Datenschutzbericht 2009.

Über diesen Bericht.

Im vergangenen Jahr hat die Deutsche Telekom erstmals einen Datenschutzbericht veröffentlicht, in dem sie die Ereignisse und Schwerpunktaktivitäten des Jahres 2008 darstellte. 2010 setzt das Unternehmen seinen Kurs fort, Ereignisse der Vergangenheit aufzuarbeiten und gleichzeitig den Datenschutz operativ weiter zu verbessern. Darüber hinaus stärkt die Deutsche Telekom weiterhin eine Unternehmenskultur, in der die Mitarbeiterinnen und Mitarbeiter die Bedeutung des Datenschutzes erkennen und entsprechend sensibel handeln.

Der Datenschutzbericht 2009 gibt über datenschutzrelevante Ereignisse Auskunft und zeigt auf, wie die Deutsche Telekom das Thema auch 2009 intern und extern konsequent weiterentwickelt hat und wie Datenschutz in Zukunft aussehen könnte.

Der Bericht hat dafür eine neue Struktur erhalten: Im Lagebericht gibt die Deutsche Telekom eine Übersicht über besondere Ereignisse des vergangenen Jahres sowie über Prüfungsprozesse durch staatliche Stellen. Gleichzeitig stellt sie ergriffene Maßnahmen für einen verbesserten Datenschutz vor. In einem weiteren inhaltlichen Schwerpunkt „Datenschutz im Detail“ bezieht der Konzern Stellung zu zentralen Bereichen des Themas und diskutiert aktuelle technische und politische Entwicklungen, die Auswirkungen auf den Datenschutz haben.

Der Datenschutzbericht 2009 sendet ein klares Signal: Die Deutsche Telekom kommuniziert das Thema Datenschutz offen und transparent – und will mit umfangreichen Maßnahmen und Aufklärung der Mitarbeiter, aber auch der Kunden Standards in der Telekommunikationsbranche setzen.

Inhalt.

Geleitwort des Vorstands.

Dr. Manfred Balz

Liebe Leserinnen und Leser,

als die Deutsche Telekom im vergangenen Jahr erstmals ihren Datenschutzbericht der Öffentlichkeit zugänglich machte, befanden wir uns mitten in der Aufarbeitung der Datenschutzvorfälle in unserem Hause, die im Jahr 2008 die öffentliche Diskussion bestimmt hatten. In der Zwischenzeit ist es uns gelungen, viele der identifizierten Schwachstellen zu beseitigen und so neue Vorfälle im Konzern zu verhindern. Dies ermöglichte nicht zuletzt die im vergangenen Jahr erreichte feste Verankerung des Datenschutzes mit den Themen Recht und Compliance im Konzernvorstand. In Zukunft werden die beschleunigte technische Entwicklung und die strategische Neuausrichtung des Konzerns die Anforderungen an den Datenschutz im Unternehmen weiter steigern.

„Der sorgsame Umgang mit personenbezogenen Daten, das darauf aufbauende Vertrauen der Kunden sowie die Transparenz im Umgang mit den Daten stehen für die Deutsche Telekom an oberster Stelle.“

Auch in Zukunft steht die Gesellschaft vor weiteren Herausforderungen: Die permanente Verfügbarkeit entscheidender Daten wird für die Nutzer immer wichtiger. Gleichzeitig wächst aber auch die Erfordernis, diese Daten so sicher wie möglich zu machen: Immer und überall verfügbare Daten müssen auch immer und überall geschützt werden. Hierbei unterstützt die Deutsche Telekom ihre Kundinnen und Kunden und entwickelt sich zum Vorreiter in Sachen Datenschutz.

Der sorgsame Umgang mit personenbezogenen Daten, das darauf aufbauende Vertrauen der Kunden sowie die Transparenz in unserem Umgang mit den Daten stehen dabei für uns an oberster Stelle. Daher stellen wir uns dem kritischen Blick von außen, etwa durch unabhängige Zertifizierungen und unseren externen Datenschutzbeirat. Auch Sie, liebe Leserinnen und Leser, möchte ich auffordern, sich selbst ein Bild über den Datenschutz bei der Deutschen Telekom zu machen. Der vorliegende Bericht soll Sie dabei unterstützen.

Ich wünsche Ihnen eine interessante Lektüre.

Ihr

Dr. Manfred Balz
Vorstand Datenschutz, Recht und Compliance

Interview mit dem Datenschutzbeauftragten.

Herr Ulmer, ist das Bewusstsein für Datenschutz bei der Deutschen Telekom seit dem Bekanntwerden der Datenvorfälle im Jahr 2008 größer geworden?

Definitiv ist das Datenschutzbewusstsein seit 2008 größer geworden. Die Datenvorfälle waren unverzeihliche Einzelfälle. Das damit einhergehende intensive Medienecho hat einen regelrechten Schock im Konzern ausgelöst. Die einzig richtige Konsequenz und Antwort darauf war, die Themen offensiv und transparent anzugehen. Die Vielzahl der ergriffenen und umfangreich kommunizierten Maßnahmen ist der deutlichste Beweis dafür, dass sich die Sensibilität für Datenschutz erhöht hat. Das stärkere Datenschutzbewusstsein zeigt sich aber nicht nur an den Reaktionen im Top-Management. Wir haben seit vergangenem Jahr mehr als doppelt so viele Beratungs- und Betreuungsanfragen für Projekte, Systeme und Geschäftsmodelle erhalten. Die Anzahl der Hinweise oder Anfragen von Mitarbeitern ist in ähnlichem Umfang gestiegen. Dies bedeutet, dass das Thema durch die gesamte Organisation hindurch angekommen ist.

Das Vertrauen der Kunden und der Öffentlichkeit war 2008 auf einem Tiefpunkt angelangt. Glauben Sie, dass Sie im vergangenen Jahr das Vertrauen zurückgewinnen konnten?

Ich bin mir zumindest sicher, dass wir wieder einen erheblichen Teil wettgemacht haben. Bereits vor den Datenvorfällen hatten wir eine Vielzahl von Regelungen und Strukturen, die den vertrauensvollen Umgang mit den Daten unserer Kunden gewährleisten sollten. Es ist immer schwierig, Missbräuche zu verhindern oder aufzudecken, die mit hoher krimineller Energie begangen werden. Auch war sicherlich das Verständnis für Datenschutzbelange nicht an allen Stellen so ausgeprägt, wie es hätte sein sollen. Auch heute läuft noch nicht alles perfekt. Wichtig für unsere Kunden ist aber, dass sie sehen, dass es uns ernst ist. Es hat zweifellos ein kultureller Wandel stattgefunden.

Mit welcher Datenschutzthematik haben Sie sich 2009 am meisten beschäftigt?

Da gab es Themen aus unterschiedlichen Bereichen. Im Vordergrund stand die weitere Aufarbeitung der Datenvorfälle. Wir haben aber auch intensiv Projekte begleitet, die auf die Zusammenführung des deutschen Konzernteils in einer Gesellschaft, der Telekom Deutschland GmbH, hingearbeitet haben. Viel haben wir im Bereich Auditierung getan: Vor allem haben wir den Aufbau unserer neuen Auditabteilung geleistet, ein neues Auditkonzept erstellt und die eigentlichen Auditierungen begleitet. Im internationalen Bereich haben wir die Fäden wieder intensiver aufgegriffen und die Koordinierungsfunktion stärker als in den Vorjahren wahrgenommen.

Was hätte Ihrer Meinung nach 2009 auf dem Gebiet des Datenschutzes bei der Deutschen Telekom besser laufen können?

Wir haben viele Maßnahmen angestoßen und viel unternommen. Vor diesem Hintergrund kann ich sagen, dass ich – trotz des zweifellos noch bestehenden Handlungsbedarfs – sehr zufrieden mit dem Verlauf des Jahres 2009 bin. Leider waren wir als Datenschutzorganisation im vergangenen Jahr wegen der hohen operativen Belastung für die Mitarbeiter nicht immer leicht erreichbar. Diesen Aspekt nehme ich aber in diesem Jahr auf, indem ich etwa plane, stärker an den einzelnen Standorten präsent zu sein.

Im Datenschutzbericht 2008 haben Sie angekündigt, eine Vorreiterrolle auf dem Gebiet des Datenschutzes übernehmen zu wollen. Ist Ihnen dies gelungen?

Der Konzern möchte in der Tat eine Vorreiterrolle im Datenschutz übernehmen. Das ist auch eine Managementaufgabe und ich begrüße das sehr. Ich meine auch, dass wir auf dem richtigen Weg sind. Die Transparenz und Konsequenz, mit der wir die Themen angehen, sind mir sonst von nirgends bekannt. Auch die Selbstkritik, mit der wir uns betrachten, habe ich in der Vergangenheit bei anderen Unternehmen eher selten beobachten können. Im operativen Bereich haben wir zudem eine Vielzahl von Maßnahmen und Prüfungen durchgeführt, die beispielhaft sind. Wir haben das gehalten, was wir auch versprochen haben. Was wir tun, sind die unseres Erachtens notwendigen Maßnahmen, um unseren Kunden ein möglichst hohes Datenschutzniveau zu bieten.

Wenn Sie einen Wunsch an die Mitarbeiter der Deutschen Telekom äußern könnten: Welcher wäre das?

Unser zentrales Geschäftsmodell ist der Umgang mit den personenbezogenen Daten unserer Kunden. Bitte denken Sie immer daran, dass jede Handlung, die Sie vornehmen, datenschutzrelevant sein kann.

Wenn Sie einen Wunsch an die Politik äußern könnten: Welcher wäre das?

Wichtig wäre es, bei den jetzt anstehenden Überarbeitungen verschiedener Datenschutzgesetze Regelungen zu schaffen, die unzweideutig auszulegen sind und für Rechtssicherheit bei allen Beteiligten sorgen. Ich kann auch nur dringend empfehlen, die Erfahrungen und Anregungen von ein paar gestandenen Datenschutzbeauftragten in die Überlegungen der Politiker einfließen zu lassen. Niemand kennt das Geschäft und seine Unwägbarkeiten besser als die Experten.

Die Deutsche Telekom verfügt über einen Datenschutzvorstand und Sie als Konzerndatenschutzbeauftragten. Worin liegt eigentlich der Unterschied zwischen Ihren Tätigkeiten?

Der Datenschutzbeauftragte ist nach den gesetzlichen Vorschriften eine unabhängige und weisungsfreie Kontroll- und Beratungsinstanz für das Unternehmen. Er darf deshalb schon per definitionem nicht der Geschäftsleitung oder dem Vorstand eines Unternehmens angehören. Die Verantwortung insbesondere für die Geschäftsentwicklung des Unternehmens könnte zu einem Interessenkonflikt mit der gesetzlichen Aufsichtsfunktion des Datenschutzbeauftragten führen. Die Deutsche Telekom hat nun als erstes Unternehmen eine entsprechende Top-Managementfunktion geschaffen. Als originärer Teil des Konzernvorstands kann der Vorstand Datenschutz, Recht und Compliance schon bei den ersten strategischen Erörterungen auf die Datenschutzbelange hinweisen. Zudem bringt er durch sein an die Organstellung gebundenes Weisungsrecht gegenüber Management und Mitarbeitern ein höheres „Kampfgewicht“ mit in den Ring. Insofern spielen die zwei Funktionen sehr gut zusammen. Natürlich hat der Vorstand Datenschutz, Recht und Compliance daneben noch eine Anzahl weiterer wichtiger Aufgaben, die über den reinen Datenschutz hinausgehen. Insbesondere Recht und Compliance sind ja keine Nebenschauplätze, sondern von mindestens ebenso großer Bedeutung für den Konzern wie der Datenschutz. Auch hier ist es meines Erachtens wichtig, dass diese Querschnittsthemen einen direkten und auch nur diesen Themen verantwortlichen Vertreter im Konzernvorstand haben.

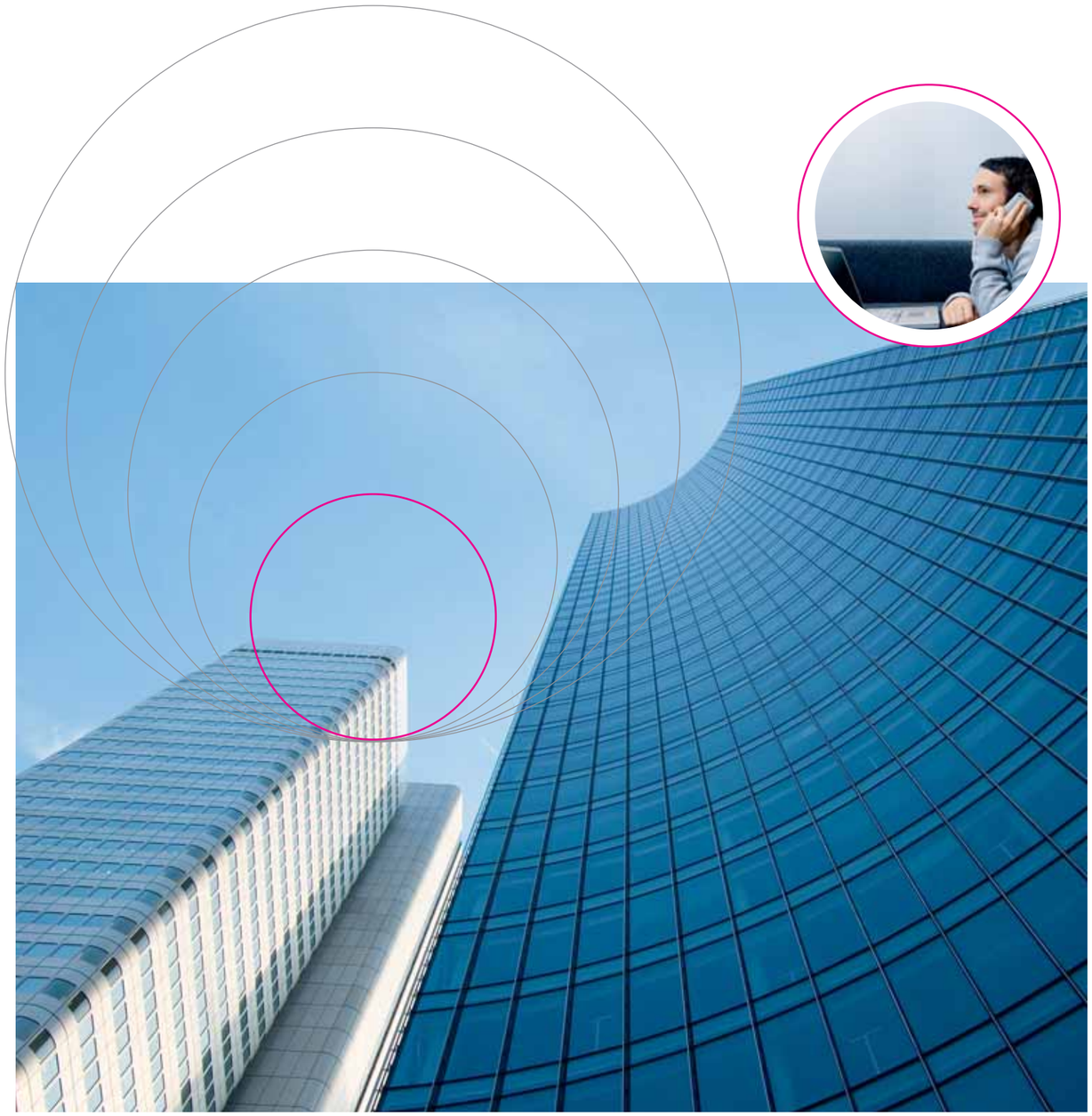
Dr. Claus Dieter Ulmer

Was ist zwingend notwendig für einen erfolgreichen Datenschutz im Unternehmen?

Wir dürfen bei alledem – und das liegt mir wirklich am Herzen – nicht vergessen, dass die Deutsche Telekom allein in Deutschland mehr als 130 000 und weltweit rund 260 000 Mitarbeiter hat. Wie ich aus den vielfältigen Reaktionen der vergangenen zwei Jahre weiß, war und ist das Thema Datenschutz für die überwiegende Mehrzahl von ihnen ein wichtiges Anliegen. Das zieht sich vom Top-Manager bis zu den Kollegen im Call-Center. Hätten wir diese Basis nicht, hätten wir darauf bei der Abarbeitung der Datenvorfälle auch nicht in dem Maße aufbauen können, wie wir es unbedingt gebraucht haben. Deshalb gilt ihnen an dieser Stelle mein besonderer Dank. Ich hoffe, wir können auch die Zukunft auf dieser Basis gemeinsam erfolgreich gestalten.

Ihr

Dr. Claus Dieter Ulmer
Konzerndatenschutzbeauftragter Deutsche Telekom AG



Wo Datenströme fließen, sind persönliche Daten im Spiel. Ihr Schutz ist für die Deutsche Telekom entscheidend. Deshalb bauen wir unsere Bemühungen im Datenschutz kontinuierlich aus und wollen Standards setzen. Daran lassen wir uns messen.

Lagebericht.

Überblick: 2009 – Ein Jahr im Wandel.

2009 war ein Jahr des Wandels für den Datenschutz, nach dem außerordentlichen Jahr 2008. Die Telekom bewältigt weiterhin unterschiedlichste Aufgaben parallel. Neben der raschen und umfassenden Aufklärung der bekannten Vorfälle hat das Unternehmen neue Strukturen geschaffen und zahlreiche Maßnahmen hinsichtlich des technischen und organisatorischen Datenschutzes umgesetzt. 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 weiter nachhaltig stärken wird.

Alle Anstrengungen im Bereich Datenschutz und Datensicherheit stehen und fallen mit der Unterstützung des Managements und der Mitarbeiter: Im Zentrum des Datenverarbeitungsprozesses steht der Mensch, der Daten verarbeitet und für den Schutz dieser Daten sensibilisiert werden muss. Daher wird der eingesetzte Prozess des kulturellen Wandels weiter fortgesetzt, der jedem Mitarbeiter bewusst macht, dass er für den Umgang der ihm zur Kenntnis gelangten Daten verantwortlich ist.

Maßnahmen zur Verbesserung des Datenschutzes: Das 10-Punkte-Sofortmaßnahmenprogramm.

Im Oktober 2008 hat die Deutsche Telekom den neuen Vorstandsbereich Datenschutz, Recht und Compliance geschaffen. Das neue Vorstandsressort hat u. a. die Aufgabe, die im Konzern notwendigen Maßnahmen zum Datenschutz und zur Datensicherheit zentral abzustimmen, ihre Umsetzung anzustoßen und zu überwachen.

Der verantwortliche Vorstand, Dr. Manfred Balz, stellte im März 2009 ein 10-Punkte-Sofortmaßnahmenprogramm vor. In dessen Zentrum stehen zum einen Maßnahmen zum internen Datenschutz, zum anderen Maßnahmen, die den Schutz von Daten vor Diebstahl und Missbrauch gewährleisten sollen. Die Punkte im Einzelnen:

1. Verstärkter Schutz der Aufsichtsräte.
Die Aufsichtsräte werden durch ein neues „Konsultationsverfahren“ stärker vor unberechtigten internen Ermittlungen geschützt. Das heißt: Zusätzlich zu den regelmäßig stattfindenden Rechtmäßigkeitsprüfungen muss der Vorstand das zuständige Aufsichtsratsgremium konsultieren, bevor er interne Ermittlungen einleitet.

2. Schutz der Betriebsräte.
Zum Schutz der Betriebsräte hat die Deutsche Telekom einen ähnlichen Freigabeprozess wie für die Aufsichtsräte etabliert. Hier muss vor Beginn interner Ermittlungen der jeweilige Vorsitzende des Betriebsrats informiert werden. Ähnliches gilt für die Mitglieder der Sprecherausschüsse, die die leitenden Angestellten vertreten.

3. Schutz von Medienvertretern.
Interne Ermittlungen gegen Medienvertreter sind grundsätzlich ausgeschlossen. Weil aber auch Journalisten – unabhängig von ihrer Berufsausübung – Delikte begehen können, ist ein absolutes Verbot von internen Ermittlungen gegen Medienvertreter nicht möglich. In einem konkreten Verdachtsfall müssen die Ermittlungen jedoch einvernehmlich durch den Vorstand Datenschutz, Recht und Compliance, Dr. Manfred Balz, und den Leiter der Unternehmenskommunikation, Philipp Schindera, freigegeben werden.

4. Gegenzeichnung des Vorstands Datenschutz, Recht und Compliance bei Beauftragung von externen Ermittlungsdienstleistungen.
Sollte in Einzelfällen die Beauftragung externer Ermittlungsdienstleistungen notwendig sein, erfolgt eine solche Beauftragung ausschließlich nach Prüfung und Gegenzeichnung durch den Vorstandsbereich Datenschutz, Recht und Compliance. Hierbei gilt das Vier-Augen-Prinzip, das prozessual in den Einkaufs-, Bestellungs- und Abrechnungssystemen der Deutschen Telekom verankert ist.

5. Schutz von Verkehrsdaten.
Das Telekommunikationsgesetz fordert die Wahrung des Fernmeldegeheimnisses. In strengen Ausnahmefällen erlaubt das Gesetz bei Anhaltspunkten auf Missbrauch, entsprechende Verkehrsdaten auszuwerten, um rechtswidrige Nutzungen des Telekommunikationsnetzes aufzudecken oder zu unterbinden. Bei der Deutschen Telekom wird sichergestellt, dass jeder Datenzugriff auf Verkehrsdaten in höchstmöglichem Maße gesetzes- und regelkonform erfolgt, streng kontrolliert wird und nachverfolgbar ist. Die für einen möglichen Datenzugriff auf Verkehrsdaten zuständigen Mitarbeiter wurden in Schulungen intensiv eingewiesen.

