Deloitte.

Deloitte & Touche GmbH
Wirtschaftsprüfungsgesellschaft

Schwannstraße 6
40476 Düsseldorf

Postfach 30 02 26
40402 Düsseldorf
Deutschland

Tel: +49 (0)211 8772 01
Fax: +49 (0)211 8772 2277
www.deloitte.com/de

Deutsche Telekom AG, Bonn

Kurzfassung
des Berichts

über die
Prüfung der Angemessenheit, Implementierung
und Wirksamkeit
des datenschutzbezogenen
Compliance Management Systems
im DTAG-Konzern

30. September 2014

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
ADV	Auftragsdatenverarbeitung
BCRP	Binding Corporate Rules Privacy
BDSA	Basis-Datenschutzaudit
BDSG	Bundesdatenschutzgesetz
CMS	Compliance Management System
DPO	Data Privacy Officer
DRC	Datenschutz, Recht und Compliance
DTAG	Deutsche Telekom AG
GPR	Group Privacy
IDW	Institut der Wirtschaftsprüfer
IT	Informationstechnologie
KPI	Key Performance Indicators
PCoC	Privacy Code of Conduct
PS	Prüfungsstandard des IDW
PSA	Privacy & Security Assessment
SGB	Sozialgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz

1 PRÜFUNGSAUFTRAG

Die gesetzlichen Vertreter der

DEUTSCHE TELEKOM AG,

Bonn

(im folgenden kurz "DTAG")

haben uns mit Schreiben vom 21. Mai 2014 beauftragt, eine Prüfung der Angemessenheit, Implementierung und Wirksamkeit ihres in nachstehender Anlage 1 beigefügten datenschutzbezogenen Compliance Management Systems durchzuführen.

Für die Durchführung des Auftrags und unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht als Anlage 2 beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 vereinbart.

Wir erstellen diese Berichterstattung auf Grundlage des mit der DTAG geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich besteht.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung haben wir einen Bericht erstattet, der ausschließlich an die DTAG zur Verwendung für interne Zwecke gerichtet ist. Die Inhalte des Berichts gehen über die dieser Kurzfassung hinaus. Ein vollumfängliches Verständnis über unseren Auftrag, die Vorgehensweise unserer Prüfung sowie unserer Feststellungen kann regelmäßig nur durch das Lesen unseres Berichts gewonnen werden.

2 GEGENSTAND, ART UND UMFANG DER PRÜFUNG

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten CMS-Beschreibung enthaltenen Aussagen über das datenschutzbezogene CMS.

Bei der Einrichtung des CMS wurden die folgenden CMS-Grundsätze (nachfolgend „CMS-Grundsätze zum Datenschutz") zugrunde gelegt, welche für die Ausgestaltung des CMS der DTAG im Prüfungszeitraum maßgeblich waren:

- das Bundesdatenschutzgesetz (BDSG)
- die datenschutzrelevanten Bestimmungen des Telekommunikationsgesetzes (TKG), des Telemediengesetzes (TMG) und anderer relevanter Nebengesetze
- diesbezügliche Vorgaben seitens der Aufsichtsbehörden (u.a. Bundesbeauftragter für Datenschutz und Informationsfreiheit)
- die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogenen Daten und zum freien Datenverkehr
- die im Vorschlag zur Europäischen Datenschutzgrundverordnung vom 25. Januar 2012 und dem laufenden Gesetzgebungsverfahren ausgeführten und diskutierten Prinzipien zum Datenschutz

Die Verantwortung für das CMS einschließlich der Dokumentation des CMS und für die Inhalte der CMS-Beschreibung sowie die Entwicklung und Implementierung entsprechender Grundsätze und Maßnahmen und deren Wirksamkeit liegt bei den gesetzlichen Vertretern der DTAG.

