatenschutzbeauftragten die nationalen Gesellschaften unmittelbar in Fragen des Datenschutzes und wirkt konzernweit auf ein angemessenes Datenschutzniveau in der Deutschen Telekom Gruppe hin. Der Konzerndatenschutzbeauftragte nimmt die gesetzliche Funktion des Datenschutzbeauftragten wahr, bestimmt die strategische Ausrichtung des Konzerns in Fragen des Datenschutzes und vertritt den Konzern in allen Angelegenheiten des Datenschutzes nach innen wie nach außen.

Der Konzerndatenschutz untergliederte sich 2008 in vier Abteilungen. Aufgrund der Datenschutzvorfälle wurde eine weitere Abteilung (Auditierung und technischer Sachverständiger) eingerichtet, die sich derzeit in der Implementierungsphase befindet.

Als Datenschutzansprechpartner vor Ort sind auf Ebene der Legaleinheiten, Betriebe und sonstigen Organisationseinheiten Datenschutzschnittstellen und Datenschutzkoordinatoren installiert. Bei den internationalen Beteiligungen wird diese Funktion von den hierzu benannten „Data Protection Officers“ wahrgenommen. Sowohl die Datenschutzkoordinatoren als auch die Data Protection Officers stehen in ständigem Kontakt mit dem Konzerndatenschutz.

Die Abteilungen im Einzelnen:

1. Grundsatzangelegenheiten.
Die Abteilung Grundsatzangelegenheiten ist verantwortlich für Grundsatzfragen im Datenschutz. Zur Sicherstellung eines rechtskonformen, einheitlichen Handelns werden konzernweit gültige Leitlinien und Policies zum Datenschutz erarbeitet und die Prozesse innerhalb des Konzerndatenschutzes entwickelt. Neben interner und externer Kommunikation im Datenschutz und der Koordinierung der internationalen Datenschutzorganisation im Konzern, zählen die Steuerung fachübergreifender Projekte sowie datenschutzrelevante Entwicklungen zum Aufgabenspektrum des Teams.

2. Kundendatenschutz.
Die Abteilung Kundendatenschutz berät und unterstützt den Konzern und die strategischen Geschäftsfelder des Konzerns in Fragen des Kundendatenschutzes; insbesondere bei der Einführung von Geschäftsmodellen und -prozessen bezüglich der rechtlichen Möglichkeiten und der organisatorischen Anforderungen zur Nutzung von Kundendaten sowie der Sicherstellung der technischen Anforderungen bei der IT-gestützten Verarbeitung von Kundendaten.

3. Mitarbeiter- und Aktionärsdatenschutz.
Die Abteilung Mitarbeiter- und Aktionärsdatenschutz berät und unterstützt den Konzern und die strategischen Geschäftsfelder des Konzerns in Fragen des Personaldatenschutzes und soweit es um personenbezogene Daten Dritter geht, die nicht Telekommunikationskunden sind (z. B. Aktionäre, Lieferanten). Zu den Aufgaben gehören darüber hinaus die Beratung der Betriebsräte des Konzerns, insbesondere des Konzernbetriebsrats in Fragen des Datenschutzes sowie die Vertretung der Konzerngesellschaften gegenüber den Aufsichtsbehörden in Personaldatenschutzfragen auf der operativen Ebene.

4. Produkte und Dienstleistungen.
Die Abteilung Produkte und Dienstleistungen erbringt Datenschutz-Dienstleistungen für ausgewählte Beteiligungsgesellschaften des Konzerns, unterstützt interne Projekte sowie Vertriebsaktivitäten bei Geschäftskundenprojekten und begleitet die datenschutzkonforme Entwicklung von Produkten des Konzerns.

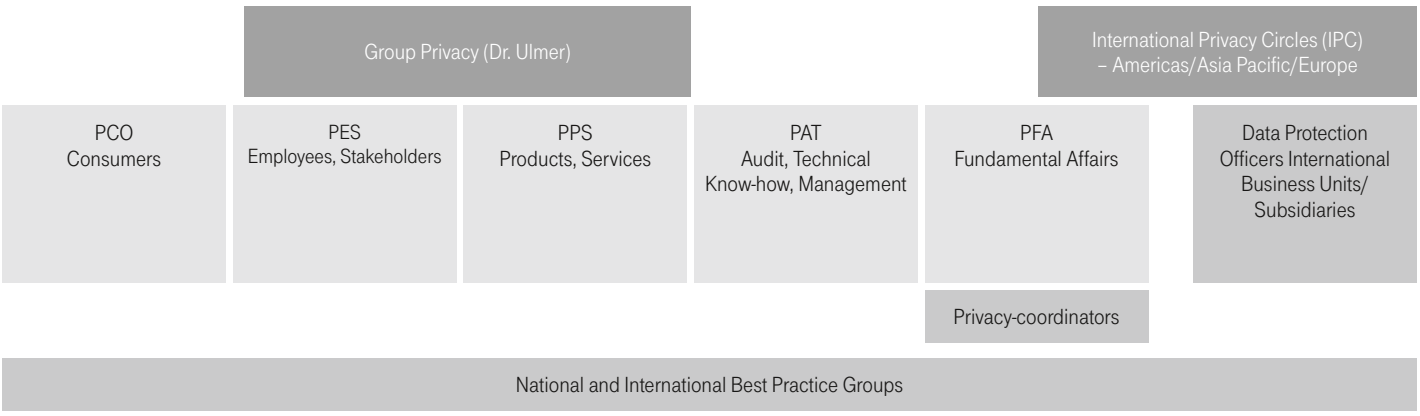
5. Auditierung und technischer Sachverständiger.
Diese Abteilung entwickelt datenschutzspezifische Auditierungsgrundsätze und -prozesse und steuert deren Implementierung im Konzern. Sie führt Audits eigenständig durch bzw. steuert datenschutzrelevante Auditierungen im Konzern. Sie konzipiert Maßnahmenpläne auf Basis der Auditierung und überwacht deren Umsetzung. Zudem ist sie interne Sachverständigen-Instanz für den Datenschutz bei komplexen technischen Fragestellungen. Die Abteilung wird derzeit ausgebaut.