6. Einführung von Datenschutzpaten.
Jeweils ein technischer und ein rechtlicher Datenschutzexperte haben die Patenschaft für zentrale IT-Systeme bei der Deutschen Telekom übernommen. Zu den Aufgaben der sog. Datenschutzpaten zählen – ergänzend zu den regulären Beratungs- und Kontrollprozessen des Konzerndatenschutzes – unangekündigte Überprüfungen der IT-Systeme. Außerdem stehen sie den einzelnen Abteilungen als individuelle Ansprechpartner für Datenschutzfragen zur Verfügung.

7. Erhöhung der Kontrolldichte.
Beim Konzerndatenschutzbeauftragten Dr. Claus Dieter Ulmer wurde ein neuer, technisch ausgerichteter Fachbereich etabliert, der sich auf Kontrollen von Prozessen, IT-Systemen und Organisationseinheiten konzentriert und damit die vorhandene Konzerninfrastruktur um entsprechende Schutz- und Sicherheitsstandards erweitert. Der bereits bestehende mehrstufige Kontrollprozess wird damit um ein wichtiges Modul ergänzt.

8. Freigabe und laufende Begleitung von IT-Systemen.
Bei der datenschutzrechtlichen Freigabe von IT-Entwicklungen hat die Telekom einen verschärften Prozess etabliert. Die neu implementierte Beteiligungsrichtlinie konkretisiert die Anforderungen aus dem im Konzern Deutsche Telekom geltenden Privacy Code of Conduct (Schutz der Persönlichkeitsrechte im Umgang mit personenbezogenen Daten) und regelt die Prozesse einer frühzeitigen Beteiligung des Konzerndatenschutzes hinsichtlich einer datenschutzgerechten Entwicklung und eines datenschutzgerechten Betriebs von IT-Systemen, Prozessen und Geschäftsmodellen.

9. Implementierung von Datenschutz-Brückenköpfen.
In der Geschäftsleitungsebene sowie den IT-Abteilungen der strategischen Geschäftsfelder der Deutschen Telekom sind Ansprechpartner für das Thema Datenschutz benannt worden, die die Kommunikation mit dem Vorstandsbereich Datenschutz, Recht und Compliance, die Umsetzung der datenschutzrechtlichen Anforderungen sowie datenschutzgerechte Prozessabläufe sicherstellen.

10. Gründung des Datenschutzbeirats.
Im Februar 2009 gründete die Telekom einen Datenschutzbeirat als erstes Gremium seiner Art in Deutschland. Dieser berät den Vorstand der Deutschen Telekom in datenschutzrelevanten Themen. Zu seinen Mitgliedern zählen führende Datenschutzexperten und Persönlichkeiten aus Politik, Lehre, Wirtschaft und unabhängigen Organisationen. Diese wollen dazu beitragen, vorbildliche Datenschutzstandards im Unternehmen zu verwirklichen und Impulse für den gesamten Markt zu geben.

Umsetzung neuer gesetzlicher Regelungen.

Im September 2009 ist die Novelle des Bundesdatenschutzgesetzes in Kraft getreten. Viele Regelungsinhalte betreffen auch die Deutsche Telekom. Der Konzerndatenschutz hat die Neuregelung durch ein konzernweites Projekt eingeführt und mit umfangreichen Informations- und Kommunikationsmaßnahmen begleitet. Wesentliche Themen für die Deutsche Telekom sind:

Konkretisierung der Regelungen zur Auftragsdatenverarbeitung.
Die Legislative hat die Regelungen zur Auftragsdatenverarbeitung konkretisiert. Gesetzlich ist jetzt genauer festgelegt, was vertraglich vereinbart sein muss, etwa was der Gegenstand und die Dauer des Auftrags sind. Darüber hinaus sind Angaben zu Umfang, Art und Zweck der vorgesehenen Erhebung, zur Verarbeitung und Nutzung sowie zu Art und Umfang der Daten zwingend. Der Auftraggeber ist verpflichtet, sich vor Beginn und während der Datenverarbeitung von der Einhaltung der Regelungen zu überzeugen und das Ergebnis zu dokumentieren.

Die bei der Deutschen Telekom schon vor der Novellierung eingeführten detaillierten Auftragsdatenverarbeitungsmuster entsprachen im Wesentlichen schon den strengen Anforderungen der Neuregelung und mussten daher nur geringfügig angepasst werden. Der Konzerndatenschutz hat die Neuregelung jedoch zum Anlass genommen, die Handhabbarkeit der zur Verfügung gestellten Formularverträge durch Erläuterungen zu vereinfachen.

Anforderungen an eine Einwilligung.
Einwilligungen von Kunden, mit denen bestimmte Datenverarbeitungen erlaubt werden, bedurften bislang grundsätzlich der Schriftform. Im Falle einer mündlich oder elektronisch erteilten Einwilligung war daher eine schriftliche Bestätigung des Unternehmens erforderlich. Nach den Neuregelungen kann ausnahmsweise von einer schriftlichen Bestätigung abgesehen werden, wenn die Einwilligung elektronisch protokolliert wird, der Betroffene den Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

Die elektronische Protokollierung einer Einwilligung war in der Telekommunikations- und Telemedienbranche auch schon vor der Novellierung des Bundesdatenschutzgesetzes zwingend. Insofern begrüßt die Deutsche Telekom die allgemeine Einführung im Sinne eines einheitlich hohen Datenschutzniveaus in Deutschland.

Adresshandel und Werbung –
OptIn-Grundsatz und Kennzeichnungspflicht.
Die Verwendung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist seit der Novellierung des Bundesdatenschutzgesetzes grundsätzlich nur dann zulässig, wenn der Betroffene ausdrücklich eingewilligt hat (OptIn-Grundsatz). Voreingestellte Häkchen in Einwilligungsfeldern oder Streichlösungen sind nun unzulässig.

Bereits im Jahr 2007 hat sich die Deutsche Telekom mit dem „Leitfaden für verbraucherfreundliche digitale Produkte und Dienstleistungen“ selbst zur Einführung des OptIn-Verfahrens über die gesetzlichen Regelungen hinaus verpflichtet und dies als zusätzliches Qualitätskriterium für verbraucherfreundliche digitale Produkte und Dienstleistungen definiert und empfohlen.

Dr. Manfred Balz (Mitte) bei der Übergabe eines Zertifikats.

Die Deutsche Telekom hat ihre Aktivitäten rund um Zertifizierungen und Auditierungen wesentlich ausgeweitet.

Informationspflicht bei Datenpannen.
Betroffene müssen darüber informiert werden, wenn Dritte unrechtmäßig Kenntnis ihrer Daten erlangen und schwerwiegende Beeinträchtigungen ihrer Rechte oder schutzwürdigen Interessen drohen. Neben den Betroffenen ist auch der Bundesbeauftragte für Datenschutz und die Informationsfreiheit zwingend zu informieren.

Die Deutsche Telekom geht über diese Anforderungen hinaus, indem sie als erstes Telekommunikationsunternehmen in Deutschland auf einer speziellen Internetseite (www.telekom.com/datenschutz) und in ihrem öffentlichen Datenschutzbericht über aktuelle und kritische Datenschutzvorgänge berichtet.

Arbeitnehmerdatenschutz.
Das Bundesdatenschutzgesetz legt fest, welche Daten für die Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden dürfen. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur unter bestimmten Voraussetzungen verwendet werden. Da diese Regelung im juristischen Umfeld unterschiedlich ausgelegt wird, hat sich die Deutsche Telekom für eine sehr enge Auslegungsvariante entschieden, die die Datenschutzkonformität bis zum Vorliegen einer eindeutigen gesetzlichen Regelung oder einer klaren gerichtlichen Entscheidung gewährleistet.

Prüfungen durch staatliche Stellen.

Der Konzerndatenschutz der Deutschen Telekom führt mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie der Bundesnetzagentur kontinuierlich Gespräche zu aktuellen Fragen des Datenschutzes sowie den im Unternehmen ergriffenen Maßnahmen. Durch die frühzeitige Einbindung der Aufsichtsbehörden in kritische Datenschutzthemen wird die Transparenz gegenüber den Aufsichtsbehörden erhöht und rechtzeitig auf gesetzeskonformes Handeln hingewirkt.

Im Jahr 2009 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit vier Beratungs- und Kontrollbesuche durchgeführt. Zwei dieser Besuche betrafen die Vorratsdatenspeicherung bei T-Home und T-Mobile. Darüber hinaus führte der Bundesdatenschutzbeauftragte im Mai 2009 einen dreitägigen Kontrollbesuch bei T-Mobile Deutschland durch. Schwerpunkte waren die Überprüfung der Verarbeitung von Verkehrsdaten im Rahmen des Abrechnungsprozesses sowie die Überprüfung eines Systems zur Erkennung von Missbrauch. Im August 2009 besuchte der Bundesbeauftragte ein externes Call-Center für den Kundenservice. Dabei untersuchte er schwerpunktmäßig die Einführung und Umsetzung der technischen und organisatorischen Anforderungen zur Auftragsdatenverarbeitung aus der Novellierung des Bundesdatenschutzgesetzes.

Zertifizierungen und Auditierungen.
Die Deutsche Telekom hat ihre Aktivitäten rund um Zertifizierungen und Auditierungen im Jahre 2009 wesentlich ausgeweitet. Als eine der Sofortmaßnahmen des neuen Vorstandbereichs Datenschutz, Recht und Compliance wurde im Verantwortungsbereich des Konzerndatenschutzbeauftragten Dr. Claus Dieter Ulmer ein neuer Fachbereich zur Verstärkung der Auditierungstätigkeiten im Datenschutz eingerichtet. Insgesamt wurden im Jahr 2009 über 450 interne Audits und mehrere hundert externe Audits zu den Themen Datenschutz und Datensicherheit durchgeführt. Die Deutsche Telekom stützt sich bei der Sicherstellung eines hohen Datenschutz- und Datensicherheitsniveaus damit sowohl auf interne als auch auf externe Fachkompetenz.

Zertifizierung durch den TÜV.
Der TÜV Informationstechnik (TÜViT), ein Unternehmen der TÜV NORD Gruppe, hat den Rechnungsprozess für Privatkunden im Festnetz auditiert und zertifiziert. Im Rahmen des Rechnungsprozesses werden sämtliche Verkehrsdaten verarbeitet und bepreist, die tagtäglich durch etwa 30 Millionen Kunden beim Telefonieren und der Nutzung von Internet und E-Mail erzeugt werden. Es handelt sich hierbei um eine sehr sensible und vor allem umfassende Datenverarbeitung der Deutschen Telekom.

Daneben prüfte und zertifizierte der TÜV Rheinland drei verschiedene Kundenportale im Vertriebsbereich. Diese Portale sind datenverarbeitende Anwendungen, die im täglichen Kundenkontakt eingesetzt werden und den Kundenbetreuern den Zugriff auf die dahinter liegenden Kundendatenbanken geben. Der TÜV Rheinland begutachtete die Abläufe, Sicherheitsmaßnahmen und Zugriffsmöglichkeiten auf Daten über diese Systeme. Außerdem kontrollierten die TÜV-Fachleute, wie die Kundenberater mit den Portalen umgehen. Sie besuchten Telekom Shops, Service Center und Vertriebspartner und sprachen dort mit den Mitarbeitern. Auch die der Datenverarbeitung durch Vertriebspartner zugrunde liegenden vertraglichen Vereinbarungen wurden vom TÜV Rheinland geprüft und zertifiziert.

Zertifizierung durch die DEKRA.
Die neutrale Prüforganisation DEKRA hat den Shops der Deutschen Telekom ihr Siegel „Datenschutz und Datensicherheit“ verliehen. Die Prüfung umfasste im Wesentlichen zwei Bereiche: Zum einen überprüften die DEKRA-Experten die räumliche Sicherheit, zum anderen untersuchten sie den Umgang mit Kundendaten. Alle geprüften mehrere hundert Shops erhielten das Datenschutzsiegel.

Interne Auditierungen.
Interne Überprüfungen sind wichtig, um die Umsetzung und Einhaltung von Vorgaben zu Datenschutz und Datensicherheit zu überprüfen. Das interne Auditkonzept der Deutschen Telekom stützt sich auf drei Säulen, die an späterer Stelle des Berichts detailliert erläutert werden.

Besondere Ereignisse im Jahr 2009.

Unautorisierte Zusammenarbeit mit Subpartnern.
Ende Mai 2009 erhielt die Deutsche Telekom von mehreren externen Hinweisgebern die Information, dass Call-Center, die nicht durch den Konzern autorisiert sind, Aufträge für T-Home generiert hatten. In diesem Zusammenhang wandte sich auch ein Call-Center-Betreiber aus der Türkei an die Deutsche Telekom, der behauptete, für verschiedene Vertriebspartner der Deutschen Telekom tätig gewesen zu sein. Jedoch habe er von diesen keine Prämienzahlungen erhalten.

Die Analyse der zur Verfügung gestellten Auftragsdaten bestätigte den Verdacht, dass Subpartner mit nicht autorisierten Call-Centern in der Türkei zusammengearbeitet hatten. Die internen Ermittlungen ergaben, dass die Aufträge über verschiedene Vertriebspartner und Vertriebskanäle erfolgten. Dadurch wurden bewusst die Schwellenwerte zur Missbrauchserkennung umgangen. In der Folge hat die Deutsche Telekom Strafanzeige erstattet.

Die Deutsche Telekom sprach Abmahnungen gegen drei Hauptvertriebspartner aus und verhängte Vertragsstrafen. Außerdem erhob sie Prämienrückforderungen. Die Vertriebspartner versicherten, von den illegalen Vorgängen nichts gewusst zu haben und kooperierten bei der Aufklärung der Vorgänge. Einem weiteren Vertriebspartner wurde gekündigt. Darüber hinaus wurden sämtliche Vertriebspartner nachdrücklich an die Genehmigungspflicht für Subpartner erinnert und darauf hingewiesen, dass die Deutsche Telekom bestimmte, namentlich genannte Vermarkter nicht als Subpartner akzeptiert.

Open Book.
Nach der Strafanzeige des Konzerns im Mai 2008 wegen der sog. Bespitzelungsaffäre hatte die Staatsanwaltschaft Ende Mai 2008 unter voller Kooperation des Unternehmens Dokumente aus dem Archiv der Konzernsicherheit und aus Büroräumen von Mitarbeitern sichergestellt. Im Juli 2009 hat die Staatsanwaltschaft der Deutschen Telekom denjenigen Teil der Dokumente zur Einsichtnahme zur Verfügung gestellt, bei dem sie keinen Zusammenhang zu dem Ermittlungsverfahren und keine Anhaltspunkte für verfolgbare strafbare Handlungen sah.

Anders als die Ermittlungen der Strafverfolgungsbehörden, die auf verfolgbare und noch unverjährte strafbare Handlungen gerichtet waren, wurden die Dokumente bei der internen Untersuchung auf sonstige Compliance-Verstöße hin gesichtet. Hierzu zählten – unabhängig von einer möglicherweise bereits eingetretenen Verjährung – weitere strafbare oder ordnungswidrige Handlungen, etwa Verstöße gegen Rechtsvorschriften des Datenschutzes oder des Telekommunikationsgesetzes, aber auch Vorgänge, bei denen das Handeln der Unternehmenssicherheit zwar nicht als rechtswidrig, aber jedenfalls als ethisch bedenklich anzusehen ist. Beispielsweise wurden in rechtlich unzulässiger Weise Informationen über Einkommens- und Vermögensverhältnisse und andere personenbezogene Informationen aus nicht öffentlich zugänglichen Quellen im In- und Ausland beschafft. Bedenklich sind für die Deutsche Telekom auch die Fälle, in denen aus geringfügigem Anlass unverhältnismäßig intensive Observationen stattgefunden haben oder – wenn auch aus öffentlich zugänglichen Quellen – unangemessen umfangreiche Informationen zu Personen zusammengestellt wurden. Die Konzernsicherheit hat in den festgestellten Fällen vielfach mit externen Sicherheitsdienstleistern zusammengearbeitet, deren Beauftragung durch den Vorstand Datenschutz, Recht und Compliance, Dr. Manfred Balz, seit längerem untersagt ist. Die im Projekt aufgedeckten, kritischen Sachverhalte hinterlegte die Deutsche Telekom mit entsprechenden Maßnahmen zur Aufarbeitung. Dazu gehörten nicht nur die Information der Betroffenen, sondern auch angemessene Maßnahmen gegen die handelnden Personen.

Datenschutzvorfall bei T-Mobile UK.
Im November 2009 machte der englische Datenschutzbeauftragte einen Datenschutzvorfall öffentlich, der sich bei der T-Mobile UK im Jahr 2008 zugetragen hatte. Ein Mitarbeiter hatte Kundendaten und Informationen zu Vertragserneuerungen ohne Wissen des Unternehmens an Dritte weitergegeben. Die Daten wurden offenbar von Zwischenhändlern gekauft und an andere Telefongesellschaften weiterverkauft. T-Mobile UK hatte die zuständige Aufsichtsbehörde nach interner Aufdeckung des Sachverhalts im Jahr 2007 unmittelbar informiert und um Unterstützung gebeten. Mit Hilfe der T-Mobile UK führte die Behörde ihre Ermittlungen durch. Auf Bitten der Aufsichtsbehörde wurde die Öffentlichkeit zunächst nicht über diesen Fall informiert. Die Ermittlungen führten zu dem Ergebnis, dass ein Mitarbeiter der T-Mobile UK im Rahmen seiner Kompetenzen missbräuchlich auf Daten zugegriffen hat. Der betreffende Mitarbeiter hat das Unternehmen mittlerweile verlassen.

Behauptete Sicherheitslücke bei T-Mobile USA.
Ein Blogger hatte behauptet, Server der T-Mobile USA gehackt zu haben. Der Vorwurf wurde inzwischen eingehend untersucht. Es konnten jedoch keinerlei Hinweise gefunden werden, dass Hacker Zugriff auf Kunden- oder Firmeninformationen gehabt hätten. Die angeblich betroffenen Systeme werden aufgrund der Behauptung nun stärker überwacht.

Sonstiges: Anfragen zum Datenschutz.

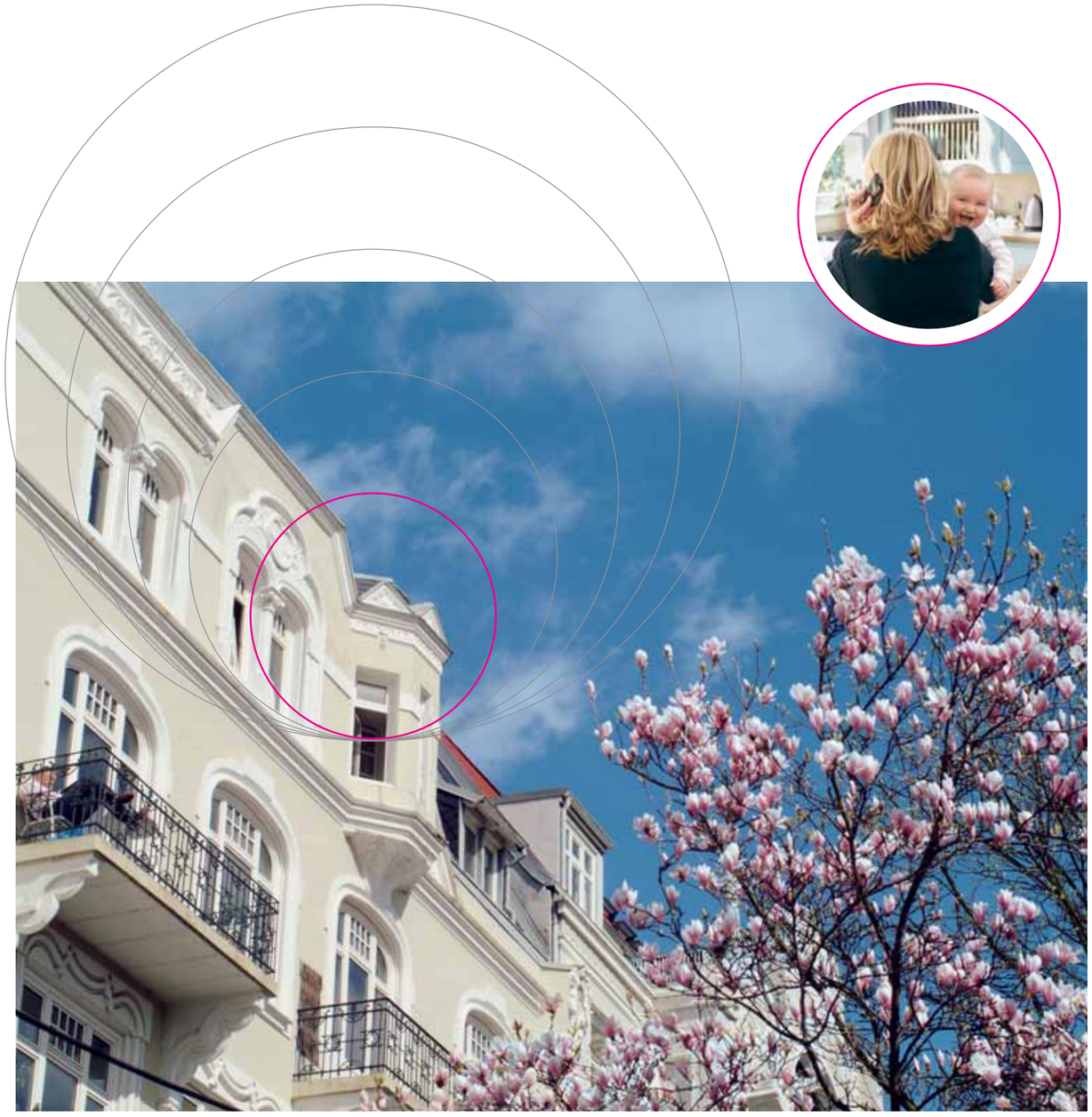
Anfragen.
Die Zahl der Kundenanfragen ist seit den Datenvorfällen stark angestiegen. Waren es 2007 etwa 600 Anfragen, stieg die Anzahl 2008 bereits auf rund 1 400. Auch im Jahr 2009 hielt sich die Anzahl der Anfragen mit 1179 auf hohem Niveau, wobei die häufigsten Anfragen zu gespeicherten Daten (35 %), Werbemaßnahmen (15 %) und (Telefon-)Verzeichniseinträgen (8 %) gestellt wurden.