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die in der CMS-Beschreibung enthaltenen Aussagen zur Angemessenheit, Implementierung und Wirksamkeit des datenschutzbezogenen CMS abzugeben. Die Zielsetzung der Prüfung liegt als Systemprüfung nicht in dem Erkennen von einzelnen Regelverstößen. Sie ist daher nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Wir haben unsere Prüfung auf der Grundlage der für Wirtschaftsprüfer geltenden Berufspflichten unter Beachtung des IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980) durchgeführt. Hiernach haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die in der CMS-Beschreibung enthaltenen Aussagen über die dargestellten Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen angemessen dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen in Übereinstimmung mit den angewandten CMS-Grundsätzen zum Datenschutz geeignet sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Verstöße gegen den Datenschutz rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und dass die Grundsätze und Maßnahmen zum 1. März 2014 implementiert und während des Zeitraums vom 1. März 2014 bis 31. August 2014 wirksam waren.

Die Auswahl der Prüfungshandlungen haben wir nach unserem pflichtgemäßen Ermessen vorgenommen. Im Rahmen unserer Prüfung haben wir die Kenntnisse über das rechtliche und wirtschaftliche Umfeld und die Compliance-Anforderungen des Unternehmens berücksichtigt. Wir haben die in der CMS-Beschreibung dargestellten Grundsätze und Maßnahmen sowie die uns vorgelegten Nachweise überwiegend auf der Basis von Stichproben beurteilt. Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet.

Unsere Prüfungstätigkeit umfasste insbesondere die folgenden Schwerpunkte:

- Beurteilung der Beschreibung des datenschutzbezogenen CMS der DTAG und der darin aufgeführten Erklärungen zur CMS-Konzeption sowie ergänzender Dokumente (z. B. Privacy Code of Conduct)
- Durchsicht von Organisations- und Prozessbeschreibungen und Verfahrensgrundsätzen, insbesondere des Privacy & Security Assessment (PSA)-Verfahrens zur Vorabkontrolle und technisch-organisatorischen Maßnahmen zum Datenschutz
- Einsichtnahme in den Datenschutzbericht sowie in die Dokumentation interner Datenschutz-Audits
- Durchsicht und Würdigung von Protokollen und des internen Compliance Reportings zum Datenschutz
- Durchsicht und Würdigung der Schulungsunterlagen und Online-Schulung zum Datenschutz
- Beobachtung von Aktivitäten und Arbeitsabläufen, die mit dem datenschutzbezogenen CMS in Verbindung stehen
- Durchsicht und Würdigung der Darstellung des Datenschutzes bei der DTAG in internen und externen Publikationen
- Durchsicht und Würdigung von Unterlagen zum dezentralen Datenschutz sowie Beobachtung der damit verbundenen Aktivitäten
- Verwertung der Arbeit von internen und externen Prüfungen, die für Compliance Vorfälle innerhalb der DTAG durchgeführt wurden
- Befragung von Mitarbeitern der zentralen und dezentralen Datenschutzorganisation

3 FESTSTELLUNGEN UND EMPFEHLUNGEN ZUM COMPLIANCE MANAGEMENT SYSTEM

Im Zuge der Prüfung der Konzeption, Angemessenheit und Wirksamkeit des datenschutzbezogenen CMS ergaben sich weder Feststellungen, die zu einer Einschränkung oder zum Versagen geführt haben, noch sonstige Feststellungen.

Gleichwohl erlauben wir uns einige Empfehlungen auszusprechen, die im Zuge der Weiterentwicklung des CMS Berücksichtigung finden sollten.

1. Insgesamt kommen wir zu dem Ergebnis, dass die Aufbauorganisation des Bereichs Group Privacy (GPR) zweckmäßig und im Hinblick auf den Personaleinsatz der Aufgabenstellung angemessen ist. Gleichwohl erlauben wir uns darauf hinzuweisen, dass aufgrund anstehender Veränderungen im regulatorischen Umfeld (Europäische Datenschutzgrundverordnung, IT-Sicherheitsgesetz etc.) sowie vor dem Hintergrund des gestiegenen Datenschutzbewusstseins bei den Kunden und Geschäftspartnern der DTAG mit erhöhten Aufwänden in den Bereichen der Regulierung und Vorabkontrolle zu rechnen sein dürfte.