Anhang 2
Rahmenbedingungen unseres Handelns.

Gesetzliche Rahmenbedingungen.
Ausgangspunkt und Regelungsgrundlage aller Aktivitäten des Konzerndatenschutzes sind – als gesetzliche Basisregelung – das Bundesdatenschutzgesetz (BDSG) sowie die einschlägigen bereichsspezifischen Vorschriften im Bereich der Kommunikation. Zu letzteren zählen insbesondere das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG). Auf europäischer Ebene sind das die Richtlinie 95/46/EG des Europäischen Parlaments und des Rats vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie die Richtlinie 2002/58/EC des Europäischen Parlaments und des Rats vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Datenschutzrichtlinie für elektronische Kommunikation, maßgebliche Grundlagen für das Handeln des Konzerns.

Ausgehend von diesen gesetzlichen Vorgaben wurden vom Konzerndatenschutz weitere, auf die speziellen Bedingungen und Arbeitsprozesse der Datenverarbeitung in der Deutschen Telekom zugeschnittene Rahmenregelungen, Richt- und Leitlinien herausgegeben bzw. in die maßgeblichen Prozesse integriert. Wobei in diesem Kapitel ausschließlich auf die übergreifende Rahmenregelung im Konzern eingegangen wird.

Die Datenschutzorganisation.



Konzernübergreifende Rahmenregelung.
Der „Privacy Code of Conduct“, die konzernübergreifende Regelung zum Datenschutz, ist national und international die zentrale Grundlage der Verarbeitung von Kunden- und Mitarbeiterdaten im Konzern Deutsche Telekom.

Auf Grundlage der europarechtlichen Vorgaben und der Vorgaben des Bundesdatenschutzgesetzes führte die Deutsche Telekom bereits im Jahr 2004 den Privacy Code of Conduct als unternehmensinterne Regelung zum Datenschutz im Konzern ein. Der Privacy Code of Conduct regelt die internen Anforderungen an den Umgang mit personenbezogenen Daten weltweit einheitlich. Die weisungsgebundenen Gesellschaften der Deutschen Telekom Gruppe sind durch den zugrundeliegenden Vorstandsbeschluss verpflichtet, die Vorgaben des Privacy Code of Conduct bei sich verbindlich umzusetzen. Den anderen Gesellschaften wird die Einführung und Umsetzung empfohlen. Der Privacy Code of Conduct ist eine gesetzliche Voraussetzung für den internationalen Austausch personenbezogener Daten im Konzern, soweit er die Grenzen der europäischen Union überschreitet. Er enthält die nach europäischem Recht geltenden Anforderungen an den Schutz personenbezogener Daten.

Vom Privacy Code of Conduct leiten sich die weiter konkretisierten, internen Vorgaben, bis hin zum Mitarbeiterhandbuch Datenschutz, ab.

Anhang 3
Privacy Code of Conduct Deutsche Telekom AG.

Leitlinie (Code of Conduct) zum Schutz der Persönlichkeitsrechte im Umgang mit personenbezogenen Daten in der Deutschen Telekom Gruppe

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 länderübergreifenden 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.

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 Deutschen Telekom Gruppe gewährleisten. Sie ersetzen jedoch nicht die notwendige, ggf. gesetzliche Legitimation, die dem jeweiligen Umgang mit personenbezogenen Daten zugrunde 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.

Zweiter Teil
Grundsätze

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, z. B. 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.

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.

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.

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 ggf. 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.

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 personenbezogenen 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.

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).**

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, insbesondere 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.

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 Deutschen 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.

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 Mitgliedsstaat der europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

21130 49202

Deutsche Telekom AG
Friedrich-Ebert-Allee 140
D-53113 Bonn

www.telekom.com