Anfragen der Aufsichtsbehörden haben ebenfalls zugenommen. Waren im Jahr 2007 etwa 170 Anfragen zu bearbeiten, so betrug die Anzahl im Jahr 2008 rund 250. Dieses hohe Niveau wurde im Jahr 2009 mit 264 Anfragen noch übertroffen. Die häufigsten Anfragen bezogen sich auf Widersprüche zu Werbemaßnahmen (18 %), (Telefon-)Verzeichniseinträge (11 %) sowie Auskünfte zu gespeicherten Daten (5 %).

Auch die an den Konzerndatenschutz der Deutschen Telekom gerichteten Anfragen hinsichtlich Projekt-, Vertrags- und Konzeptprüfungen haben in den vergangenen Jahren erheblich zugenommen. Im Vergleich des Jahres 2007 mit 2009 stiegen die Anfragen im Bereich des Arbeitnehmerdatenschutzes von etwa 250 auf 500, im Bereich des Kundendatenschutzes von etwa 400 auf 950 und im Geschäftskunden- und Produktbereich von etwa 100 auf 350.

Fazit

Die Deutsche Telekom misst dem Thema Datenschutz seit den Vorfällen des Jahres 2008 eine grundlegend neue Bedeutung bei. Dies zeigt nicht zuletzt die Schaffung des neuen Vorstandsressorts Datenschutz, Recht und Compliance im Jahr 2008. Die Deutsche Telekom versteht Datenschutz umfassender als zuvor: Sie hat ihre bisherigen Maßnahmen zum Datenschutz überprüft und optimiert sie kontinuierlich. Gleichzeitig arbeitet sie weiter an einer lückenlosen Aufklärung sämtlicher Vorgänge, die im Zuge der Vorfälle 2008 stattgefunden haben. Eine transparente Darstellung sämtlicher relevanter Ereignisse stand und steht weiterhin im Fokus der Deutschen Telekom. Gleichzeitig legt der Konzern Wert auf eine konstruktive Zusammenarbeit mit staatlichen Stellen und auf gesicherte und zertifizierte Standards im Datenschutz.



Telefonieren, Mailen, Chatten, Internetshopping oder das Handy als mobiles Navigationsgerät: Die Möglichkeiten der Telekommunikation werden immer größer – die Menge an Daten, die jeder dabei preisgibt, auch. Die Deutsche Telekom sorgt dafür, dass diese Daten sicher sind. Für Privat- und Geschäftskunden ebenso wie für die eigenen Arbeitnehmer.

Datenschutz im Detail.

Übergreifende Regelungen und Maßnahmen.

Das Verständnis für die Belange des Datenschutzes, die Sensibilisierung der Mitarbeiter sowie die Information der Kunden waren im Jahr 2009 zentrale Anliegen des Konzerndatenschutzes der Deutschen Telekom.

Kundenkommunikation.

Datenschutzbericht.
Im Mai 2009 veröffentlichte die Deutsche Telekom als erstes DAX-30-Unternehmen in Deutschland erstmals einen Datenschutzbericht. Dieser Bericht wird nun jährlich herausgegeben. Die Veröffentlichung des Datenschutzberichts ist ein weiterer Schritt zur Einlösung des Versprechens, auf dem Gebiet des Datenschutzes für mehr Transparenz zu sorgen und sich der öffentlichen Kritik zu stellen.

Spezial-Internetseite.
Nach den Datenvorfällen im Jahr 2008 hat sich die Deutsche Telekom das Ziel gesetzt, umfassend über das Thema Datenschutz im Konzern zu berichten. Auf der Internetseite www.telekom.com/datenschutz werden Kunden über folgende Aspekte informiert:

- Tipps zum Umgang mit Daten im Internet
- Informationen über relevante Gesetze und Unternehmensregelungen
- Informationen zu Sicherheitsstandards bei der Deutschen Telekom (Zertifizierungen, Audits und Schulungen)
- Dokumentation aller Datenschutzvorfälle und der diesbezüglich getroffenen Maßnahmen
- Antworten zu den am meisten gestellten Fragen
- Möglichkeit zum Herunterladen der Datenschutzberichte
- Möglichkeit zur Kontaktaufnahme mit dem Konzerndatenschutz

Datenschutzberatungen.
Bei der CeBIT in Hannover, dem Tag der offenen Tür der Stadt Bonn und der Internationalen Funkausstellung (IFA) in Berlin beantworteten Mitarbeiter des Konzerndatenschutzes der Deutschen Telekom Fragen rund um die Themen Datenschutz und Sicherheit im Internet. Bei einem Gewinnspiel mit gezielten Fragen zum Datenschutz konnten Interessierte ihr Datenschutzwissen testen und auf mögliche Gefahren im Umgang mit persönlichen Daten im Internet aufmerksam gemacht werden. In der T-Mobile-Zentrale in Bonn gab der Konzerndatenschutzbeauftragte der Deutschen Telekom, Dr. Claus Dieter Ulmer, bei einer Fragestunde zudem allen interessierten Eltern, Lehrern und Jugendlichen Auskunft rund um die Sicherheit von Daten im Internet.

Perspektive aus dem Datenschutzbeirat.

Frage
an Prof. Peter Gola,
Vorsitzender des Vorstands der Gesellschaft für Datenschutz und Datensicherheit

Wo liegt Ihrer Meinung nach in der Informationsgesellschaft die größte Herausforderung für den Datenschutz?
Die personenbezogene Datenverarbeitung ist mittlerweile allgegenwärtig. Auch der Betroffene, der für sich selbst „Datensparsamkeit“ praktizieren will, wird sich dieser Realität nicht entziehen können. Das gilt insbesondere für die Verbreitung personenbezogener Daten im Internet. Die hierdurch bestehenden Gefährdungen des Persönlichkeitsrechts stellen eine der wichtigsten Anforderungen an den Datenschutz dar. Diese Gefährdungen können wie beim Cloud Computing technischer Natur sein, durch Datenverbreitung durch Dritte oder den Betroffenen selbst, insbesondere durch unkritische Nutzung sozialer Netzwerke, verursacht sein.

Interne Kommunikationsmaßnahmen.

Um den Datenschutz im Unternehmen nachhaltig zu verankern und das Bewusstsein für Datenschutz weiter zu verbessern, wurden auch 2009 zahlreiche interne Schulungen und Awareness-Maßnahmen durchgeführt.

Schulungen.
Das Schulungskonzept des Konzerndatenschutzes sieht sowohl verpflichtende Regelschulungen als auch spezifische Schulungen für einzelne Unternehmensbereiche und Arbeitnehmergruppen vor. Einige dieser Schulungen werden als e-Learning-Module angeboten. Neue Mitarbeiter erhalten bei ihrer Einstellung eine Datenschutzunterweisung und werden durch eine Schulung mit anschließendem Test auf das Datengeheimnis gemäß Bundesdatenschutzgesetz und das Fernmeldegeheimnis gemäß Telekommunikationsgesetz verpflichtet. Diese Schulung wird alle zwei Jahre wiederholt.

Im Jahr 2009 wurden insbesondere die Mitarbeiter der Konzernsicherheit und der Revision geschult. In über 30 ganztägigen bzw. mehrstündigen Schulungen wurden alle Mitarbeiter der Konzersicherheit detailliert mit den datenschutzrechtlichen Rahmenbedingungen und Anforderungen vertraut gemacht. Hier konnte auf einer guten Basis, dem intensiven Schulungsprogramm des Konzerndatenschutzes für den Sicherheitsbereich in 2008, aufgesetzt werden. Eine intensive Schulung erhielt der Revisionsbereich zu den Auswirkungen der Novellierung des Bundesdatenschutzgesetzes und zum Umgang mit Mitarbeiterdaten aus datenschutzrechtlicher Sicht. Die Datenschutzprüfung und die Konsultationspflichten wurden fest in die Revisionsprozesse integriert. Die Datenschutzgrundkonzeption, die gemeinsam mit der Revision entwickelt und dort eingeführt wurde, konkretisiert die spezifischen Beteiligungs- und Informationspflichten der Revision gemäß der Beteiligungsrichtlinie des Konzerndatenschutzes. Die Datenschutzgrundkonzeption klärt zudem, was im Rahmen von personenbezogenen Auswertungen zu beachten ist.

Datenschutzkongress für Führungskräfte.
Im Fokus stand auch die Unterstützung der Führungskräfte beim Umgang mit Fragen des Datenschutzes. So hat die Deutsche Telekom mit dem Datenschutzkongress für Führungskräfte in Frankfurt im November 2009 erstmals einen zweitägigen Datenschutzkongress für alle Führungskräfte der Deutschen Telekom in Deutschland organisiert. Dr. Manfred Balz, Vorstand Datenschutz, Recht und Compliance, übernahm die Schirmherrschaft. Als Referenten hatte die Deutsche Telekom namhafte Datenschutzexperten aus der Wissenschaft und Vertreter der Aufsichtsbehörden gewonnen.

Newsletter und Intranet.
Der Konzerndatenschutz informiert in einem regelmäßigen Newsletter interessierte Mitarbeiter über aktuelle Datenschutzthemen. Weitere Informationen zum Thema Datenschutz stehen den Mitarbeitern im Intranet zur Verfügung.

Zusammenarbeit mit den Datenschutzkoordinatoren/ Aufbau dezentrale Datenschutzorganisation.
Die Datenschutzkoordinatoren aller Geschäftsfelder nehmen eine wichtige Multiplikatorenfunktion für den Datenschutz im Unternehmen ein. Mitte November 2009 fand in der Konzernzentrale der Deutschen Telekom in Bonn das dritte Jahr in Folge ein Datenschutzkoordinatoren-Treffen statt. Hierbei standen Vorträge über die neuen Entwicklungen zum Datenschutz bei der Deutschen Telekom und über die Umsetzung der neuen gesetzlichen Regelungen im Mittelpunkt. Im Jahr 2010 wird die Zusammenarbeit mit den Datenschutzkoordinatoren durch mehrere Workshops weiter intensiviert.

Awareness-Maßnahmen.
Die erfolgreiche Umsetzung von datenschutz- und datensicherheitsrelevanten Anforderungen steht und fällt mit der Unterstützung durch das Management und die Mitarbeiter. Auch im Jahr 2009 wurden deshalb Awareness-Maßnahmen im Konzern zu Datenschutz und Sicherheit durchgeführt. Mit einer Kampagne wurden die Mitarbeiter darauf hingewiesen, darauf zu achten, dass sich nur befugte Personen in den Unternehmensgebäuden aufhalten. Zur Kampagne zählten auch Themen wie der Verschluss wichtiger Unterlagen oder das papierlose Büro.

Neues Vorgehensmodell bei der Beratung und Betreuung von Produkt- und Systementwicklungsprozessen.
Im Rahmen der Neustrukturierung des Vorstandbereichs Datenschutz, Recht und Compliance wurde das „Operating Model“ entwickelt. Dies definiert, wie die einzelnen Bereiche innerhalb des Vorstandsbereichs Datenschutz, Recht und Compliance zusammenarbeiten und wie sie mit den Fachabteilungen der anderen Vorstandsbereiche interagieren.
Es wurde ein einheitliches Vorgehensmodell entwickelt, wie im Rahmen der Beratung, Freigabe und Kontrolle von IT- und Netztechnik-Systemen ein adäquates Datenschutz- und Sicherheitsniveau sichergestellt werden kann. Je kritischer ein Projekt, desto umfassender ist der Beratungs- und Betreuungsaufwand durch die kontrollierenden Einheiten und desto tiefer gehen die Prüfprozesse und Auditierungen. Durch das gemeinsame Vorgehen werden Synergieeffekte im Bereich von Datenschutz und Datensicherheit genutzt.

Beteiligungs- und Informationsrichtlinie.
Im Rahmen der Sofortmaßnahmen zum Datenschutz hat der Konzerndatenschutz eine Informations- und Beteiligungsrichtlinie erstellt. In der Richtlinie ist geregelt, wann und wie der Bereich Konzerndatenschutz bei Maßnahmen mit Datenschutzbezug zu beteiligen ist. Darüber hinaus regelt die Richtlinie Informationsverpflichtungen bei Datenschutzverletzungen im Konzern. Die Richtlinie findet Anwendung auf die Deutsche Telekom AG und alle nationalen Mehrheitsbeteiligungen. Inzwischen wurde die Richtlinie weitestgehend umgesetzt.

Konzernweite Leitlinien zur Wahrung des technischen Datenschutzes.
Mehr technischer Datenschutz bedeutet höheres und vor allem nachhaltiges Kundenvertrauen – was einen Mehrwert in der Wertschöpfungskette erzeugt. Deshalb hat der Konzerndatenschutz gemeinsam mit der IT-Sicherheit an verschiedenen Grundsatzregelungen zum technischen Datenschutz gearbeitet. An der Spitze der Regelungshierarchie der Leitlinien zum technischen Datenschutz steht die Zentrale Sicherheitsleitlinie mit dem Privacy Code of Conduct. Mit diesen Leitlinien werden konzernweite Mindeststandards für ein adäquat hohes technisches Sicherheitsniveau in der Deutschen Telekom geschaffen. Auf Basis zentraler Leitlinien ergeben sich weitere themenspezifische Leitlinien, in denen ausgewählte Aspekte von besonderer Bedeutung für den Bereich Datenschutz und Datensicherheit detailliert werden.

Aufbau einer gesonderten Abteilung für Kontrollmaßnahmen.
Im Rahmen des Sofortmaßnahmenprogramms des Vorstandsbereichs Datenschutz, Recht und Compliance wurde eine neue Abteilung innerhalb des Konzerndatenschutzes gegründet. Aufgaben dieser Abteilung sind die Sicherstellung der Umsetzung von Datenschutzanforderungen durch verstärkte Kontrollen und Audits von IT-Systemen sowie das verstärkte Hinwirken auf die Etablierung einheitlicher Datenschutzstandards.

Auditierungskonzept des Konzerndatenschutzes.
Datenschutzauditierungen sind ein wichtiger Bestandteil, um die Umsetzung und Einhaltung von Vorgaben zu Datenschutz und Datensicherheit zu überprüfen.

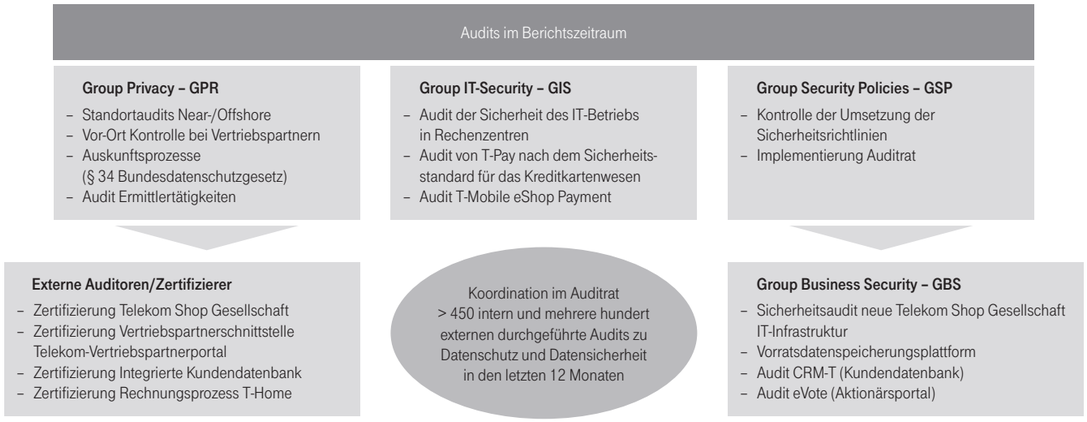
Kontrollen zu Datenschutz und Datensicherheit.

	Organisationskontrollen	Regelprozesse	Auditierungen
Intern	BilMoG CLC Datenschutz Internationales Basisdatenschutzaudit BilMoG CLC Sicherheit S-OX Kontrolle Sicherheit	Datenschutzberatung Prüfung und Freigabe von Datenschutzkonzepten Fallbezogene Überprüfungen nach internen Hinweisen Schwachstellen Management	Auditjahresprogramme Abnahmeaudits Anlassaudits Vorstandsbereich Datenschutz, Recht und Compliance
Extern	ISO 27001 Audits Prüfungen durch den Bundesdatenschutzbeauftragten	Fallbezogene Überprüfungen nach externen Beschwerden (Bundesdatenschutzbeauftragter, Kunden, Bundesnetzagentur)	Externe Zertifizierungen Prüfung Sicherheitskonzepte gem. Telekommunikationsgesetz § 109 durch Bundesnetzagentur

Dennoch sind Auditierungen nur ein, wenn auch wichtiger Baustein zum Erreichen eines adäquaten Datenschutzniveaus bei der Deutschen Telekom. Viele weitere Kontrollmechanismen stellen sicher, dass Datenschutz- und Datensicherheitsmaßnahmen implementiert sind. Dies sind neben Organisationskontrollen nach dem amerikanischen Sarbanes-Oxley Act (S-OX), dem Bilanzrechtsmodernisierungsgesetz (BilMoG) oder Zertifizierungen nach anerkannten Standards (ISO 27001) auch die Prozesse zur Beratung, Prüfung und Freigabe von Datenschutz- und Sicherheitskonzepten, externe Prüfungen durch Aufsichtsbehörden und die Bearbeitung von Hinweisen und Beschwerden von Kunden und Mitarbeitern zu Datenschutzproblemen.

Das Auditkonzept der Deutschen Telekom umfasst drei Säulen. Die erste ist das Basisdatenschutzaudit, das sowohl national als auch international durchgeführt wird. Die zweite Säule umfasst System-, Organisations- und Prozessaudits. Daneben existiert die dritte Säule, die anlassbezogene Audits bei Vorfällen oder Verdacht vorsieht. Zur dritten Säule zählen auch die Abnahmeaudits, die vor der Freigabe von priorisierten Projekten durchgeführt werden.

Überblick über Auditierungen im Konzernumfeld zum Thema Datenschutz und Datensicherheit.



Auditschwerpunkte 2009.

Die im Jahr 2009 durchgeführten Audits hatten folgende Schwerpunkte:

Internationale Audits.
Ein Schwerpunkt war die Überprüfung und Bescheinigung eines angemessenen Datenschutzniveaus von internen und externen Dienstleistern im Near- und Offshore-Umfeld. So wurden etwa mehrere Produktionsstandorte der T-Systems in Russland, Tschechien oder Ungarn auditiert. Ihnen wurde unter einigen nicht kritischen Auflagen ein angemessenes Datenschutzniveau bescheinigt. Gleiches gilt für externe Partner wie Cognizant in Indien oder Reksoft in Russland.

Datenschutzgerechte Entsorgung von Datenträgern.
Die Deutsche Telekom ließ die datenschutzgerechte Entsorgung von Papier und Datenträgern an mehreren Standorten des Konzerns und an verschiedenen Standorten des Entsorgungsunternehmens auditieren. Außerdem wurde der Prozess untersucht, der sicherstellt, dass von Kunden zurückgegebene Mobilfunkgeräte datenschutzgerecht entsorgt und die darauf gespeicherten Daten vor der Wiederverwertung sicher gelöscht werden.

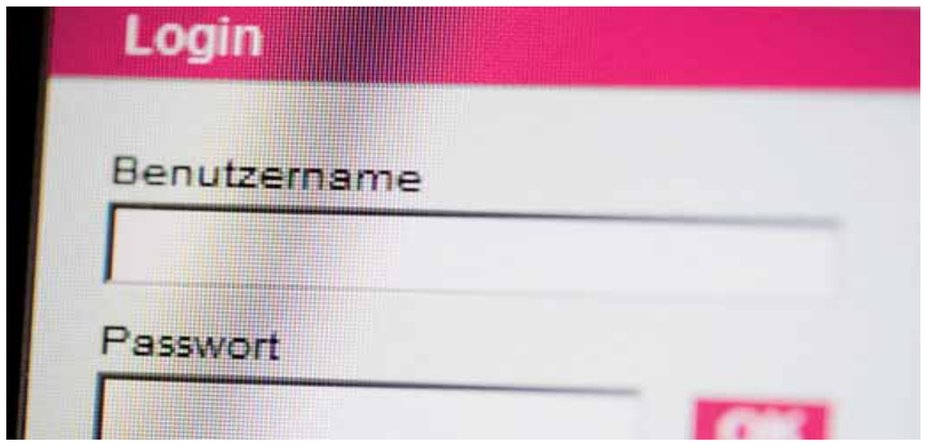
Audits bei Vertriebspartnern.
Verschiedene Vertriebspartner der Deutschen Telekom wurden ebenfalls auditiert. Außerdem wurden Auditierungs- und Zertifizierungskriterien zum Thema Datenschutz festgelegt, nach denen für bestimmte Geschäftsmodelle ausgewählte Vertriebspartner einen Zertifizierungsprozess durchlaufen müssen oder nach dem Outbound-Call-Center der Deutschen Telekom zertifiziert werden. Outbound-Calll-Center sind die Partnerunternehmen der Deutschen Telekom, die den Konzern beim telefonischen Vertrieb von Produkten des Konzerns unterstützen. Des Weiteren wurden Kriterien festgelegt, die eine Beurteilung der Einhaltung der technischen und organisatorischen Maßnahmen zum Datenschutz bei Dienstleistern auf Grundlage einer bestehenden Auftragsdatenverarbeitung eindeutiger erlauben.

Prozessaudits bei der Konzernsicherheit.
Bei der Deutschen Telekom wurden einige interne Prozesse auditiert. So wurde etwa untersucht, wie der Ermittlungsprozess der Konzernsicherheit abläuft. Dies wird nach den stattgefundenen Bespitzelungen als eine sinnvolle Maßnahme im Nachgang zur Neuordnung der Konzernsicherheit und der Einführung des Datenschutzkonzepts für diesen Bereich betrachtet.