2. Im Hinblick auf eine jederzeit umfassende Abdeckung der Gesellschaften empfehlen wir, die Benennung der Data Privacy Officer (DPO) durch eine stärkere Formalisierung für GPR transparenter zu gestalten sowie ergänzende Empfehlungen für die Bestellung von DPOs insbesondere in den Tochtergesellschaften der internationalen Einheiten zu kommunizieren. Des Weiteren empfehlen wir, vor dem Hintergrund der Binding Corporate Rules Privacy (BCRP) sowie der geplanten Einführung der europäischen Datenschutzgrundverordnung, eine Stärkung der Steuerungsmöglichkeiten der DPOs durch GPR.

3. Das Auftragsmanagement wurde Anfang 2014 implementiert und hat das Ziel, alle wesentlichen Aktivitäten in GPR zentral zu steuern und eine zentrale Ablage für die Dokumentation bereitzustellen. Wir empfehlen, den eingeschlagenen Weg konsequent zu verfolgen und die Fachabteilungen weiter durch klare Leitlinien für die Benutzung des Tools sowie den Ausbau entsprechender Reporting-Funktionalitäten zu unterstützen.

4. Aktuelle Schwachstellen der internen Verfahrensverzeichnisse im Hinblick auf die Datenqualität können im Einzelfall durch Hinzuziehen weiterer Dokumentation kompensiert werden, sodass wir das Risiko möglicher Compliance-Verstöße als derzeit für beherrschbar halten; bereits 2013 hat die Telekom IT dazu ein Projekt NAVI aufgesetzt, welches die Qualität der Compliance-Informationen verbessern soll. Wir empfehlen, das Projekt mit hoher Priorität weiterzuverfolgen, um den geplanten Projektabschluss zum Jahresende 2014 sicherzustellen.

4 PRÜFUNGSURTEIL

Unser Prüfungsurteil erstreckt sich ausschließlich auf die Beschreibung des datenschutzbezogenen CMS. Bei der DTAG besteht im Bereich Datenschutz eine Compliance-Organisation mit Zuständigkeit für die folgenden Gesellschaften

- Deutsche Telekom AG und deren Mehrheitsbeteiligungen, insbesondere
  - Telekom Deutschland GmbH und deren Mehrheitsbeteiligungen
  - T-Systems International GmbH und deren Mehrheitsbeteiligungen

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse sind die in der CMS-Beschreibung enthaltenen Aussagen über die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen angemessen dargestellt. Die in der CMS-Beschreibung dargestellten Grundsätze und Maßnahmen sind geeignet, mit hinreichender Sicherheit sowohl Risiken für wesentliche Verstöße gegen den Datenschutz rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern. Die Grundsätze und Maßnahmen waren zum 1. März 2014 implementiert und während des Zeitraums vom 1. März 2014 bis 31. August 2014 wirksam.

Zu unseren einzelnen Feststellungen und Empfehlungen verweisen wir auf unsere Ausführungen in Abschnitt 3.

Die Beschreibung des datenschutzbezogenen CMS bei der DTAG wurde zum 27. Februar 2014 erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit einzelner Grundsätze und Maßnahmen erstrecken sich auf den Zeitraum vom 1. März 2014 bis 31. August 2014. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass wegen zwischenzeitlicher Änderungen des CMS falsche Schlussfolgerungen gezogen werden.

Auch ein wirksames CMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Regelverstöße auftreten können, ohne systemseitig verhindert oder aufgedeckt zu werden.

Düsseldorf, den 30. September 2014

Deloitte & Touche GmbH
Wirtschaftsprüfungsgesellschaft

Jörg Engels
(Wirtschaftsprüfer)

Dr. Carsten Schinschel
(Partner)

Anlagen:

Beschreibung des datenschutzbezogenen CMS

Allgemeine Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften in der Fassung vom 1. Januar 2002

ANLAGE 1: BESCHREIBUNG DES DATENSCHUTZBEZOGENEN CMS

Einleitung und Zielsetzung

Dieses Dokument beschreibt das Compliance Management System (CMS) der Group Privacy (GPR), mit dessen Hilfe die Einhaltung eines hohen Datenschutzniveaus innerhalb des Konzerns Deutsche Telekom AG gewährleistet wird. Es dient der Veröffentlichung im Zusammenhang mit der Wirksamkeitsprüfung des CMS nach dem Standard IDW PS 980 (IDW Prüfungsstandard: Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen).

Dieses CMS wirkt auf die Einhaltung des Datenschutzes in den folgenden Gesellschaften hin:

- Deutsche Telekom AG (DTAG) und deren Mehrheitsbeteiligungen, insbesondere
    - Telekom Deutschland GmbH und deren Mehrheitsbeteiligungen
    - T-Systems International GmbH und deren Mehrheitsbeteiligungen

Dieses Compliance Management System gilt in allen Konzerngesellschaften, in denen der Leiter des Konzerndatenschutzes zum Datenschutzbeauftragten berufen worden ist. Grundsätzlich gilt erfolgt diese Bestellung zum Datenschutzbeauftragten für alle Konzerngesellschaften; Ausnahmen sind in Kapitel 5.1 beschrieben. Eine stets aktuelle Liste dieser Bestellungen zum Datenschutzbeauftragten ist im Intranet der Deutschen Telekom veröffentlicht.

In den nachfolgenden sieben Kapiteln werden die sieben Grundelemente des Prüfungsstandards PS 980 und deren Umsetzung bei der Telekom dargestellt. Einleitend enthält jedes Kapitel die Anforderung des Standards, danach werden in den Unterkapiteln die konkrete Umsetzung bei der Deutschen Telekom beschrieben.

1 Privacy Compliance-Kultur

IDW PS 980: Die Compliance-Kultur stellt die Grundlage für die Angemessenheit und Wirksamkeit des CMS dar. Sie wird vor allem geprägt durch die Grundeinstellungen und Verhaltensweisen des Managements sowie durch die Rolle des Aufsichtsorgans („tone at the top"). Die Compliance-Kultur beeinflusst die Bedeutung, welche die Mitarbeiter des Unternehmens der Beachtung von Regeln beimessen und damit die Bereitschaft zu regelkonformem Verhalten.

1.1 Vorstandsressort Datenschutz, Recht und Compliance

Die Compliance-Kultur der Deutschen Telekom zielt darauf ab, alle gesetzlichen Anforderungen zum Datenschutz strikt einzuhalten und das Bewusstsein der Mitarbeiter für die Notwendigkeit der Gewährleistung eines hohen Datenschutzniveaus zu fördern.

Die Förderung eines hohen Datenschutzniveaus ist in der Unternehmenskultur der Telekom fest verankert. Dies wird auch außerhalb der DTAG so wahrgenommen. So wurde die Telekom laut Sicherheitsreport 2013 des Instituts für Demoskopie Allensbach[1] bei einer Befragung von 1490 Personen ab 16 Jahren mit deutlichem Abstand als vertrauenswürdigstes Unternehmen eingestuft, was den Umgang mit persönlichen Daten umgeht.

Die Deutsche Telekom verfügt als eines der wenigen DAX-Unternehmen über ein eigenes Vorstandsressort für Datenschutz, Recht und Compliance (DRC). Damit stehen der Datenschutz und die Compliance ganz oben auf der Agenda der DTAG.

Neben internen Maßnahmen wie der Formulierung verbindlicher Leitlinien, der Schulung aller Mitarbeiter, der regelmäßigen Überprüfung des erreichten Niveaus und der Definition und Umsetzung von Verbesserungsmaßnahmen sucht die Deutsche Telekom auch den Dialog mit der Öffentlichkeit, um auch außerhalb des Unternehmens in Politik und Wirtschaft ein hohes Datenschutzniveau zu fördern.