Unternehmensüberwachung im Rahmen des Bilanzrechtsmodernisierungsgesetzes.
Die Deutsche Telekom hat nach den Anforderungen des Bilanzrechtsmodernisierungsgesetzes (BilMoG) ein internes Kontrollsystem aufgebaut, das die unterschiedlichsten Unternehmensbereiche umfasst. Dieses Kontrollsystem wird jährlich von externen Prüfern auf seine Tauglichkeit und Umsetzung hin untersucht. Dem Datenschutz wurde darin ein eigenes Kontrollumfeld zugewiesen, das sich spezifisch mit der Organisation sowie den Regelungen und Prozessen zur Einhaltung der gesetzlichen Datenschutzvorgaben befasst. Die Prüfung wurde im Jahr 2009 erstmals erfolgreich durchgeführt. Die dabei identifizierten Verbesserungspotenziale wurden an die verantwortlichen Stellen adressiert und die Umsetzung angestoßen.

Ausblick Auditschwerpunkte 2010.

Im Jahr 2010 finden verstärkt Auditierungen bei Vertriebspartnern und Auftragsdatenverarbeitern statt. Im internationalen Umfeld ist neben der Auditierung von internen und externen Dienstleistern im Near- und Offshore-Bereich die Vor-Ort-Auditierung der Umsetzung und Einhaltung des Privacy Code of Conduct in den internationalen Einheiten der Deutschen Telekom ein Schwerpunkt. Des Weiteren werden die kritischsten und wichtigsten Applikationen und Datenbanken im Konzern auditiert und für die wichtigsten IT-Systeme und Plattformen Abnahmeaudits vorgenommen.



Die Deutsche Telekom hat ein internes Kontrollsystem aufgebaut, das die unterschiedlichsten Unternehmensbereiche umfasst. Dieses wird jährlich von externen Prüfern auf seine Tauglichkeit und Umsetzung hin untersucht.

Perspektive aus dem Datenschutzbeirat.

Fragen
an Prof. Dr. Peter Wedde,
Professor für Arbeitsrecht und Recht in der Informationsgesellschaft an der Fachhochschule Frankfurt/Main

In jüngster Zeit wurde ein Arbeitnehmerdatenschutzgesetz diskutiert. Brauchen wir Ihrer Meinung nach mehr Rechtsvorschriften auf diesem Gebiet?
Eine geschlossene und vollständige gesetzliche Regelung zum Arbeitnehmerdatenschutz ist längst überfällig. Ein Arbeitnehmerdatenschutzgesetz würde für Arbeitgeber wie für Beschäftigte Rechtssicherheit schaffen und viele Konflikte gar nicht erst entstehen lassen. Hierzu gehört beispielsweise die Festlegung klarer Grenzen für die Zulässigkeit der Überwachung von Beschäftigten durch technische Einrichtungen wie Videokameras ebenso wie die Regelung der Zulässigkeit ärztlicher Untersuchungen in Bewerbungsverfahren. Wichtig ist auch die Begrenzung der Zulässigkeit „freiwilliger" Einwilligungen von Beschäftigten für die Fälle, in denen sich das Vorliegen einer Drucksituation nicht sicher ausschließen lässt.

Sollte die private Nutzung des Internets am Arbeitsplatz erlaubt sein?
Internetanwendungen wie E-Mail oder der Zugriff auf das Web sind für viele Menschen heute selbstverständliche Informationsquellen und Kommunikationsmittel. Viele Arbeitgeber haben kein Problem damit, wenn Beschäftigte betriebliche Internetzugänge gelegentlich auch privat nutzen. Problematisch ist nur, dass die Erlaubnis der privaten Nutzung zwingend die Anwendbarkeit des Telekommunikationsgesetzes nach sich zieht. Arbeitgeber werden damit aus rechtlicher Sicht automatisch denselben hohen Datenschutz- und Datensicherungsanforderungen unterworfen wie etwa Anbieter von Mobiltelefondiensten. Hieraus resultieren einerseits hohe Anforderungen an die technische Sicherung der betrieblichen Systeme. Regeln des Telekommunikationsgesetzes schließen zudem aus, dass Arbeitgeber Einblick in Kommunikationsinhalte ihrer Beschäftigten nehmen können, ohne dass etwa differenziert wird, ob es sich um geschäftliche oder private E-Mails handelt. Es wäre gut, wenn der Gesetzgeber dafür sorgen würde, dass dieser Mechanismus aufgehoben wird. Notwendig wäre hierfür nur eine kleine Modifikation des Telekommunikationsgesetzes, die ausschließt, dass die begrenzte Privatnutzung betrieblicher Systeme schon für sich allein die Anwendbarkeit dieses Gesetzes nach sich zieht.

Status Arbeitnehmerdatenschutz.

Die Serie von im Jahr 2009 bekannt gewordenen Fällen, in denen deutsche Unternehmen Mitarbeiterdaten unzulässigerweise erhoben und genutzt haben, verdeutlicht das zumindest in Teilen der Wirtschaft immer noch fehlende Verständnis und die unzureichende Kenntnis hinsichtlich des zulässigen Verwendungsrahmens von personenbezogenen Daten.

Nach dem Motto „Vertrauen ist gut, Kontrolle ist besser" rechtfertigen Unternehmen ihre Kontrollaktionen mit dem Bedürfnis, sich aktiv gegen Verfehlungen der Beschäftigten schützen zu wollen. Rechtlich betrachtet geht es um eine Abwägung zwischen Arbeitgeberrechten, dem Schutz des Unternehmens und dem im Grundgesetz verankerten Persönlichkeitsrecht der Arbeitnehmer.

Ein Generalverdacht darf zum Eingriff in das Persönlichkeitsrecht jedoch keinesfalls ausreichen. Eine Auswertung personenbezogener Daten ist nach dem Bundesdatenschutzgesetz nur in besonderen Fällen zulässig, z. B. beim konkreten Verdacht einer Straftat im Arbeitsverhältnis. Und dies auch nur dann, wenn weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind.

Rahmenbedingungen im Konzern Deutsche Telekom.

Bei der Deutschen Telekom sind zentrale Rahmenbedingungen zum Arbeitnehmerdatenschutz im Privacy Code of Conduct und den Betriebsvereinbarungen festgelegt. Im Privacy Code of Conduct werden die internen Anforderungen an den Umgang mit personenbezogenen Daten in der Deutschen Telekom Gruppe einheitlich geregelt. Die Betriebsvereinbarungen schaffen zusätzlich spezielle Rechte und Pflichten für Arbeitgeber und Arbeitnehmer und bilden so verbindliche Normen für den Umgang mit personenbezogenen Daten in den Regelungsbereichen, für die sie abgeschlossen wurden. Ein prominentes Beispiel für eine Betriebsvereinbarung mit starkem datenschutzrechtlichen Anteil ist die Regelung zum Umgang mit Videoüberwachungsmaßnahmen: Auswertungen von Beschäftigtendaten sind nur bei Sicherheitsvorfällen erlaubt und dürfen nur durch dazu berechtigte Stellen vorgenommen werden. Diese Stellen sind abschließend in einem Datenschutzkonzept aufgelistet. Weiter gehende Verhaltens- und Leistungskontrollen sind ausdrücklich verboten. Es sind ferner Regelungen zu Löschfristen enthalten. Die Beschäftigten werden darüber hinaus über den Einsatz von Videoanlagen informiert.

Alle zwei Jahre werden die in Deutschland beschäftigten Mitarbeiter des Konzerns auf den Datenschutz und das Fernmeldegeheimnis verpflichtet.

Projekte aus dem Jahr 2009.

Telekom Awareness for Compliance and Ethics.
Ein weltweit führender Anbieter für Compliance-Schulungen stellt seit 2009 eine einheitliche Unterweisungs- und Kommunikationsplattform rund um die Einhaltung von Verhaltensregeln, Gesetzen und Richtlinien u. a. zur Korruptionsvermeidung zur Verfügung. Die Deutsche Telekom ist aufgrund ihrer Börsennotierung in den USA und der daraus resultierenden Anforderungen zur konzernweiten Umsetzung von speziellen Schulungsmaßnahmen verpflichtet. Einige dieser webbasierten Schulungen betreffen ausgewählte Beschäftigte, andere muss jeder Mitarbeiter innerhalb einer bestimmten Zeitspanne absolvieren. Das Dienstleistungsverhältnis selbst sowie die Systematik von Schulungen hat die Deutsche Telekom den hohen Datenschutzanforderungen im Konzern angepasst. Insbesondere hat das Unternehmen sichergestellt, dass keine unzulässigen Auswertungen bezogen auf die Schulungsergebnisse stattfinden können.

1000° Umfragetool der Multimedia Solutions GmbH (MMS).
„1000°" ist ein neues, webbasiertes System, das die Deutsche Telekom seit 2009 für Umfragen unter Mitarbeitern nutzt. Hier musste der Konzern gewährleisten, dass weder die Teilnahme an der Umfrage noch die Aussagen in der Umfrage auf einzelne Mitarbeiter heruntergebrochen werden können: Um Mehrfachteilnahmen zu vermeiden, wird der Teilnehmerkreis zwar mittels personalisierter Einladung per Mail auf eine Umfrage hingewiesen. Der Personenbezug wird nach der Zustellung jedoch automatisch gelöscht und die Antworten werden so nicht personenbezogen ausgewertet. Werden Bereichsergebnisse abgefragt, werden diese nur für Bereiche, die eine bestimmte Mitarbeiteranzahl übersteigen, ausgewertet, um eine indirekte Rückführbarkeit auf einzelne Personen zu verhindern. Die einzelnen Umfragen werden zur Genehmigung beim Konzerndatenschutz vorgelegt.

Überprüfung der elektronischen Personalakte.
Im Jahr 2009 wurde das System zur Verwaltung von Personalakten auf einen elektronischen Arbeitsprozess umgestellt. Voraussetzung dafür war die Verfügbarkeit der Personalakten in elektronischer Form. In diesem Zusammenhang wurden die elektronischen Personalakten der Mitarbeiter durch den Konzerndatenschutz und den Personal Service Telekom unter Einbindung der Arbeitnehmervertretung überprüft, ob ihnen fälschlicherweise personenbezogene Daten anderer Mitarbeiter zugeordnet waren. In 2 056 424 Dokumenten wurden 3 678 Dokumente mit personenbezogenen Daten anderer Mitarbeiter gefunden. Dies entspricht einer (geringen) Fehlerquote von 0,18 %. Hauptursache dieser Fehler waren fehlerhafte Zuordnungen bereits in den Dokumenten, die zur Digitalisierung bereitgestellt worden waren. Sollten sich in den Personalakten in Einzelfällen nach wie vor personenbezogene Daten anderer Personen befinden, kann jeder Mitarbeiter diese mit Hilfe eines mit der Arbeitnehmervertretung vereinbarten Beanstandungs- und Korrekturprozesses im Intranet korrigieren.

Konzernweite Verpflichtung auf das Daten- und Fernmeldegeheimnis im Jahr 2009.
Alle zwei Jahre werden die in Deutschland beschäftigten Mitarbeiter des Konzerns auf den Datenschutz und das Fernmeldegeheimnis verpflichtet. In den weiteren Konzernteilen sind regelmäßige Schulungen über den Privacy Code of Conduct vorgeschrieben. Durch die regelmäßige Wiederholung der Verpflichtung im Zusammenhang mit einer Schulungs- und Sensibilisierungsmaßnahme wird sichergestellt, dass alle Mitarbeiter nachhaltig und kontinuierlich darauf hingewiesen werden, dass es notwendig ist, die Datenschutzbestimmungen einzuhalten. Neben der Sicherstellung eines hohen Datenschutzniveaus kommt die Deutsche Telekom damit auch den vertraglichen und gesetzlichen Verpflichtungen gegenüber ihren Kunden nach.

Implementierung des § 32 Bundesdatenschutzgesetz (BDSG).
Besondere Anforderungen bestanden im Jahr 2009 hinsichtlich der Umsetzung der Vorgaben des neuen § 32 BDSG. Die Vorschrift regelt erstmals explizit die Grundsätze des Arbeitnehmerdatenschutzes im allgemeinen Datenschutzrecht. Der Wortlaut der Vorschrift hatte zu einiger Unsicherheit in der Fachwelt geführt, auch wenn es Ziel des Gesetzgebers war, die bis dahin bestehende Rechtslage eindeutiger darzustellen. Die neue Vorschrift schafft zum einen klare Regelungen zum Umgang mit Arbeitnehmerdaten, zur Durchführung des Arbeitsverhältnisses und zur Verwendung von Arbeitnehmerdaten bei der Verfolgung strafrechtlicher Verfehlungen der Arbeitnehmer im Arbeitsverhältnis. Gleichzeitig hat sie jedoch die Unsicherheiten im Bereich der Massendatenverarbeitung zur Kontrolle von Prozessen weiter erhöht. Die Frage, inwiefern die Verarbeitung von größeren Datenmengen zur Überprüfung des ordnungsgemäßen Handelns von Mitarbeitern noch zulässig ist, ist so nach wie vor nicht geklärt. Der Vorstand der Deutschen Telekom hat daher beschlossen, entsprechende Kontrollprozesse zunächst auf ihren abgesichert zulässigen Kern zu beschränken. Dies hat zur Folge, dass insbesondere konzerninterne Ermittlungen durch Konzernsicherheit und Konzernrevision in der Regel nicht mehr durchgeführt werden. Ausnahmen unterliegen einem strengen Freigabeprozess.

Umgang mit Gesundheitsdaten.
Der Umgang mit Daten, die den Gesundheitszustand von Beschäftigten betreffen, ist bei der Deutschen Telekom restriktiv geregelt. Die Verarbeitung solcher Daten darf nur dann erfolgen, wenn dies zur Durchführung des Beschäftigungsverhältnisses zwingend erforderlich ist und Rechtsvorschriften dies verlangen. Fragen nach dem Gesundheitszustand der Mitarbeiter sind nur dann zulässig, wenn befürchtet werden muss, dass der entsprechende Mitarbeiter für einen vorgesehenen Arbeitsplatz beeinträchtigt ist. Bei Arbeitsunfähigkeit dürfen Fragen nach deren Grund sowie der ärztlichen Diagnose nicht gestellt werden. Lediglich die aus tatsächlichen und rechtlichen Gründen notwendigerweise unmittelbar mit dem jeweiligen Vorgang befassten Personen dürfen – unter strenger Auslegung des Erforderlichkeitsgrundsatzes – Kenntnis erhalten. Alle Führungskräfte im Inland wurden im Jahr 2009 noch einmal ausdrücklich auf diese Regelung hingewiesen.

Ausblick.
Als Orientierungshilfe zum Umgang mit personenbezogenen Daten der Beschäftigten wird künftig ein Leitfaden zum Personaldatenschutz entwickelt und im Konzern eingeführt. Er soll die zum Teil isolierten datenschutzrechtlichen Regelungen, Standardfragen und Vorschriften zusammenfassen und den Beschäftigten als „Datenschutzkompass“ dienen. Ziel: Mit klaren Vorgaben und Normen die Kommunikation erleichtern, inhaltliche Komplexität abbauen und das grundsätzliche Verständnis in Bezug auf die Verarbeitung von Mitarbeiterdaten fördern.

Nach dem Urteil des Bundesverfassungsgerichts hat die Deutsche Telekom Speicherung und Beauskunftung sämtlicher Vorratsdaten unverzüglich gestoppt.

Status Kundendatenschutz.

Rahmenbedingungen im Konzern Deutsche Telekom.
Im Jahr 2009 traten etliche gesetzliche Regelungen in Kraft, die zu Änderungen und Neuerungen im Kundendatenschutz führten:

Vorratsdatenspeicherung.
Mit Beginn des Jahres 2008 wurde die Vorratsdatenspeicherung für die Festnetz- und Mobilfunktelefonie eingeführt. Die Regelung sah für Telekommunikationsunternehmen die Verpflichtung vor, u. a. die Telefonnummer des Anrufenden, Zeit und Länge des Anrufs und im Mobilfunk die Funkzelle, in der eine Verbindung begonnen wurde, zu speichern. Im Januar 2009 trat zusätzlich die Speicherpflicht für E-Mails und Internetnutzung in Kraft. Nach dem Telekommunikationsgesetz mussten ab diesem Zeitpunkt beim Versenden einer E-Mail die Postfachkennung des Absenders und jedes Empfängers, die IP-Adresse des Absenders sowie Datum und Uhrzeit des Versands unter Angabe der Zeitzone für sechs Monate gespeichert werden. Im Falle der Internetnutzung umfasste die Verpflichtung zur Vorratsdatenspeicherung die dynamische IP-Adresse des Nutzers, die eindeutige Anschlusskennung, über die der Zugang erfolgte, sowie Beginn und Ende der Internetnutzung unter der zugewiesenen IP-Adresse nach Datum, Uhrzeit und Zeitzone.

Der Konzerndatenschutz der Deutschen Telekom hatte die zuständigen Fachbereiche datenschutzrechtlich dabei unterstützt, die Vorgaben zur Vorratsdatenspeicherung im Konzern umzusetzen. Im Vordergrund standen hierbei die Trennung des Datenbestands vom eigentlichen Kundendatenbestand, die Sicherung gegen unberechtigte Zugriffe und die Beachtung der gesetzlichen Löschfristen. Im Rahmen eines Informationsbesuchs verschaffte sich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im Jahr 2009 einen Überblick über die konkrete Umsetzung der Vorratsdatenspeicherung bei T-Home und T-Mobile. Die gewählten Lösungen überzeugten die Aufsichtsbehörde.

Nach dem Urteil des Bundesverfassungsgerichts vom 2. März 2010, das die bestehende Regelung zur Vorratsdatenspeicherung für verfassungswidrig erklärte, hat die Deutsche Telekom Speicherung und Beauskunftung sämtlicher Vorratsdaten unverzüglich gestoppt; Die gespeicherten Daten wurden unwiederbringlich gelöscht.

Perspektive aus dem Datenschutzbeirat.

Frage

an Prof. Dr. Hansjörg Geiger,
Honorarprofessor für Verfassungsrecht an der Johann-Wolfgang-Goethe-Universität, Frankfurt, Staatssekretär im Bundesministerium der Justiz (1998 bis 2005)

1983 hat das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht und der Menschenwürde abgeleitet. Greift die Nutzung von Bonitätsdaten in das Recht auf informationelle Selbstbestimmung ein?
Die Thematik der Bonitätsdaten betrifft in mehrerlei Hinsicht das Recht auf informationelle Selbstbestimmung. Das beginnt mit der Frage nach der Rechtmäßigkeit der Erhebung von Bonitätsdaten oder von den Informationen, aus denen „Bonitätsdaten“ abgeleitet werden. Hierbei kann wesentlich sein, ob dies mit Einwilligung oder zumindest Kenntnis des Betroffenen geschieht.

Ein weiterer entscheidender Punkt ist hierbei auch, ob die Bonitätsdaten tatsächlich die aktuelle Bonität eines Betroffenen richtig wiedergeben. Auch die Art des Zustandekommens solcher Bonitätsdaten, also etwa die Transparenz des „Berechnens“ der Bonität, berührt den Datenschutz. Zu beurteilen ist auch, inwieweit derartige Daten auf Vorrat für nicht klar bestimmbare Zwecke gespeichert werden und ob dies für eigene berechtigte geschäftliche Zwecke im Zusammenhang mit vertraglichen Beziehungen zu dem Betroffenen im hierfür erforderlichen Umfang erfolgt.

Die Nutzung von Bonitätsdaten, also deren Erhebung, Speicherung, Weitergabe und sonstige Verarbeitung, berührt also selbstverständlich das Recht auf informationelle Selbstbestimmung, weil Bonitätsdaten personenbezogene Informationen darstellen. Das bedeutet jedoch nicht das Verbot jeglicher Nutzung von Bonitätsdaten. Deren Nutzung kann zum einen mit ausdrücklicher und eindeutiger Zustimmung durch den jeweiligen Betroffenen zulässig sein, sofern diese Einwilligung in Kenntnis deren Bedeutung (informed consent) erteilt und nicht von der Erbringung sonstiger Leistungen abhängig gemacht wird. Außerdem kann deren Nutzung erlaubt sein, sofern hierfür eine entsprechende normenklare gesetzliche Regelung besteht und der Grundsatz der Verhältnismäßigkeit gewahrt ist.

Perspektive aus dem Datenschutzbeirat.

Frage
an Prof. Dr. Peter Wedde,
Professor für Arbeitsrecht und Recht in der Informationsgesellschaft an der Fachhochschule Frankfurt/Main

Was halten Sie vom Zukauf von Daten zu Werbezwecken?
Mit Blick auf die zahlreichen Missbrauchsfälle auch in diesem Bereich stehe ich diesem Thema aus datenschutzrechtlicher Sicht skeptisch gegenüber. Zudem ist es dem Gesetzgeber bei der letzten Novelle des Bundesdatenschutzgesetzes nicht wirklich gelungen, die Rechte der Kunden und Verbraucher wirksam zu stärken und zu sichern. Solange nicht ausgeschlossen ist, dass Betroffene durch den Zukauf Nachteile erleiden können oder persönlich belastet werden, favorisiere ich deshalb eine restriktive Bewertung der Zulässigkeit des Zukaufs von Daten zu Werbezwecken.

Ortungsdienste (Location Based Services).
Das Telekommunikationsgesetz regelt die Verwendung von Mobilfunk-Standortdaten für Ortungsdienste, sog. Location Based Services (LBS). Es existieren zwei verschiedene Ortungsarten: Bei der Eigenortung ermittelt der Teilnehmer seinen Standort im Rahmen eines Ortungsdienstes selbst, um etwa Einrichtungen in seiner Nähe ausfindig zu machen. Zum anderen bieten verschiedene Ortungsdienste eine Fremdortung an. Diese erlaubt es Teilnehmern, den Standort weiterer Teilnehmer zu orten. Diese Dienstleistung ermöglicht es etwa Eltern, den geografischen Standort ihrer Kinder zu bestimmen.

Für beide Ortungsarten schreibt § 98 Telekommunikationsgesetz vor, dass der Mobilfunknutzer der Verwendung seiner Standortdaten, also der Ortung, im Vorfeld zugestimmt haben muss. Auf Initiative der Politik wurde im August 2009 die Regelung in Bezug auf die Fremdortungsdienste verschärft: Die Einwilligung hat seitdem schriftlich zu erfolgen. Außerdem muss der Teilnehmer spätestens nach jeder fünften Ortung per SMS über die Ortungen informiert werden. Die LBS-Anbieter werden von T-Mobile vertraglich verpflichtet, die entsprechende Einwilligung schriftlich einzuholen. Darüber hinaus gibt T-Mobile den konkreten Einwilligungstext vor und lässt sich entsprechende Kontrollrechte beim LBS-Anbieter zusichern. Die Informations-SMS wird von T-Mobile direkt an den Teilnehmer versendet. Vor diesem Hintergrund ist die Diskussion um die Frage, ob die genannte Neuregelung in § 98 Telekommunikationsgesetz den Netzbetreiber oder den Diensteanbieter adressiert, für die Deutsche Telekom nicht relevant: T-Mobile ist als Netzbetreiber in Vorleistung getreten und hat die notwendigen Schritte bereits umgesetzt.

Bei diesen Geschäftsmodellen wird sich in Zukunft ein Wandel ergeben: Künftig wird die Unterstützung der Mobilfunkbetreiber bei der Ortung nicht mehr benötigt: Mobile Endgeräte verfügen zunehmend über eine eigene, viel genauere Ortungsmöglichkeit über GPS und geben ihren Standort direkt über die Internetanbindung an den jeweiligen Diensteanbieter. Hieran knüpfen neue Dienste an.

Werbliche Nutzung von Daten.
Die Novellierung des Bundesdatenschutzgesetzes, die am 1. September 2009 in Kraft trat, sieht vor, dass die werbliche Nutzung von Daten der aktiven Einwilligung des Betroffenen bedarf. Bislang musste der Betroffene widersprechen, wenn er keine Werbung erhalten wollte. Diese Änderung hatte für die Deutsche Telekom keine Auswirkungen: Das für Telekommunikations-Dienstleister geltende Telekommunikationsgesetz hat eine solche Einwilligung bereits zuvor verlangt. Die Deutsche Telekom hat ihre Kunden gemäß dieser gesetzlichen Regelung schon in der Vergangenheit aktiv nach ihrem Einverständnis zur werblichen Nutzung ihrer Daten befragt. Willigt ein Kunde mündlich ein, erhält er zudem eine schriftliche Bestätigung, in der der genaue Wortlaut sowie Erläuterungen zum Gegenstand der Werbeeinwilligung enthalten sind.

Themen aus dem Jahr 2009.

Zusammenarbeit mit Vertriebspartnern.
Der Schutz von Kundendaten in Vertrieb und Service beschäftigte den Konzerndatenschutz während des gesamten Jahres 2009. Im Jahr 2008 waren mit den Vertriebspartnern bereits Vermarktungsverträge mit neuen, strengeren Vereinbarungen zur Auftragsdatenverarbeitung vereinbart worden. Im Jahr 2009 wurden verschiedene technische Hürden eingeführt, die eine rechtswidrige massenhafte Verarbeitung von Kundendatensätzen verhindern sollen. Diese Hürden werden jeweils individuell nach Bedarf und Einsatzszenario in die IT-Systeme eingebaut.

Die Deutsche Telekom führte darüber hinaus eine Liste von IP-Adressen ein, die explizit für den Zugriff auf Kundendaten freigegeben wurden. Gleichzeitig erstellte sie eine Aufstellung der IP-Adressen, die ausdrücklich für den Zugriff gesperrt wurden. Des Weiteren konzipierte sie verschiedene Alarmsysteme, die anschlagen, wenn Auffälligkeiten wie erhöhte Zugriffszahlen auf Daten auftreten.

Der Schutz von Kundendaten in Vertrieb und Service beschäftigte den Konzerndatenschutz während des gesamten Jahres 2009: Die Deutsche Telekom hat verschiedene technische Hürden eingeführt, die eine rechtswidrige massenhafte Verarbeitung von Kundendatensätzen verhindern sollen.

Perspektive aus dem Datenschutzbeirat.

Frage
an Peter Franck,
Chaos Computer Club (CCC)

Welches sind Ihrer Meinung nach die größten Datengefahren für Internetnutzer?
Eine ernstzunehmende, wenn auch schwer greifbare Gefahr ist die ständig wachsende Anzahl von Datensammlungen, in denen jeder Nutzer – meist unbewusst – Spuren hinterlässt. Diese Informationen sind mittlerweile ein gewichtiger Wirtschaftsfaktor geworden. Betroffen sind allerdings nicht nur Internetnutzer, sondern beispielsweise auch Nutzer von Mobiltelefonen, die kontinuierlich Informationen über berufliche und soziale Beziehungen sowie ihren Aufenthaltsort preisgeben.

Die größte Gefahr liegt in der Zusammenführung verschiedener Datenbestände, da sich daraus ein präzises Profil jeder einzelnen Person herstellen lässt, das deren persönliche, soziale, politische und wirtschaftliche Verhältnisse abbildet. Die Deutsche Telekom verfügt über eine beachtliche Menge solcher Datensammlungen, da sie in vielen verschiedenen Rollen, u. a. als Netzbetreiber, Auskunftei, Zahlungssystem- und Medienanbieter, auftritt.

Einführung eines TAN-Verfahrens.
Um die Daten der Kunden noch besser zu schützen, wurde bereits 2008 im Mobilfunkbereich das sog. TAN-Verfahren eingeführt. Kunden, die sich an einen Kundenbetreuer in den Telekom Shops wenden, erhalten eine TAN (Transaktionsnummer) per SMS auf ihr Mobilfunkgerät gesendet, sobald der Kundenbetreuer Kundendaten im System aufrufen möchte. Erst wenn der Telekom-Mitarbeiter die ihm vom Kunden mitgeteilte TAN in das System eingegeben hat, kann er auf die Daten des betreffenden Kunden zugreifen.

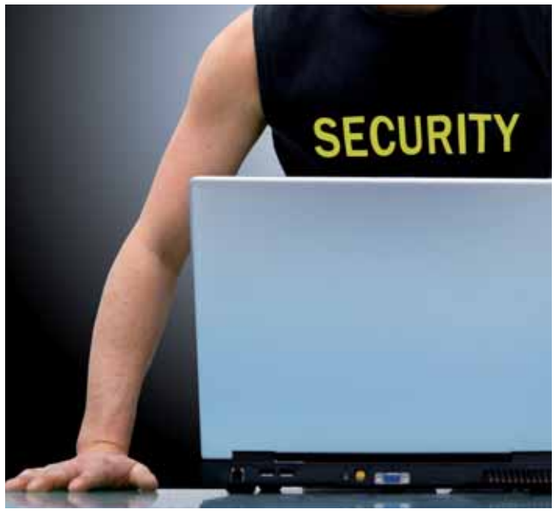
Nach seiner Einführung hat sich herausgestellt, dass das TAN-Verfahren in Einzelfällen nicht angewendet werden kann. Dies ist dann der Fall, wenn die SIM-Karte gesperrt oder das Mobiltelefon verloren wurde. Im Jahr 2009 wurde für diese Einzelfälle ein TAN-Alternativ-Verfahren eingeführt. Hierbei nennt der Kunde dem Kundenbetreuer außer seiner Rufnummer die SIM-Kartennummer, die Kundennummer oder die Kundenkontonummer. Nur nach dieser Vorgehensweise kann der Kundenbetreuer auf die Bestandsdaten des betreffenden Kunden zugreifen. Darüber hinaus erhält der Kunde eine Bestätigungs-SMS, um sicherzustellen, dass keine unzulässigen Bestellungen oder Änderungen vorgenommen werden. Um das TAN-Alternativ-Verfahren auf Einzelfälle zu beschränken, dürfen die Telekom Shops jeweils nur einen festgelegten Prozentsatz von Kunden über dieses Verfahren betreuen.

T-Home Entertain: Datenlieferung der Set-Top-Boxen.
Das für T-Home Entertain verwendete Empfangsgerät, die Set-Top-Box, ist an das Internet angeschlossen. Über den Internetanschluss liefert die Deutsche Telekom die vom Kunden gewünschten Fernsehprogramme und Videos an die Set-Top-Box.

Neben den notwendigen Betriebsdaten, die für die Inanspruchnahme der Dienste von T-Home Entertain erforderlich sind, erfasste die Set-Top-Box für statistische Zwecke (Einschaltquote) auch die Nutzungsdaten des Kunden, also den Zeitpunkt, den Zeitraum und den Inhalt der jeweiligen TV-Nutzung.

Die Nutzungsdaten wurden an einen zentralen Server übermittelt und anschließend für die statistischen Auswertungen anonymisiert. Dieses Verfahren wurde vom Konzerndatenschutz bemängelt, da die Anonymisierung zu einem möglichst frühen Zeitpunkt erfolgen sollte. In der Folge wurden das Erheben und die Übermittlung der Daten vollständig eingestellt. Derzeit werden Verfahren geprüft, die eine möglichst frühzeitige Anonymisierung oder starke Pseudonymisierung der Daten ermöglichen. Ebenso werden Einwilligungsmodelle besprochen, die eine Übermittlung für Zwecke von Zusatzdiensten erlauben.

SMS zur Inverssuche bei T-Mobile.
Bei einer Inverssuche nennt die Telefonauskunft den zu einer Rufnummer gehörenden Namen eines Teilnehmers. T-Mobile Deutschland hatte die Inverssuche in der Vergangenheit nicht unterstützt und ihre Kunden daher nicht über die Möglichkeit dieser Suche informiert. Dementsprechend nutzte T-Mobile Deutschland auch keine Kundendaten für die Inverssuche oder übermittelte sie an Anbieter von Auskunftsdiensten. Diese Praxis entsprach der im Markt weit verbreiteten Auffassung, dass der die Inverssuche regelnde § 105 Absatz 3 Telekommunikationsgesetz allein das Recht, aber nicht die Pflicht der Dienstleister enthalte, die Möglichkeiten der Inverssuche zu nutzen. In einem Urteil vom Juli 2007 hat der Bundesgerichtshof allerdings eine abweichende Auslegung der entsprechenden Vorschriften des Telekommunikationsgesetzes zugrunde gelegt. Zum Schutz des Geschäftsmodells der Anbieter von Auskunftsdiensten sind – entgegen dem Wortlaut des § 105 Absatz 3 Telekommunikationsgesetz – Telekommunikationsdiensteanbieter verpflichtet, Anbietern von Auskunftsdiensten ihre Kundendaten für die Inverssuche zur Verfügung zu stellen. Das Urteil wirkt zwar unmittelbar nur zwischen den betroffenen Streitparteien, also nicht gegenüber T-Mobile, jedoch hat sich T-Mobile entschlossen, entsprechend dem Urteil des Bundesgerichtshofs die Inverssuche zu ermöglichen.



Die im Telekommunikationsgesetz festgelegten Beschränkungen zur Verarbeitung von Bestands- und Verkehrsdaten in Drittstaaten sind aus Sicht der Deutschen Telekom überarbeitungsbedürftig.

Im Juni 2009 setzte T-Mobile die Inverssuche technisch um. Als Voraussetzung musste T-Mobile die betroffenen Kunden über die neue Suche informieren und sie insbesondere auf ihr Recht hinweisen, der Freigabe ihrer Daten für die Inverssuche zu widersprechen. Im Juni 2009 verschickte T-Mobile an rund 900 000 Kunden, die bereits auf eigenen Wunsch im Telefonbuch eingetragen waren, eine SMS. Hierin wies das Unternehmen auf die Inverssuche und die damit verbundene Datenspeicherung, sowie die Möglichkeit zum Widerspruch hin. Die SMS führte zu einer geringen Anzahl von Nachfragen durch Journalisten und Kunden. Die Datenschutzorganisation und die Kundenbetreuung informierten die Betroffenen ausführlich über die Hintergründe und Notwendigkeiten der Aktion. Die Erläuterungen wurden positiv aufgenommen. Nachhaltige Beschwerden gab es nicht.

Unerwünschter Telefonverzeichniseintrag.
Durch einen Hinweis des Bundesdatenschutzbeauftragten wurde die Deutsche Telekom darauf aufmerksam, dass bei einem Produktwechsel durch Kunden ein Telefonverzeichniseintrag gegen ihren Willen vorgenommen worden war. Die Recherche des Konzerndatenschutzes ergab, dass dies auf die Einspielung von rund 720 000 fehlerhaften Datensätzen über zwei Wochen hinweg in ein System zurückzuführen war, das die Verzeichniseinträge vornimmt. Der Fehler wurde auf Veranlassung des Konzerndatenschutzes behoben.

Vivento Customer Services.
Das Fraunhofer-Institut prüfte im Auftrag des Deutschen Telekom Kundenservice (DTKS) alle internen und externen Dienstleister, die im Rahmen einer Auftragsdatenverarbeitung für den DTKS tätig sind. Am 3. Februar 2009 wurde ein Audit bei der Vivento Customer Services (VCS), einer Tochter der Deutschen Telekom, durchgeführt. Dabei diskutierte das Fraunhofer-Institut mit VCS-Mitarbeitern Sachverhalte zu Organisation, Personal, Informationssicherheit und Unterweisungen. Das Fraunhofer-Institut bescheinigte VCS, die Anforderungen an die Auftragsdatenverarbeitung zu erfüllen. Im Abschlussbericht hob das Institut insbesondere die Einbindung des Konzerndatenschutzes in die Abnahme neuer oder geänderter Software positiv hervor. Daneben würdigte es die klaren Zuständigkeiten, eine gute Prozessdokumentation, den hohen Organisationsgrad des fünf Jahre alten „Start-ups“ sowie die erfolgreich erprobte Einrichtung eines Sicherheitsmanagements mit regionalen Sicherheitsmanagern.

Regelungs- und Handlungsbedarfe.

Überarbeitung des Bundesdatenschutzgesetzes.
Der Koalitionsvertrag der Bundesregierung von Oktober 2009 schreibt eine leichtere Verständlichkeit und Lesbarkeit des Bundesdatenschutzgesetzes fest. Die Deutsche Telekom begrüßt dieses Vorhaben. Die Regelungen zur werblichen Nutzung von Daten waren bereits vor der Novellierung des Bundesdatenschutzgesetzes sehr umfangreich. Mit der Novellierung vom September 2009 sind neue Regelungen und Differenzierungen hinzugekommen, die eine rechtssichere Beurteilung der verschiedenen Sachverhalte erschweren.

Überprüfung von Sonderregelungen für die Telekommunikationsbranche.
Die im Telekommunikationsgesetz festgelegten Beschränkungen zur Verarbeitung von Bestands- und Verkehrsdaten in Drittstaaten sind aus Sicht der Deutschen Telekom überarbeitungsbedürftig. Die Regelung in § 92 Telekommunikationsgesetz untersagt die Verarbeitung von Telekommunikationsdaten im Ausland mit wenigen Ausnahmen.
Verkehrsdaten der Telekommunikation sind besonders sensible Daten. Dies rechtfertigt in den Augen der Deutschen Telekom jedoch die starke Einschränkung der Datenverarbeitung in Drittstaaten über die Regelung des § 92 Telekommunikationsgesetz nicht, wenn vor Ort ein angemessenes Datenschutzniveau gegeben ist. Im Rahmen einer Neuregelung könnten bei Telekommunikationsdaten höhere Anforderungen gestellt werden als in anderen Wirtschaftsbereichen.

Ein Unternehmen wie die Deutsche Telekom ist für die Wartung und den Service für seine in Deutschland betriebenen Rechenzentren auf international agierende Unternehmen angewiesen, die die Wartungsaufgaben auf ihre weltweiten Niederlassungen nach dem „Follow-the-Sun-Prinzip“ verteilen. Dies bedeutet auf Deutschland bezogen, dass die Wartung morgens aus Asien, mittags aus Europa und abends aus den amerikanischen Ländern erfolgt. Die aktuelle gesetzliche Regelung verhindert eine solch globale, preisgünstige Wartung, da Unterstützungsleistungen in vielen Fällen notwendig auch den Blick auf Daten erfordern. So muss die Deutsche Telekom zusätzliche Ressourcen für einen Drei-Schicht-Betrieb in Europa aufbauen.

Datenschutzauditgesetz.
Im Rahmen der Novellierung des Bundesdatenschutzgesetzes ist es im Jahr 2009 nicht zum Erlass eines eigenständigen Datenschutzauditgesetzes gekommen. Die Deutsche Telekom hält ein solches Gesetz, das das Verfahren und die Rahmenbedingungen von Datenschutzauditierungen in Unternehmen regelt, für dringend erforderlich. Die Regierungskoalition hat nun eine eigenständige Stiftung Datenschutz angekündigt, die zur Aufgabe haben soll, eigenständig und neutral die Datenschutzkonformität von Produkten und Dienstleistungen zu prüfen und zu bewerten. Dies begrüßt die Deutsche Telekom ausdrücklich. Es muss jedoch sichergestellt werden, dass Datenschutzprüfungen künftig auf einheitlichen und verlässlichen Standards aufsetzen, um die vertrauensbildende Wirkung von Prüfsiegeln nicht zu verlieren. Gerade im Kundenkontakt ist die extern bestätigte Datenschutzkonformität ein wichtiges Mittel, um das Kundenvertrauen nachhaltig zu gewinnen.

Gerade im Kundenkontakt ist die extern bestätigte Datenschutzkonformität ein wichtiges Mittel, um das Kundenvertrauen nachhaltig zu gewinnen.

Status Datenschutz bei Geschäftskunden und Großprojekten.

Projekte aus dem Jahr 2009.

De-Mail.
Mit der Kommunikationslösung De-Mail, die T-Systems gemeinsam mit Partnerunternehmen wie United Internet und dem Bundesministerium des Innern entwickelt hat, lassen sich elektronische Nachrichten rechtsverbindlich, vertraulich und fälschungssicher versenden. Voraussetzung dafür ist, dass Sender und Empfänger sich eindeutig identifizieren. Um den Versand und die Zustellung einer De-Mail nachzuweisen, erhält der Nutzer vom Provider außerdem eine rechtsverbindliche Bestätigung. Von Oktober 2009 bis März 2010 wird De-Mail in der T-City Friedrichshafen, der „Zukunftswerkstatt“ der Deutschen Telekom, in einem Pilotprojekt getestet. Nach erfolgreicher Pilotphase plant die Deutsche Telekom, das Produkt bundesweit einzuführen.

Der Konzerndatenschutz hat das Projekt in Friedrichshafen begleitet. Ein Datenschutzkonzept, das im Entwurf des zugrunde liegenden Bürgerportalgesetzes gefordert ist, hat der Konzerndatenschutz geprüft und freigegeben.

Elektronische Gesundheitskarte/Elektronische Patientenakte.
Elektronische Gesundheitskarten sollen in Zukunft die bisherigen Krankenversichertenkarten ablösen und als Zugangsschlüssel zu verschiedenen Anwendungen im Gesundheitswesen dienen. Versicherte, niedergelassene Ärzte und Krankenhäuser sollen künftig gemeinsam auf zentral gespeicherte Patientenakten zugreifen können.

T-Systems hat mit Unterstützung von Datenschutz- und Datensicherheitsexperten der Deutschen Telekom ein entsprechendes System entwickelt. Der Abruf der Patientendaten setzt voraus, dass sich der Patient mit seiner elektronischen Gesundheitskarte und seiner PIN und der Arzt sich mit seinem elektronischen Heilberufsausweis identifiziert. Um eine Verbindung zum Server der elektronischen Patientenakte herstellen zu können, wird zudem eine spezielle Hardware, ein sog. Konnektor, benötigt. Ein Zugriff vom PC zu Hause ist somit nicht möglich. Patienten können an Selbstbedienungsstationen in Krankenhäusern oder bei Ärzten ihre Patientendaten einsehen.

Mit der elektronischen Gesundheitskarte wird erstmals die Verfügungshoheit über die eigene Akte vom Arzt auf den Patienten übertragen. Der Patient kann damit einem neuen Arzt Zugriff auf seine Akte gewähren, ohne den bisher behandelnden Arzt um deren Herausgabe bitten zu müssen.

Neuer (elektronischer) Personalausweis.
Im November 2010 soll ein neuer Personalausweis flächendeckend in Deutschland eingeführt werden. Damit erhält jeder Bürger – entweder im Regeltausch oder auf freiwilliger Basis – ab 16 Jahren einen Personalausweis, der die Größe einer Scheckkarte hat.

Dieser neue Personalausweis ist mit einem sog. RFID-Chip (Radio Frequency Identification, zu Deutsch: Identifizierung mit Hilfe von elektromagnetischen Wellen) ausgestattet. Der Chip speichert Daten, kann ver- und entschlüsseln und ermöglicht alle notwendigen Prozesse zur Behandlung und Nutzung von Zertifikaten. Der neue Personalausweis ermöglicht zudem eine elektronische Signatur. Als Resultat der öffentlichen Diskussion in Deutschland wird ein biometrischer Fingerabdruck nur noch auf Wunsch des Bürgers, jedoch nicht mehr zwingend erfasst. Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik werden keine Daten zentral gespeichert. Weiterhin werden nur die Daten, die in gedruckter Form auf dem Ausweis vermerkt sind, dezentral von den Ausweisbehörden erfasst.

Bei der Entwicklung des neuen Personalausweises wurde T-Systems von Datensicherheits- und Datenschutzexperten der Deutschen Telekom begleitet. Um sicherzustellen, dass nur diejenigen Daten auslesen können, die daran ein berechtigtes Interesse haben, sind die Daten auf der Karte verschlüsselt abgelegt. Jeder Dienste- oder Serviceanbieter, der entsprechende Daten auslesen können muss, erhält vorab von einer zentralen Stelle ein Berechtigungszertifikat, das beschränkt ist auf die gesetzlich zulässigen Verwendungszwecke. Wer diese zentrale Stelle zur Ausgabe und Verwaltung der Berechtigungszertifikate (Berechtigungsdienst und Sperrdienst) sein wird, wird aktuell diskutiert. Das Berechtigungszertifikat und die angeforderten Daten, eingeteilt in notwendige und freiwillige Angaben, werden dem Ausweisinhaber beim Einsatz seines Ausweises angezeigt. Freigegeben werden die Daten vom Ausweisinhaber durch seine aktive Bestätigung und Eingabe einer nur ihm bekannten sechsstelligen PIN. Nach einer dreimaligen falschen PIN-Eingabe werden die Funktionen des Ausweises gesperrt.

Beim Cloud Computing erfolgen Datenverarbeitung und Diensterbringung nicht mehr auf den Computern der Nutzer, sondern über einen Netzservice, auf den die Nutzer von ihren jeweiligen Endgeräten aus Zugriff haben.

Regelungs- und Handlungsbedarfe.

Umsetzung neuer Beratungsmodelle und Herangehensweisen des Konzerndatenschutzes im Geschäftskunden- und Produktentwicklungsbereich.
Ein wichtiger Baustein der Aktivitäten des Konzerndatenschutzes ist künftig die Neugestaltung des Beratungsgeschäfts bei Großprojekten. Großkunden fragen vermehrt Datenschutz- und Datensicherheitslösungen nach. Dafür werden in Zukunft die bereits für den Privatkundenmarkt und den Mitarbeiter-Datenschutz eingeführten, stärker standardisierten Prüfungsprozesse angewandt, was eine noch stärkere fachliche Einbindung der Vertriebsmitarbeiter erfordert. Hierdurch wird gewährleistet, dass Großkunden kompetente datenschutzrechtliche Beratung vom ersten Kontakt an erhalten. Auch im Produktbereich, in dem neue Dienste und Geschäftsmodelle für den Konzern entwickelt werden, wird künftig stärker über standardisierte Vorgaben beraten.

Cloud Computing.
Nachdem die technischen Voraussetzungen geschaffen wurden, ist das sog. Cloud Computing verstärkt in den Fokus des Konzerndatenschutzes gerückt. Beim Cloud Computing erfolgen Datenverarbeitung und Diensterbringung nicht mehr auf den Computern der Nutzer, sondern über einen Netzservice, auf den die Nutzer von ihren jeweiligen – ggf. mobilen – Endgeräten aus Zugriff haben. Als eine wichtige technische Voraussetzung musste die Deutsche Telekom zunächst Datenübermittlungen mit entsprechend hohen Datenübertragungsraten auch von mobilen Endgeräten aus ermöglichen. Nur so können den Kunden zufriedenstellende Laufzeiten für einen Geschäftsvorgang angeboten werden. Das Unternehmen muss eine Vielzahl weiterer technischer Rahmenbedingungen schaffen, die intensiver datenschutzrechtlicher Betreuung bedürfen.

Status Internationaler Datenschutz.

Der internationale Datenschutz vor neuen Herausforderungen.
In den vergangenen Jahren hat die Tendenz, persönliche Daten länderübergreifend zu verarbeiten, weiter zugenommen: Durch global agierende Unternehmen wachsen die Märkte weiter zusammen. Gleichzeitig sind die Kunden selbst dynamischer und fordern von ihren Dienstleistern globale Interaktion.

Diese Marktentwicklung macht einen angemessenen, länderübergreifenden Datenschutz nötig. In Deutschland und der Europäischen Union werden die Rahmenbedingungen zur Nutzung persönlicher Daten immer weiter ausgestaltet, außerhalb der Union verfolgen die Länder eine andere Datenschutzpolitik. Ein homogener internationaler Datenschutz existiert derzeit nicht – ein Zustand, den internationale Datenschutzexperten bemängeln. Bei der 31. Internationalen Datenschutzkonferenz vom 4. bis 6. November 2009 in Madrid haben mehr als 1 000 Vertreter von Unternehmen und Organisationen aus über 80 Ländern mit dem „International Standard on the Protection of Personal Data and Privacy“ ein Papier erarbeitet, das für die Schaffung von internationalen Datenschutzstandards ein wichtiger Schritt ist. Für international agierende Unternehmen sind die Initiativen der Politik, einen einheitlichen Datenschutzstandard auch international zu erreichen, von großer Bedeutung.

Perspektive aus dem Datenschutzbeirat.

Frage
an Prof. Dr. Hansjörg Geiger,
Honorarprofessor für Verfassungsrecht an der Johann-Wolfgang-Goethe-Universität, Frankfurt, Staatssekretär im Bundesministerium der Justiz (1998 bis 2005)

Unter welchen Voraussetzungen sollen Online-Durchsuchungen erlaubt sein?
Artikel 1 Absatz 1 des Grundgesetzes betont, dass die Menschenwürde unantastbar ist. Daraus leitet das Bundesverfassungsgericht einen „Kernbereich privater Lebensgestaltung“ ab, in den nicht eingegriffen werden darf und der auch jeder Abwägung mit noch so wichtigen anderen Gütern entzogen ist. Das allgemeine Persönlichkeitsrecht nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz umfasst auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Eine Online-Durchsuchung ist eine heimliche Maßnahme, die einen besonders schwerwiegenden Eingriff in Grundrechte darstellt. Es besteht die allgemeine Vermutung, dass auf einem privaten „informationstechnischen System“ viele sensible personenbezogene Daten gespeichert sind. Die Gesamtschau der auf einem solchen informationstechnischen System gespeicherten Daten ermöglicht auch nach der Beurteilung des Bundesverfassungsgerichts wegen des potenziell äußerst großen und aussagekräftigen Datenbestands weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zur möglichen Bildung von Verhaltensprofilen. Die Informationen, die auf einem privat genutzten Computer gespeichert sind, und die Rückschlüsse auf persönliche Interessen, die sich aus der Nutzung des Computers als Mittel zur Kommunikation und zur Informationsgewinnung im Netz zum Teil ergeben, können den Kernbereich privater Lebensgestaltung berühren.

Daraus folgt, dass eine Online-Durchsuchung nur dann mit dem Grundgesetz vereinbar sein kann, wenn sichergestellt ist, dass dieser Kernbereich privater Lebensgestaltung und damit die Menschenwürde des von einer solchen Durchsuchung Betroffenen nicht verletzt wird.

Selbst eine Online-Durchsuchung, die diesen Kernbereich wahrt, darf nicht unverhältnismäßig in die Rechte des Betroffenen eingreifen. Es gilt zu beachten, dass „Sicherheit“ nie alleiniger Maßstab sein darf für die Zulässigkeit von schwerwiegenden Grundrechtseingriffen. Vielmehr ist stets die vom Grundgesetz gebotene Balance zwischen Freiheit und Sicherheit zu wahren. Das bedeutet, dass eine Online-Durchsuchung überhaupt nur in Betracht zu ziehen ist, wenn es um den Schutz für überragend wichtige Güter wie etwa Leben von Personen oder den Bestand des Staates geht.

Der Gesetzgeber selbst hat auch die erforderlichen verfahrensrechtlichen Vorkehrungen anzuordnen, um Eingriffe in den Kernbereich privater Lebensgestaltung sowie unverhältnismäßige Maßnahmen zu verhindern. Übrigens wäre auch eine Online-Durchsuchung, die das informationstechnische System eines unbeteiligten Dritten, also eines Nichtstörers, erfasste, nicht verhältnismäßig. Gerade auch der Ausschluss derartiger Nichtstörer verlangt intensive Vorermittlungen, die der Gesetzgeber im Rahmen der notwendigen Vorkehrungen zum Schutz Unbeteiligter treffen muss. Außerdem ist auch die grundrechtlich verbürgte Unverletzlichkeit der Wohnung zu achten. Schließlich hat der Gesetzgeber die Voraussetzungen für eine effektive richterliche Kontrolle zu regeln und für eine angemessene Unterrichtung des Betroffenen Sorge zu tragen.

Internationaler Datenschutz bei der Deutschen Telekom.
Die Deutsche Telekom, die in weltweit 50 Ländern vertreten ist, hat aufgrund der fehlenden internationalen Standards zum Datenschutz mit dem Privacy Code of Conduct eine eigene Grundlage für den internationalen Datenschutz geschaffen. Diese stellt bei der Muttergesellschaft und ihren Töchtern weltweit eindeutige Rahmenbedingungen und eine klare organisatorische Struktur mit verbindlichen Verantwortungen zum Datenschutz auf.

Zur Unterstützung der internationalen Aktivitäten der Deutschen Telekom fördert und koordiniert der Konzerndatenschutz den Aufbau eines internationalen Netzwerks von Datenschutzexperten. Auf internationaler Ebene tragen Datenschutzbeauftragte die Verantwortung für den Datenschutz in ihrer Landesgesellschaft. Sie kümmern sich um die Implementierung, Umsetzung und Einhaltung des Privacy Code of Conduct. Darüber hinaus beraten und begleiten sie Projektteams bei datenschutzrelevanten Projekten und berichten sowohl regulär als auch bei Vorfällen an den Konzerndatenschutz der Deutschen Telekom.

Auch im Jahr 2009 führte der Konzerndatenschutz der Deutschen Telekom Audits in den Ländergesellschaften durch, um die lokale Umsetzung der Datenschutzvorgaben zu prüfen und zu unterstützen. Ferner stehen der Konzerndatenschutz und die lokalen Datenschutzbeauftragten den Landesgesellschaften sowohl auf rechtlicher als auch technischer Ebene bei allen Datenschutzfragestellungen zur Verfügung.

Die Erfahrungen in der Zusammenarbeit von Muttergesellschaft und den Tochtergesellschaften der Deutschen Telekom haben gezeigt, dass zur nachhaltigen Sicherung des Datenschutzniveaus die weitere Verstärkung der internationalen Kooperation sinnvoll ist.

Internationale Projekte aus dem Jahr 2009.

Projekt „Internationalisierung Datenschutz, Recht und Compliance“.
Mit dem Projekt „Internationalisierung Datenschutz, Recht und Compliance“ hat der Vorstandsbereich Datenschutz, Recht und Compliance die Zusammenarbeit mit den Landesgesellschaften der Deutschen Telekom in den Mittelpunkt gestellt. Beim Datenschutz wird auf der durch den Konzerndatenschutz koordinierten internationalen Datenschutzorganisation aufgebaut.

Perspektive aus dem Datenschutzbeirat.

Frage
an Prof. Peter Gola,
Vorsitzender des Vorstands der Gesellschaft für Datenschutz und Datensicherheit

Immer mehr persönliche Daten werden elektronisch gespeichert. Wie sicher kann eine solche Speicherung überhaupt sein?
Eine absolute Sicherheit wird sich – wie generell beim Einsatz von Technik – nicht erreichen lassen. Der Sicherheitsstandard muss durch die vom Gesetzgeber vorgegebenen und weiterzuentwickelnden Kriterien jeweils auf einem derartigen Level sein, dass ein ggf. noch bestehendes Gefährdungsrisiko hingenommen werden kann. Maßgebend ist das Verhältnismäßigkeitsprinzip.

Internationales Datenschutzhandbuch.
Mit der Erstellung des Datenschutzhandbuchs „International Manual Data Protection at Companies of the Deutsche Telekom Group“ wurde neben dem Privacy Code of Conduct eine weitere Grundlage geschaffen, um die Internationalisierung des Datenschutzes im Konzern zu unterstützen. Im Datenschutzhandbuch finden sich Informationen zur Umsetzung von Konzerndatenschutzstandards in den Tochtergesellschaften. Daneben beinhaltet es Schulungsprogramme und Unterstützung zu internationalen Fragestellungen.

Begleitung internationaler Projekte.
Die zunehmende Internationalität der Projekte führt zu stetig steigendem Beratungsbedarf im internationalen Datenschutz. Der Konzerndatenschutz hat eine Vielzahl von Projekten im Kunden- und Personaldatenschutz begleitet. Zugenommen haben auch die Anfragen zur Unterstützung bei Großaufträgen der T-Systems International GmbH. Multinationale Konzerne verlangen als Kunden nach multinationalen Lösungen, die die Deutsche Telekom datenschutzrechtlich begleiten muss. Auch den Erwerb von Anteilen an ausländischen Telekommunikationsgesellschaften hat der Konzerndatenschutz im Jahr 2009 unterstützt. Die Landesgesellschaften wenden sich mit immer mehr Anfragen und komplexen Fällen von länderübergreifenden Vereinbarungen zur Verarbeitung von Auftragsdaten an die Muttergesellschaft. Diese Entwicklung macht den allgemeinen Trend zur Internationalisierung deutlich und fordert eine eingehende Betreuung bei grenzüberschreitenden Datenschutzfragen.

Internationale Auditierungen.
Der Konzerndatenschutz der Deutschen Telekom führt Datenschutzaudits in den Ländergesellschaften durch, um die lokale Umsetzung der Datenschutzvorgaben des Privacy Code of Conduct zu unterstützen. Im Rahmen des internationalen Basisdatenschutzaudits nehmen die teilnehmenden Gesellschaften im Rahmen einer Selbstauskunft Stellung zu ihrer Konformität zum Privacy Code of Conduct. Im Jahr 2009 nahmen unter anderen Spanien, Ungarn, Großbritannien, Österreich und die Niederlande sowie außerhalb der EU die USA, Mexiko, Südafrika und Japan an diesen Basisdatenschutzaudits teil. Im Jahr 2010 wird anhand mehrerer Stichprobenkontrollen, sog. Spottests, die Umsetzung vor Ort überprüft werden.

Regelungs- und Handlungsbedarfe.
Durch die Verflechtung unterschiedlicher Technologien und die Weiterentwicklung des Internets zu einer globalen, sozialen Kommunikationsplattform steht der Datenschutz vor immer komplexeren Herausforderungen. Eine Schaffung von internationalen Datenschutzstandards ist also unabdingbar. Die Deutsche Telekom als global agierendes Telekommunikationsunternehmen wird sich auch in der Zukunft diesen Herausforderungen stellen und eigene internationale Datenschutzstandards gemeinsam mit ihren Landesgesellschaften umsetzen.

Status Zusammenarbeit mit staatlichen Stellen.

Beratungs- und Kontrollbesuche des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.
Im Jahr 2009 hat der Bundesbeauftragte für Datenschutz die Deutsche Telekom vier Mal im Rahmen von Beratungs- und Kontrollbesuchen aufgesucht. Die Besuche bezogen sich auf folgende Bereiche:

Prüfung der Verarbeitung von Verkehrsdaten bei T-Mobile Deutschland.
Schwerpunkte des dreitägigen Kontrollbesuchs bei T-Mobile Deutschland im Mai 2009 waren die Überprüfung der Verarbeitung von Verkehrsdaten im Rahmen des Abrechnungsprozesses sowie die Prüfung eines Missbrauchserkennungssystems. Der Bundesbeauftragte stellte Regelungsbedarf bei einzelnen Speicherfristen und der Protokollierung von Zugriffen auf die Verkehrsdaten fest. Die fachverantwortlichen Stellen setzen aktuell die neuen Anforderungen um. Dieser Prozess wird vom Konzerndatenschutz beratend begleitet. Auch die Aufsichtsbehörde ist in die Aufarbeitung eingebunden, um sicherzustellen, dass alle Anforderungen vollständig erfüllt werden.

Datenschutzprüfung im Call-Center.
Der Beratungs- und Kontrollbesuch im August 2009 bei einem Call-Center für den Kundenservice hatte insbesondere die technischen und organisatorischen Prozesse und Maßnahmen zum Gegenstand, die nach den gesetzlichen Regelungen in § 11 Bundesdatenschutzgesetz erforderlich sind, um bei einem Auftragsverhältnis mit externen Dienstleistern das erforderliche Datenschutzniveau und die Datensicherheit zu gewährleisten. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hatte im Hinblick auf die zum 1. September 2009 zusätzlich in Kraft getretenen Verschärfungen konkrete Anforderungen gelistet, die als Grundlage der Prüfung dienten. Er zeigte sich mit dem Ergebnis des Kontrollbesuchs zufrieden und stellte fest, dass die Deutsche Telekom seine Forderungen in den Vertragsdokumentationen umsetzt. Des Weiteren bescheinigte er dem Vertriebspartner, dass dieser die vereinbarten technischen und organisatorischen Maßnahmen einhält.

Staatliche Sonderauflagen.
Verschiedene Gesetze des Bundes und der Länder verpflichten die Telekommunikationsunternehmen, den Sicherheitsbehörden zu ermöglichen, die Telekommunikation zu überwachen sowie Auskünfte über Verkehrs- und Bestandsdaten an die Sicherheitsbehörden zu erteilen.

Die rechtliche Grundlage für die Telekommunikationsüberwachung ergibt sich aus der Strafprozessordnung und den einzelnen Landespolizeigesetzen. Eine Telekommunikationsüberwachung muss richterlich angeordnet werden.

Bei Verkehrsdaten handelt es sich um die Daten, wer, wann, mit wem mittels nachrichtentechnischer Einrichtungen kommuniziert hat. Nicht mitgeteilt werden – wie bei einer Telekommunikationsüberwachung – die Inhalte einer Telekommunikation. Anordnungsvoraussetzungen ergeben sich aus der Strafprozessordnung und den einzelnen Landespolizeigesetzen sowie für die Nachrichtendienste aus dem Bundesverfassungsschutzgesetz und den einzelnen Landesverfassungsschutzgesetzen. In der Regel bedarf es einer richterlichen Anordnung.

Bei Bestandsdaten handelt es sich um die Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Die Rechtsgrundlage für die Auskunft über Bestandsdaten findet sich im Telekommunikationsgesetz. Soweit die Auskunft für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist, bedarf es keiner richterlichen Anordnung.

Bei der Deutschen Telekom sind drei „Regionalstellen für staatliche Sonderauflagen“ in Frankfurt, Hannover und Berlin damit befasst, Auskünfte im Bereich des Festnetzes und des Internets zu erteilen. Die Stelle „Behördenauskünfte“ in Münster erteilt Auskünfte für den Mobilfunk. Eine rechtlich korrekte Erledigung der Anfragen von Sicherheitsbehörden ist nicht zuletzt deshalb zentral, weil ein Telekommunikationsunternehmen wie die Deutsche Telekom schnell in Gefahr gerät, sich selbst wegen Strafvereitelung (bei angeblich unzureichender Auskunftserteilung) oder wegen Bruch des Fernmeldegeheimnisses (bei zu „großzügiger“ Auskunftserteilung) strafbar zu machen.

Polizeiliche Auskunftsersuche.
Gemäß § 113 Absatz 1 Telekommunikationsgesetz hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, im Einzelfall den zuständigen Stellen auf deren Verlangen hin unverzüglich Auskünfte über Bestandsdaten zu erteilen, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung erforderlich ist. Die Polizei ist als Behörde, die Straftaten oder Ordnungswidrigkeiten verfolgt und die zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständig ist, zu einem Auskunftsersuchen ermächtigt. Nach einer Anordnung der Bundesnetzagentur und eines Beschlusses des Oberverwaltungsgerichts Münster sind Auskünfte über Namen und Anschrift eines mittels dynamischer IP-Adresse individualisierten Anschlussinhabers auch dann den zuständigen Stellen zu erteilen, wenn zu ihrer Ermittlung auf Verkehrsdaten zurückgegriffen werden muss.

Die Regionalstellen für staatliche Sonderauflagen der Deutschen Telekom beantworten polizeiliche Auskunftsersuche gegenwärtig auf der Grundlage dieser Vorgabe, ohne die Vorlage eines richterlichen Beschlusses zu verlangen.

Auskünfte an Inhaber von Urheber- und Leistungsschutzrechten.
Provider wie die Deutsche Telekom sind seit September 2008 verpflichtet, Inhabern von Urheber- und Leistungsschutzrechten auf Verlangen Auskunft über Kunden zu geben, die urheberrechtlich geschützte Werke in Internet-Tauschbörsen angeboten haben sollen. Der Auskunftsanspruch der Rechteinhaber geht aus dem Urheberrechtsgesetz hervor. Aufgrund des damit verbundenen Eingriffs in das Fernmeldegeheimnis muss der Rechteinhaber zuvor jedoch eine gerichtliche Erlaubnis beantragen.

In datenschutzrechtlich zulässiger Weise speichert die Deutsche Telekom die entsprechenden Daten sieben Tage lang. Innerhalb dieses Zeitraums muss die einstweilige Anordnung des Gerichts vorliegen. Das Gericht prüft, ob alle gesetzlichen Voraussetzungen für eine Auskunft vorliegen. Untersucht wird dabei, ob der Antragsteller tatsächlich Inhaber der Urheber- bzw. Leistungsschutzrechte ist, ob es sich um eine offensichtliche Urheberrechtsverletzung in gewerblichem Ausmaß handelt und ob die Ermittlung der relevanten IP-Adresse, deren Zuordnung beim Provider abgefragt werden soll, durch die Rechteinhaber ordnungsgemäß erfolgt ist. Liegen alle Voraussetzungen vor, erfolgt ein Gerichtsbeschluss, auf den hin die Deutsche Telekom die gesicherten Daten (IP-Adresse, Datum, Uhrzeit, Vorname, Nachname, Straße, Postleitzahl, Ort, Benutzerkennung) an den jeweiligen Rechteinhaber oder dessen anwaltliche Vertretung herausgibt. Nach Abschluss des Vorgangs löscht die Deutsche Telekom gemäß den gesetzlichen Vorgaben alle entsprechenden Daten.

Status Datensicherheit bei der Deutschen Telekom.

Experten unterscheiden zwischen Datenschutz und Datensicherheit. Das Bundesamt für Sicherheit in der Informationstechnik versteht unter dem Begriff Datenschutz den Schutz personenbezogener Daten vor Missbrauch durch Dritte. Mit Datensicherheit ist die Vertraulichkeit, Verfügbarkeit und Integrität von informationsverarbeitenden und informationslagernden Systemen gemeint. Ein anderer Begriff für Datensicherheit ist die Bezeichnung „Informationssicherheit“.

Bei der Deutschen Telekom sind drei Vorstandsressorts mit dem Thema Datensicherheit befasst. Der Vorstandsbereich „Datenschutz, Recht und Compliance“, der von Dr. Manfred Balz geleitet wird, legt konzernweit die Datensicherheitsstrategie sowie konkrete Regelungen zum Thema Datensicherheit fest. Das Vorstandsressort „Produktentwicklung, Technologie- und IT-Strategie“ setzt diese Sicherheitsvorgaben in technische Systeme um. Der Vorstandsbereich der Deutschland-Gesellschaft verantwortet die Überprüfung der prozessualen und technischen Sicherheitsmaßnahmen. Durch die Streuung der Datensicherheitsthemen auf drei Vorstandsbereiche ist ein Mehr-Augen-Prinzip gewährleistet. Dies trägt dem hohen Stellenwert von Datensicherheit im Unternehmen Rechnung.

Innerhalb des Vorstandsbereichs von Dr. Manfred Balz ist die Abteilung Group IT-Security für die Festlegung der Datensicherheitsstrategie und konkrete Regelungen zum Thema Datensicherheit zuständig. Leiter ist Thomas Tschersich, der seit 1995 mit Sicherheitsthemen der Deutschen Telekom betraut ist.

Datensicherheitsprojekte aus dem Jahr 2009.

Privacy and Security Assessment.
Ziel des Projekts „Privacy and Security Assessment“ war, integrierte IT-Sicherheits- und Datenschutzkonzepte sowie entsprechende Vorgaben in diesen Bereichen frühzeitig in den jeweiligen Entwicklungsprozessen des Konzerns zu verankern. Bisherige dezentrale und uneinheitliche Freigabeprozesse wurden abgelöst und ein einheitliches, standardisiertes Verfahren für IT-Sicherheit und Datenschutz in den Projekten eingeführt. So ist sichergestellt, dass nur explizit auf Sicherheits- und Datenschutzanforderungen getestete IT-Systeme und Plattformen in Betrieb gehen.

Vulnerability and Advisory Management.
Ein geringes Unsicherheitsmoment liegt in der Natur von IT-Systemen. Mit der Zeit treten neue Schwachstellen auf, die zu einem früheren Zeitpunkt noch nicht bekannt waren. Diese Situation macht es zum einen notwendig, neu entstandene Schwachstellen zeitnah zu schließen. Zum anderen muss sichergestellt werden, dass Meldungen über neue Schwachstellen von den IT-Systemverantwortlichen zeitnah bearbeitet werden können.

Über die im Jahr 2009 installierte Plattform CERT (Computer Emergency Response Team) erhalten IT-Systemverantwortliche aktuelle Sicherheitsmeldungen bezüglich ihrer Systeme und Software. Gleichzeitig wird die Behebung erkannter Schwachstellen mit hinterlegten Fristen durchgängig überwacht. Darüber hinaus etablierte die Deutsche Telekom ein zentrales IT-Abtastsystem, das in der Lage ist, innerhalb des Netzes des Konzerns sämtliche IT-Systeme nach aktuellen Schwachstellen zu durchsuchen. Dies geschieht in regelmäßigen Abständen, wobei die Systemteile, die mit besonders sensiblen Daten arbeiten, häufiger überprüft werden als andere: Die Kritikalität des Systems bestimmt die Abtastfrequenz.

Identity and Access Management (IAM)-System.
Ziel eines „Identity and Access Management“-Systems (IAM) ist es, physische Personen oder Dienste in einer Organisation eindeutig zu identifizieren. Des Weiteren kontrolliert das System den Zugriff auf Ressourcen in dieser Organisation. Ressourcen dürfen nur nach einem Genehmigungsprozess freigegeben werden. Dieser wird vom IAM-System überwacht und dokumentiert. Wenn die Gültigkeit des Ressourcenzugriffs abgelaufen ist, entzieht das IAM-System den Zugriff. Durch die Einrichtung eines zentralen IAM-Systems an Stelle der heutigen dezentralen Systeme können die Datensicherheit weiter erhöht und Kosten gesenkt werden.

Optimierung Sicherheitsrichtlinien.
Nur wenn einheitliche Sicherheitsrichtlinien im gesamten Konzern leicht angewendet werden können, geschieht dies in der Praxis auch. Die Erarbeitung von klaren, verständlichen und eindeutigen Sicherheitsrichtlinien ist das Ziel des Projekts „Optimierung Sicherheitsrichtlinien“. Die Optimierung schafft Transparenz und erhöht die Akzeptanz der Richtlinien bei den Anwendern. Dies wiederum beeinflusst die Einhaltung der Sicherheitsrichtlinien und damit die IT-Sicherheit im Ganzen positiv. Des Weiteren ermöglichen die verständlich verfassten Richtlinien Mitarbeitern von Projekten, die von den Sicherheitsrichtlinien berührt sind, Fragen zur Datensicherheit selbstständig zu klären.

Next Generation Network Security Framework.
Das Next Generation Network (NGN), das Netzwerk der nächsten Generation, ist in Zukunft die Netzinfrastruktur für Dienste wie Sprache, Daten, Video und IPTV. Es basiert auf der Technik des Internets. Dies bedeutet, dass alle Daten sämtlicher Dienste mittels des „Internet-Protokolls“ (IP) transportiert werden. Die neuartige Technologie und Architektur der zukünftigen Netzinfrastruktur bringen neuartige Risiken und Gefahren mit sich. Sie sind eine große Herausforderung für die Gewährleistung eines adäquaten Sicherheitsniveaus.

Ziel des Projekts „Next Generation Security Framework“ war es im Jahr 2009, ein generelles Rahmenwerk für die Sicherheit in einer NGN-basierten Infrastruktur zu entwerfen, das nunmehr die Basis für den Aufbau der Sicherheitsfunktionen in den nächsten Netzwerkgenerationen bildet.

Zukunft

Neue Modelle zur Datenverarbeitung stellen immer auch die Datenschützer vor neue Herausforderungen. Aktuell in der Diskussion: Cloud Computing. Dabei werden Speicherleistungen und Anwendungen nicht mehr vom privaten Computer zu Hause geleistet, sondern von einem Netzwerk von Rechenzentren in einer sog. Cloud, der Wolke. Verschiedene Wolken sind denkbar: Private Clouds, in denen nur ein Unternehmen Speicherleistungen und Anwendungen bündelt, oder öffentliche Wolken, in denen sich verschiedene Kunden die Kapazitäten teilen. Eine solche öffentliche Wolke wiederum kann sich auf verschiedene geografische Bereiche beziehen. Experten diskutieren aktuell, wie sensible Daten beim Cloud Computing optimal geschützt und gesichert werden können. Der Branchenverband der IT- und Telekommunikationsindustrie Bitkom fordert eine eigene „Cloud made in Germany“.

Interview mit Thomas Tschersich.

Welches sind die künftigen Herausforderungen an die Datensicherheit? Thomas Tschersich, Leiter IT-Sicherheit, gibt Auskunft.

Was ist Ihrer Meinung nach die größte Datensicherheitsherausforderung der kommenden Jahre?

Zweifellos die Virtualisierung von IT-Systemen, die wir gerade im Geschäftskundenumfeld sehen. Der Begriff Cloud Computing ist hierbei in aller Munde. Es geht darum, dass nicht für jede Anwendung ein einzelnes System aufgebaut wird, sondern viele „virtuelle“ Systeme auf ein und demselben Rechner installiert werden. Damit steigen die Komplexität und auch das potenzielle Sicherheitsrisiko.

Auf welches Datensicherheitsprojekt der vergangenen Jahre sind Sie besonders stolz?

Ich bin stolz darauf, dass wir es geschafft haben, unsere Vertriebspartnersysteme vom TÜV Rheinland zertifizieren zu lassen. Das war eine besondere Herausforderung, da die Zertifizierer sehr strenge Maßstäbe anlegen. Besonders stolz bin ich darauf, dass das aus vielen Einheiten des Konzerns zusammengesetzte Projektteam die Herausforderung angenommen und die Umsetzung der notwendigen Maßnahmen für eine Zertifizierung der Systeme in Rekordzeit geschafft hat.

Eines Ihrer Ziele für 2010 ist die Etablierung von einheitlichen Verfahren und Methoden für das Identitäts- und Berechtigungsmanagement. Was genau ist darunter zu verstehen?

Die Herausforderung in großen Unternehmen mit einer Vielzahl von IT-Systemen liegt darin, in all diesen Systemen unterschiedliche Benutzer und deren jeweilige Berechtigungen zu verwalten und aktuell zu halten. Benutzer wechseln innerhalb eines Unternehmens, bekommen zusätzliche Berechtigungen und müssen andere abgeben. Mit der Zeit entsteht dabei ein extrem komplexes Geflecht, das schon alleine aus Effizienzgründen enormes Optimierungspotenzial beinhaltet. Ziel für 2010 ist, gemeinsam mit der IT-Abteilung zentrale Systeme zu etablieren, über die die Benutzer verwaltet werden.

Ein weiteres Ziel ist die Etablierung von Frühwarnsystemen und Notfallreaktionsprozessen. Können Sie Beispiele für Notfälle im Bereich der Datensicherheit nennen?

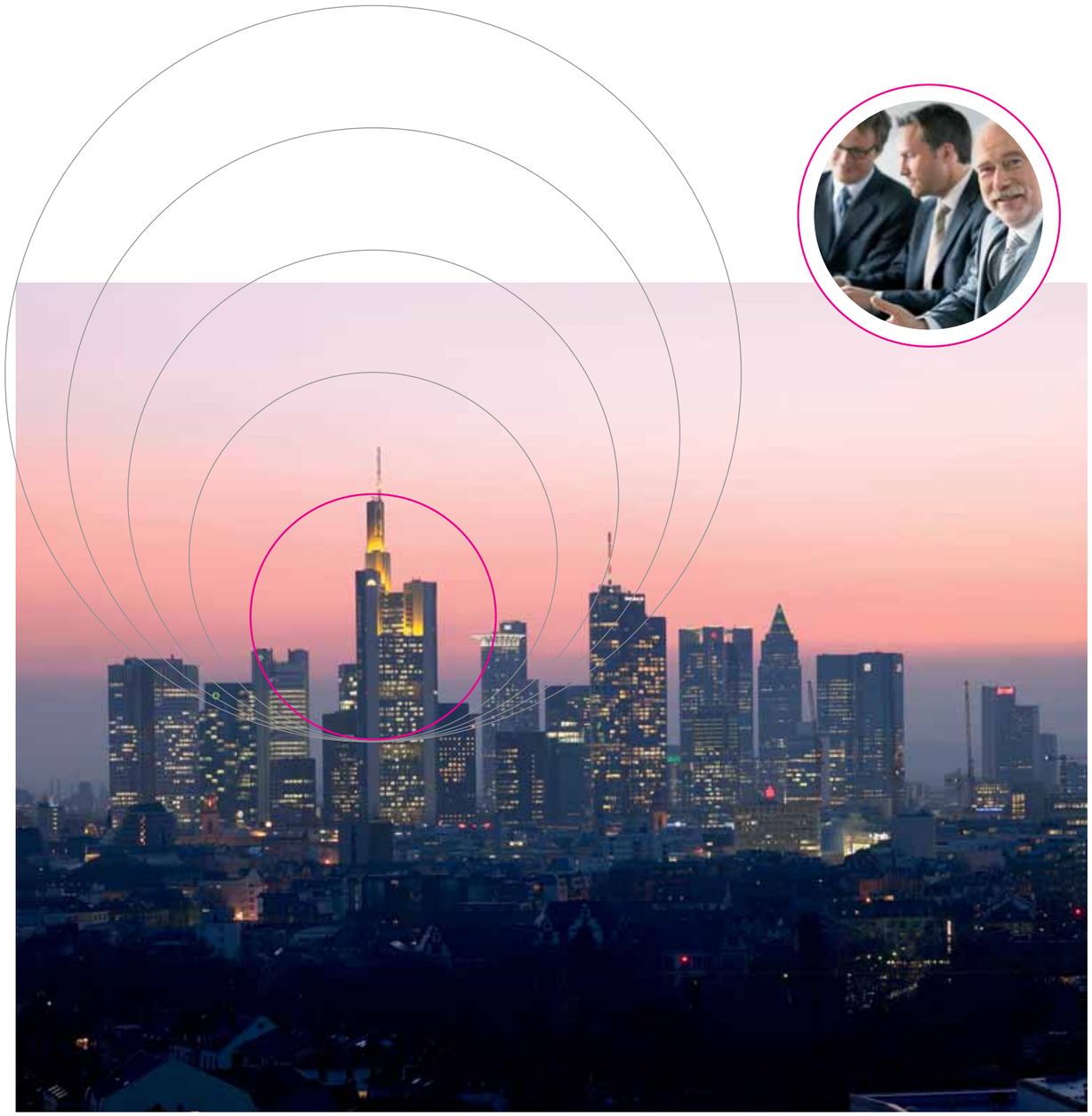
Jeder von uns kennt die Meldungen, in denen über neue Sicherheitslücken und Risiken in IT-Systemen berichtet wird. Es ist unsere Aufgabe, dafür zu sorgen, dass neu erkannte Schwachstellen nicht zum Schaden unserer Kunden ausgenutzt werden können. Insbesondere hinsichtlich der Frühwarnsysteme besteht auch bei der Deutschen Telekom noch Handlungsbedarf. Es geht darum, neue Schwachstellen so frühzeitig zu erkennen, dass sie, bevor sie von Kriminellen ausgenutzt werden können, möglichst schon geschlossen sind. Wir arbeiten hierzu auf internationaler Ebene mit den sog. „Computer Emergency Response Teams“, einer Art Feuerwehr für IT-Systeme, zusammen.

NGN bezeichnet die zukünftige Netzinfrastruktur für Dienste wie Sprache, Daten, Video und IPTV. Dabei werden alle Daten mittels des Internet-Protokolls übertragen. Welche Datensicherheitsherausforderungen sind damit verbunden?

Früher hatten wir eine Telekommunikationsinfrastruktur, die quasi in sich geschlossen war. Das Telefonnetz wurde weltweit von wenigen Unternehmen betrieben, und es gab keine offenen Schnittstellen zu anderen Systemen. In der heutigen Welt ist das anders. Alle Systeme sind miteinander über das Internet vernetzt. So vielfältig die neuen Kommunikationsmöglichkeiten sind, so vielfältig sind auch die damit verbundenen Herausforderungen, die beteiligten Systeme gegeneinander abzusichern.

Was bedeutet „Kritikalität eines IT-Systems“? Welche IT-Systeme der Deutschen Telekom haben hinsichtlich ihrer Datensicherheit eine hohe Kritikalität? Welche eine geringe?

Jedes System der Deutschen Telekom wird hinsichtlich seiner Kritikalität bewertet. Dabei geht es darum, ob in einem System besonders sensitive Daten wie beispielsweise Kundendaten verarbeitet werden. Es gilt folgendes Prinzip: Je höher die Kritikalität, also je sensibler die Inhalte in einem System, desto höher die Anforderungen, die wir an die zu treffenden Sicherheitsmaßnahmen stellen.



Experten aus Wirtschaft, Recht und Verbänden eröffnen neue Blickwinkel. Deshalb setzt die Deutsche Telekom im Bereich Datenschutz seit Anfang 2009 auf ein unabhängiges Beratergremium. Perspektivwechsel garantiert.

Datenschutzbeirat.

Der Datenschutzbeirat der Deutschen Telekom.

Im Februar 2009 wurde der Datenschutzbeirat der Deutschen Telekom gegründet. Der Beirat setzt sich mit Gestaltungsansätzen zum Datenschutz in der Telekommunikation und den Telemedien auseinander. Er erarbeitet Vorschläge zur datenschutzfreundlichen Gestaltung von Prozessen und Produkten des Konzern Deutsche Telekom und der Telekommunikationsbranche. Mit folgenden Themen befasst er sich im Detail:

- Geschäftsmodelle zur Handhabung von Kundendaten
- Geschäftsprozesse zum Umgang mit Mitarbeiterdaten
- IT-Sicherheit und Angemessenheit von Maßnahmen
- Internationale Datenverarbeitung
- Einführung neuer gesetzlicher Regelungen

Zu seinen Mitgliedern zählen führende Datenschutzexperten sowie Persönlichkeiten aus Politik, Lehre, Wirtschaft und unabhängigen Organisationen.

- Wolfgang Bosbach, MdB, Rechtsanwalt und Vorsitzender des Innenausschusses
- Dr. Michael Bürsch, MdB a. D.
- Peter Franck, Chaos Computer Club (CCC)
- Prof. Dr. Hansjörg Geiger, Honorarprofessor für Verfassungsrecht an der Johann-Wolfgang-Goethe-Universität in Frankfurt und von 1998 bis 2005 Staatssekretär im Bundesministerium der Justiz
- Prof. Peter Gola, Vorsitzender des Vorstands der Gesellschaft für Datenschutz und Datensicherheit
- Bernd H. Harder, Rechtsanwalt, Mitglied des Hauptvorstands des BITKOM e. V.
- Dr. Gerhard Schäfer, Vorsitzender Richter am Bundesgerichtshof i. R.
- Lothar Schröder, Vorsitzender des Datenschutzbeirats, Mitglied des ver.di Bundesvorstands und stellvertretender Aufsichtsratsvorsitzender der Deutschen Telekom AG
- Silke Stokar von Neuforn, MdB a. D.
- Prof. Dr. Peter Wedde, Professor für Arbeitsrecht und Recht in der Informationsgesellschaft an der Fachhochschule Frankfurt/Main

Perspektive aus dem Datenschutzbeirat.

Fragen
an Peter Franck,
Chaos Computer Club (CCC)

Warum arbeiten Sie als Hacker und Mitglied des Chaos Computer Clubs im Datenschutzbeirat der Deutschen Telekom?
Ich wurde Ende 2008 von der Deutschen Telekom zur Teilnahme am Datenschutzbeirat eingeladen. Die Entscheidung zur Teilnahme ist mir nicht leicht gefallen. Für mich war die Chance, zugunsten der Netzbürger gestaltend auf den größten deutschen Netzbetreiber zu wirken, letztlich größer als das Risiko, womöglich als „Feigenblatt“ herzuhalten.

Was kann ein Unternehmen wie die Deutsche Telekom vom Chaos Computer Club lernen?
Als Hacker hat man eine völlig andere Sicht auf Netze und Systeme. Diese kann ich im Datenschutzbeirat einbringen. Ich wünsche mir, dass die Deutsche Telekom die offene Kommunikationskultur, die das Internet hervorgebracht hat, verinnerlicht und sich an der Zukunftsdiskussion nicht nur in Form von Pressemitteilungen und Produktvorstellungen beteiligt. Das ist z. B. für den Chaos Computer Club von jeher eine Selbstverständlichkeit gewesen.

Der Datenschutzbeirat hat sich als wichtiges Beratungsgremium für die Deutsche Telekom in Sachen Datenschutz und Datensicherheit etabliert. Natürlich kann und soll er nicht sämtliche datenschutzrelevanten Vorgänge im Konzern betrachten. Nichtsdestotrotz hat er sich im vergangenen Jahr mit einer breiten Palette von Vorgängen beschäftigt.

Er befasste sich mit der Neuorganisation der Konzernsicherheit und der Neuausrichtung des Datenschutzes. Auch beriet er in der Öffentlichkeit diskutierte Themen wie Datenschutz im indirekten Vertrieb sowie Arbeitnehmerdatenschutz. Er diskutierte die Wirksamkeit der von der Deutschen Telekom ergriffenen Maßnahmen hinsichtlich eines verbesserten Datenschutzniveaus, etwa das Vier-Augen-Prinzip bei der Beauftragung externer Ermittlungsdienstleister, die konzernweite Sperrung bestimmter Dienstleister sowie den Umgang mit Anfragen von Behörden auf Datenbereitstellung. Außerdem setzte er sich mit der Vorratsdatenspeicherung und den Datenschutzaspekten von T-Home Entertain auseinander.

Die Ergebnisse der Beratungen reichen von der reinen Kenntnisnahme ohne weitere Empfehlungen, über die Bitte um detaillierte Darstellung aufgetretener Fragestellungen bis hin zu konkreten Prozessempfehlungen. Letztere wurden von der Deutschen Telekom angenommen und umgesetzt.

Die Einrichtung des Datenschutzbeirats hat sich als wirksame Maßnahme zur weiteren Verbesserung des Datenschutzes im Konzern erwiesen. Auch im Jahr 2010 rechnet die Deutsche Telekom mit zentralen Beiträgen des Beirats für den Datenschutz.

Perspektive aus dem Datenschutzbeirat.

Fragen

an Lothar Schröder,

Vorsitzender des Datenschutzbeirats, Mitglied des ver.di Bundesvorstands und stellvertretender Aufsichtsratsvorsitzender der Deutschen Telekom AG

Warum haben Sie sich entschlossen, Mitglied im Datenschutzbeirat der Deutschen Telekom zu werden?
Ich war zunächst wütend und distanziert dem Unternehmen gegenüber, weil unverantwortlich handelnde Personen mit der Bespitzelungsaffäre an der Geschäftsgrundlage des Unternehmens und meinen Persönlichkeitsrechten gekratzt haben. Dann aber hat sich bei mir die Überzeugung durchgesetzt, dass es notwendig ist, das Aufarbeiten und Aufräumen zu unterstützen, gerade weil zehntausende von Menschen im Unternehmen in Sachen Datenschutz jeden Tag einen guten Job machen und man nicht zulassen darf, dass das dummdreiste Handeln Weniger zum Schaden Aller wird. Ich habe über den Aufsichtsrat der Telekom dem Vorstand des Unternehmens empfohlen, einen Datenschutzbeirat zu gründen, um sich den Empfehlungen einer kritischen Fachwelt zu stellen. Dem ist der Vorstand gefolgt. Nachdem ich aus dem Unternehmen heraus und über die Staatsanwaltschaft vom Missbrauch meiner Telefondaten erfuhr, war es für mich selbstverständlich, im Datenschutzbeirat mitzuarbeiten, auch weil ich einmal Forschungsarbeit in Sachen Datenschutz gemacht habe.

Was waren Ihrer Meinung nach die wichtigsten Themen, über die der Datenschutzbeirat 2009 beraten hat?
Wir haben zunächst über unsere Geschäftsgrundlage geredet und klargestellt, dass wir auch von uns aus Themen aufgreifen wollen. Die Bespitzelungsaffäre kam immer wieder auf die Tagesordnung. Wir haben uns mit den Empfehlungen des Berichts der Kanzlei Oppenhoff beschäftigt, die mit einer unabhängigen Untersuchung der Bespitzelungsfälle betraut war, und viele Schritte zur Verbesserung der Datenschutzorganisation im Telekom Konzern begleitet.

Welche Themen werden 2010 im Datenschutzbeirat diskutiert?
Die Nacharbeiten zum Schäfer-Bericht werden uns beschäftigen. Der ehemalige Vorsitzende Richter am Bundesgerichtshof hat sich umfassend mit dem gesamten Datenschutz im Konzern beschäftigt. Wir haben den Datenschutz im Entertain-Paket auf die politische Tagesordnung gesetzt und wollen uns u. a. erneut mit dem kontrollierten Zugriff von Dienstleistern auf die Kundendaten der Deutschen Telekom beschäftigen. Mitte des Jahres wollen wir eine Bilanz unserer bisherigen Arbeit der Öffentlichkeit vorstellen. Gegen Ende des Jahres ist eine kritische Evaluation der eigenen Arbeit geplant.

Wann ist Ihrer Meinung nach die Arbeit des Datenschutzbeirats erledigt?
Wenn wir uns selbst überflüssig gemacht haben sollten und der Standard beim Datenschutz im Konzern so hoch ist, dass es keiner externen kritischen Reflexion mehr bedarf. Dieses Ziel zu erreichen, würde mich freuen, es würde mich aber wundern, wenn wir es angesichts des raschen technischen Fortschritts und der laufenden Anforderungsänderungen zum Datenschutz bald erreichen könnten.

Die Einrichtung des Datenschutzbeirats hat sich als wirksame Maßnahme zur weiteren Verbesserung des Datenschutzes im Konzern erwiesen. Auch im Jahr 2010 rechnet die Deutsche Telekom mit zentralen Beiträgen des Beirats für den Datenschutz.

Die technische Weiterentwicklung ist immer auch eine Herausforderung für den Datenschutz: Mitarbeiterinnen und Mitarbeiter müssen stets informiert sein über die neuen Trends. Gleichzeitig gilt es, sie weiter für den verantwortungsvollen Umgang mit Daten zu sensibilisieren. Auch in Zukunft arbeitet die Deutsche Telekom an den besten Lösungen.

Fazit und Ausblick.

Fazit und Ausblick von Dr. Claus Dieter Ulmer.

Das Jahr 2009 war wie bereits das Jahr 2008 geprägt von zahlreichen operativen und strategischen Maßnahmen, die getroffen wurden, um den Datenschutz im Konzern Deutsche Telekom weiter zu stärken. Alle bereits angestoßenen Maßnahmen sind bereits umgesetzt oder wurden konsequent weitergeführt. Die operativen Aufgaben werden allerdings mit Blick auf die organisatorischen und technischen Entwicklungen im Konzern und in der Informations- und Telekommunikationsbranche nicht weniger werden.

Auch im Jahr 2009 haben wir eine weitere Entwicklung und Festigung der Sensibilität im Umgang mit dem Datenschutz, sowohl bei unseren Mitarbeitern als auch in der Öffentlichkeit, festgestellt. Eine hohe Sensibilität für den Datenschutz macht die datenschutzrechtlichen Anforderungen besser vermittelbar und sichert ihre Umsetzung. Die Etablierung des Ressorts Datenschutz, Recht und Compliance hat die bereits mehrfach beschriebene erhöhte Wahrnehmung des Datenschutzes durch das Management im Konzern gefördert. Die Zusammenarbeit mit den im Ressort vereinigten Bereichen hat zudem dazu geführt, dass Datenschutz den Konzern operativ deutlich stärker als zuvor durchdringt.

Trotz allem dürfen die Bemühungen um die Festigung des kulturellen Wandels, der bereits eingesetzt hat, nicht nachlassen. Deshalb sind neben den notwendigen technischen und organisatorischen Maßnahmen auf allen Ebenen weitere Sensibilisierungsmaßnahmen erforderlich. In Ergänzung zu den bereits eingeführten, vielfältigen Instrumenten im Schulungs- und Informationsbereich ist für 2010 etwa konzernweit die Etablierung eines „Welcome Days“ für alle neuen Mitarbeiter im Unternehmen geplant. Hier haben die neuen Mitarbeiter die Gelegenheit, sich zu Beginn des Arbeitsverhältnisses mit den datenschutzrechtlichen Anforderungen und deren Umsetzung bei der Deutschen Telekom vertraut zu machen. Für die Datenschutzorganisation besteht ihrerseits die Möglichkeit, ihre Ansätze und Planungen transparent und ihre Organisation und Ansprechpartner bekannt zu machen.

Datenschutz spielt sich nicht nur in Deutschland ab. Die neuen Geschäftsmodelle, wie insbesondere das Cloud Computing, haben mittelfristig den internationalen Datentransfer zum Gegenstand. Beim Cloud Computing verlässt sich der Nutzer nicht mehr auf seinen Computer und die darauf aufgespielten Programme zu Hause. Er nutzt vielmehr zentrale Netzdienste, um die jeweils benötigten Anwendungen und Speicherkapazitäten zu nutzen. Dabei hat er den Vorteil, immer auf die aktuellsten Programme zugreifen zu können und durch die aktuellsten Sicherheitslösungen geschützt zu sein. Für die anbietenden Unternehmen bedeutet dies jedoch, neue Konzepte zum vertraulichen Umgang mit den Daten ihrer Kunden zu entwickeln. Für die Unternehmen, die die Daten der Kunden zukünftig in verschiedenen Rechenzentren der Welt verarbeiten wollen – nach dem durchaus nachvollziehbaren Prinzip „Wo gerade Platz ist“ –, bedeutet es, dass sie für den internationalen Bereich völlig neue Rahmenbedingungen entwickeln und einführen müssen. Hier müssen die Datenschutzorganisationen der Unternehmen rechtzeitig konzeptionelle Vorarbeit leisten. Für die Daten der Kunden soll von Tag eins eines solchen Modells an der größtmögliche Schutz gewährleistet sein.

In diesem Zusammenhang möchte ich auf die „Delphi-Studie 2030 [1)]“ verweisen. Die Studie hat Ende 2009 eine breite Diskussion über Chancen und Risiken der Informations- und Wissensgesellschaft angestoßen. Rund 550 Informationstechnologie-Experten aus Politik, Wirtschaft und Wissenschaft wurden zu den wesentlichen Entwicklungen ihrer Branchen in den kommenden 20 Jahren befragt. Die Studie verdeutlicht die ungebrochene Dynamik, mit der die Informations- und Kommunikationstechnologien die Welt verändern werden. Einige der Kernbotschaften der Zukunftsstudie sind:

1. Die Digitalisierung und die weiter zunehmende informationelle Durchdringung aller privaten und beruflichen Lebensbereiche werden die Informationsgesellschaft in Zukunft noch umfassender formen.
2. Akzeptanz und Vertrauen der Menschen im Umgang mit Informationstechnologien sind die Grundlage der Entwicklung einer modernen und offenen Informationsgesellschaft.
3. Die mobile Nutzung des Internets und seiner Dienste wird sich nachhaltig auf die Informationsgesellschaft auswirken und eigenständige neue Anwendungsfelder schaffen.

Diese Botschaften machen den Stellenwert des Datenschutzes für die zukünftigen Entwicklungen deutlich.

[1)] http://www.tns-infratest.com/presse/zukunft_Informationstechnologie.asp

Datenschutz wird weiterhin im Fokus bleiben. Sowohl in der Öffentlichkeit als auch bei der Deutschen Telekom. Die Datenschutzorganisation des Konzerns steht bereit, dieses für die Zukunft so wichtige Anliegen zu begleiten und zu stützen. Im Sinne des Leitbilds „Vertrauensräume schaffen!“

Bereits in sechs bis zehn Jahren werden im Rahmen des oben genannten Cloud Computing in Deutschland und in Europa Werkzeuge und digital vernetzte Assistenten verbreitet sein, die die Nutzer im Umgang mit ihren digitalen Daten in unterschiedlichen Nutzungskontexten unterstützen und die dem Einzelnen etwa die Verwaltung seiner (multiplen) Identitäten im Internet ermöglichen. Einen ersten Vorgeschmack von diesen Möglichkeiten haben wir in jüngster Vergangenheit mit den Kleinstapplikationen erhalten, den sog. Apps, die auf die mobilen Endgeräte aufgespielt werden können. Jede dieser Anwendungen verarbeitet in größerem oder geringerem Umfang personenbezogene Daten. Gerade auch vor diesem Hintergrund bleibt die vollständige Kontrolle des Einzelnen über die Verwendung seiner persönlichen Daten weiter ein zentrales und nach Stand der Dinge nur mit erheblichem Aufwand zu erreichendes Ziel. Die zentralen Fragestellungen im Umgang mit der digitalen Identität eines Menschen sind weltweit weder gelöst noch besteht ein abgestimmter Ansatz der beteiligten Unternehmen oder Staaten zum Umgang damit.

Auch Programme, die den Zugriff auf im Netz gespeicherte Daten über lange Zeit ermöglichen und diese zur Verfügung stellen, sind weiter ein ungelöstes Problem. Die Verfügbarkeit der Informationen für Dokumentationszwecke ist dabei nur ein Aspekt. Der andere ist die Frage, wie der Nutzer ihn betreffende Inhalte wieder aus dem Netz entfernen kann. Digitale Dokumente, die in das Netz gestellt werden, mit einem digitalen Haltbarkeitsdatum, also einem vorgesehenen Löschzeitpunkt, zu versehen, ist dabei nur eine mögliche Lösung.

Insgesamt können sich aus allen diesen Fragestellungen erhebliche wirtschaftliche Chancen, aber auch Risiken für die informationstechnologische Industrie ergeben. Letztere müssen jedoch gelöst und diese Lösungen weltweit umgesetzt werden. Es bedarf vor allem auch geeigneter Maßnahmen der IT-Sicherheit. Gemeint sind die sichere E-Signatur, sichere E-Mail-Kommunikation, die Sicherstellung von digitalen Identitäten und ein für jeden Einzelnen zuverlässiges, einfach handhabbares Identitätsmanagement. Nur so kann langfristig eine sichere und zuverlässige digitale Kommunikation zwischen Menschen wie auch zunehmend zwischen Menschen und Maschinen garantiert und das Vertrauen der Nutzer verdient werden. Natürlich können die Unternehmen diese Anstrengungen nicht alleine leisten. Insbesondere die weltweite Schaffung von anerkannten Standards muss von den gesellschaftlich relevanten Institutionen mitgetragen und vorangetrieben werden.

Neben diesen zukunftsorientierten Fragestellungen werden uns im Jahr 2010 und darüber hinaus die operativen Belange weiterhin beschäftigen. Die Begleitung der Vielzahl der im Nachgang der Datenvorfälle angestoßenen Projekte und Einzelmaßnahmen wird weiterhin einen großen Raum einnehmen. Allem voran wird der Konzerndatenschutz der Deutschen Telekom für die Kundenkontaktbereiche, also Vertrieb, Kundenservice und technischer Service, neue übergreifende, einheitliche Regelungen erstellen, die einen angemessenen Umgang mit den Daten unserer Kunden noch besser gewährleisten werden. Wir werden die Maßnahmen zur Auditierung von Vertriebspartnern unterstützen und uns gemeinsam mit den Kollegen aus der Datensicherheit noch stärker in die Entwicklungsprozesse von IT-Systemen einbringen. Ein konzernweites Projekt, das von der Compliance-Abteilung ausgeht und das den Verbraucherschutz im Fokus hat, werden wir intensiv von Datenschutzseite begleiten.

Im Bereich Arbeitnehmerdatenschutz werden wir die gesetzlichen Neuerungen, die wir im Jahr 2010 erwarten, begleiten, aufarbeiten und die Umsetzung im Konzern anstoßen. Ziel ist es auch hier, aus der Einzelregelungslandschaft der Gesellschaften zu möglichst einheitlichen Regelungen für den Gesamtkonzern zu kommen.

Nicht zuletzt steht auch die langwierige und extrem zeitintensive Umstellung der Konzern-IT-Infrastruktur und der Kommunikationsnetze auf die nächste Generation an. Auch hier erwarten wir im Jahr 2010 bereits erste wesentliche Umsetzungen, die es zu begleiten gilt.

Datenschutz wird also im Fokus bleiben. Sowohl in der Öffentlichkeit als auch bei uns. Die Datenschutzorganisation der Deutschen Telekom steht bereit, dieses für die Zukunft so wichtige Anliegen zu begleiten und zu stützen. Im Sinne des Leitbilds

„Vertrauensräume schaffen!“

ist der Konzerndatenschutz der Deutschen Telekom fest entschlossen, das Vertrauen der Kunden, der Öffentlichkeit und der Mitarbeiter zu stärken und stetig zu verbessern.

Funktionierender Datenschutz bedarf einer funktionierenden Organisation. Die Deutsche Telekom entwickelt ihren Bereich Datenschutz kontinuierlich weiter. Eng gefasste Verhaltensleitlinien geben allen Mitarbeitern Sicherheit im Umgang mit Daten.

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.

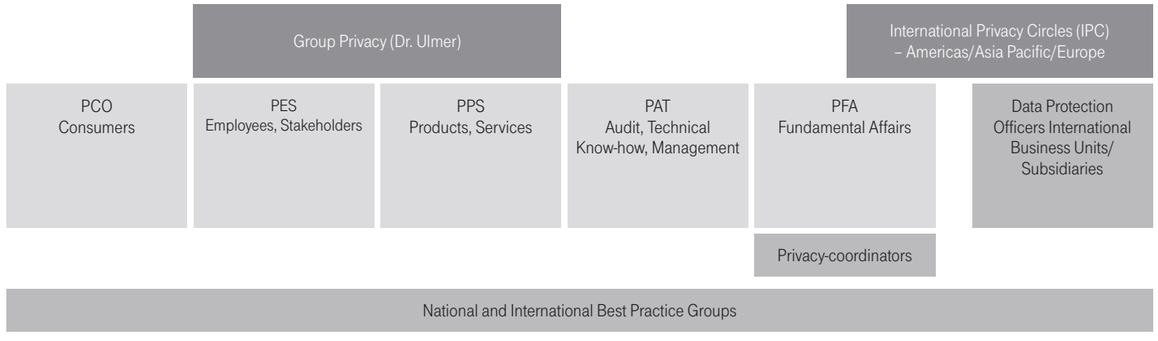
Als Datenschutzansprechpartner vor Ort sind auf Ebene der Legaleinheiten, Betriebe und sonstigen Organisationseinheiten Datenschutzschnittstellen und Datenschutzkoordinatoren installiert. Bei den internationalen Beteiligungen wird diese Funktion von den hierzu benannten „Data Protection Officers“ wahrgenommen. 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.

Die Datenschutzorganisation.



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 Datenschutzdienstleistungen 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.

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.

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 ist 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. Darüber hinaus ist 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 Grundlage 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.

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 zugrunde liegenden 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 ist 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 darf 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 Direktmarketings 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, des Zwecks der Verarbeitung und der 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
Datenschutzorganisation 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 ggf. 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.

Glossar.

Audit. Audits sind Untersuchungsverfahren, die bewerten, ob und wie weit Anforderungen und Richtlinien erfüllt werden. Speziell geschulte Auditoren führen die Audits durch.

Awareness. Awareness (englisch: Bewusstsein) bezeichnet im Datenschutz das Verantwortungsbewusstsein beim Umgang mit Daten durch die Mitarbeiter eines Unternehmens.

Bilanzrechtsmodernisierungsgesetz (BilMoG). Das Gesetz zur Modernisierung des Bilanzrechts ist ein deutsches Gesetz zur Reform des Bilanzrechts.

Bundesdatenschutzgesetz (BDSG). Das deutsche Bundesdatenschutzgesetz regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischeren Regelungen den Umgang mit personenbezogenen Daten, die in IT-Systemen oder manuell verarbeitet werden. Es wurde zuletzt im Jahr 2009 novelliert.

Cloud Computing. Beim Cloud Computing erfolgen Datenverarbeitung und Diensterbringung nicht mehr auf den Computern der Nutzer, sondern über einen Netzservice, auf den die Nutzer von ihren jeweiligen – ggf. mobilen – Endgeräten aus Zugriff haben. Die Anwendungen und Daten befinden sich nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der (metaphorischen) Wolke (englisch: Cloud).

Company Level Controls (CLC). Company Level Controls sind konzernweite Prüfkriterien und Prüfungen, die sich aus dem so genannten Sarbanes-Oxley Act (S-OX) und dem Bilanzrechtsmodernisierungsgesetz (BilMoG) ableiten.

Compliance. Compliance bedeutet die Einhaltung von Verhaltenskodizes und die Erfüllung von Gesetzen, Standards und internen Richtlinien. Dadurch sollen materielle und immaterielle Schäden von den Unternehmen und ihren Mitarbeitern abgewendet werden.

Computer Emergency Response Team (CERT). Sicherheits- und Computer-Notfallteam.

e-Learning. Alle Formen von Lernen, bei denen elektronische oder digitale Medien für die Präsentation und Distribution von Lernmaterialien oder zur Unterstützung zwischenmenschlicher Kommunikation eingesetzt werden.

Internationale Organisation für Normung (ISO). Die Internationale Organisation für Normung erarbeitet internationale Normen in vielen Bereichen. Ausnahmen: Elektrik und Elektronik, für die die Internationale elektrotechnische Kommission (IEC) zuständig ist, sowie Telekommunikation, für die die Internationale Fernmeldeunion (ITU) zuständig ist. Gemeinsam bilden die drei Organisationen die WSC (World Standards Cooperation).

IP-Adresse. Adresse in Computernetzen, die auf dem Internet-Protokoll (IP) basieren. Sie wird Geräten zugewiesen, die an das Netz angebunden sind, und macht die Geräte so adressierbar und damit erreichbar.

Location Based Services (LBS). Location Based Services (deutsch: standortbezogene Dienste) stellen einem Nutzer ortsbezogene Informationen über ein mobiles Gerät zur Verfügung.

Nearshore. Aus mitteleuropäischer Perspektive: Verlagerung von Prozessen und Funktionen eines Unternehmens in osteuropäische Länder.

Offshore. Aus mitteleuropäischer Perspektive: Verlagerung von Prozessen und Funktionen eines Unternehmens ins (Übersee-)Ausland.

Outbound-Call-Center. Ein Outbound-Call-Center schafft aktive Marktkontakte, ruft also Personen an. Beispiel: Direktmarketing. Demgegenüber agiert ein Inbound-Call-Center passiv, wird also von Personen angerufen. Beispiel: Beratungshotline.

Privacy Code of Conduct. Der Privacy Code of Conduct (PCoC) ist eine konzernweite Leitlinie der Deutschen Telekom zum Datenschutz, den sie auf Grundlage europarechtlicher Vorgaben im Jahr 2004 eingeführt hat. Er regelt einheitlich die internen Anforderungen des Umgangs mit personenbezogenen Daten in der Deutschen Telekom Gruppe.

Radio Frequency Identification (RFID). Radio Frequency Identification (deutsch: Identifizierung mit Hilfe von elektromagnetischen Wellen) bietet die Möglichkeit, Daten über elektromagnetische Wellen auszulesen und zu speichern.

Sarbanes-Oxley Act (S-OX). Sarbanes-Oxley Act ist ein US-Bundesgesetz, das als Reaktion auf Bilanzskandale die Verlässlichkeit der Berichterstattung von Unternehmen verbessern soll. Ziel des Gesetzes ist es, das Vertrauen der Anleger in die Richtigkeit und Verlässlichkeit der veröffentlichten Finanzdaten von Unternehmen wiederherzustellen. Das Gesetz gilt für US-amerikanische und ausländische Unternehmen, deren Wertpapiere u. a. an US-Börsen gehandelt werden, sowie für deren Tochterunternehmen.

Verkehrsdaten. Verkehrsdaten im Sinne des Telekommunikationsgesetzes sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.

Zertifizierung. Verfahren, mit dessen Hilfe die Einhaltung bestimmter Standards für Produkte oder Dienstleistungen und ihrer jeweiligen Herstellungsverfahren nachgewiesen werden kann.

Impressum.

Deutsche Telekom AG
Corporate Communications
Postfach 2000, D-53105 Bonn
Telefon 0228 181 4949
Telefax 0228 181 94004

www.telekom.com

Konzept:
Deutsche Telekom AG und
HGB Hamburger Geschäftsberichte GmbH & Co. KG, Hamburg

Gestaltung und Produktion:
HGB Hamburger Geschäftsberichte GmbH & Co. KG, Hamburg

Fotos:
Deutsche Telekom AG
plainpicture

Reproduktion:
PX2@Medien GmbH & Co. KG, Hamburg

Druck:
Broermann Offset-Druck GmbH, Troisdorf-Spich

KNr. 642 100 129 (deutsch)
KNr. 642 100 135 (englisch)

Kontakt.

Datenschutz Deutsche Telekom AG
datenschutz@telekom.de
www.telekom.com/datenschutz

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

www.telekom.com