1.2 Besuche vor Ort

Der Konzerndatenschutzbeauftragte besucht regelmäßig Ländergesellschaften, um sich mit dem Management zum Datenschutz auszutauschen. Es soll erreicht werden, dass dem Thema Datenschutz mehr Aufmerksamkeit geschenkt und ein einheitliches Verständnis für den Datenschutz aufgebaut wird. In 2013 hat der Konzerndatenschutzbeauftragte unter anderem die folgenden Länder besucht: Niederlande, China, Polen, Slowakei, Tschechien, Dänemark

[1] Sicherheitsreport 2013: Ergebnisse einer repräsentativen Bevölkerungsbefragung (http://www.telekom.com/static/-/198372/2/Sicherheitsreport-2013-si)

1.3 Datenschutzbeirat

Der Datenschutzbeirat der Deutschen Telekom ist ein unabhängiges Beratungsgremium. Er besteht aus führenden Datenschutzexperten und Persönlichkeiten aus Politik, Lehre, Wirtschaft und unabhängigen Organisationen, berät den Vorstand der Deutschen Telekom und ermöglicht einen konstruktiven Austausch zu datenschutzrelevanten Themen. Der Datenschutzbeirat wurde im Februar 2009 gegründet und ergänzt die interne Datenschutz- und Sicherheitsorganisation der Deutschen Telekom um einen unabhängigen und gesellschaftlich vielfältigen Blick von außen.

Der Datenschutzbeirat deckt ein breites Themenfeld ab: Er befasst sich mit Geschäftsmodellen und -prozessen zum Umgang mit Kunden- und Mitarbeiterdaten ebenso wie mit der IT-Sicherheit und der Angemessenheit von entsprechenden Maßnahmen, mit internationalen Datenschutzfragen sowie mit den Implikationen neuer gesetzlicher Regelungen. Zu seinen Aufgaben gehören die Beurteilung von Datenschutz- und Datensicherheitsmaßnahmen sowie die Erarbeitung von Vorschlägen und Empfehlungen an Vorstand und Aufsichtsrat auch im Kontext der "digitalen" Gesellschaft.

1.4 Transparenzbericht „Datenschutz und Datensicherheit“

Jährlich veröffentlicht die Deutsche Telekom den Transparenzbericht „Datenschutz und Datensicherheit“[2]. Darin werden aktuelle Datenschutz-Themen des Unternehmens und gesellschaftlich relevante Fragestellungen diskutiert. Im Bericht findet sich auch eine Aufzählung der bei der Telekom aufgetretenen Datenschutz-Fragestellungen und der abgeleiteten Lösungen.

[2] Datenschutzbericht 2013 (http://www.telekom.com/static/-/212804/3/datenschutzbericht-2013-si)

2 Privacy Compliance-Ziele

***IDW PS 980**: Die gesetzlichen Vertreter legen auf der Grundlage der allgemeinen Unternehmensziele und einer Analyse und Gewichtung der für das Unternehmen bedeutsamen Regeln die Ziele fest, die mit dem CMS erreicht werden sollen. Dies umfasst insb. die Festlegung der relevanten Teilbereiche und der in den einzelnen Teilbereichen einzuhaltenden Regeln. Die Compliance-Ziele stellen die Grundlage für die Beurteilung von Compliance-Risiken dar.*

Die Compliance-Ziele ergeben sich aus dem Geschäftsauftrag des Konzerndatenschutzes der Deutschen Telekom:

I. Mandat

Entwicklung und Transformation der konzernweiten Datenschutz-Strategie.

Definition und Erlass der Konzernrichtlinien zum Datenschutz.

Sie sind unter Beachtung der Konzernrichtlinie zur Erstellung von Konzernrichtlinien zu erlassen. Ihre Umsetzung hat in dezentraler Verantwortung unter Beachtung der jeweils gültigen nationalen Vorschriften in der Kompetenz der jeweils zuständigen Organe zu erfolgen. Die Überprüfung der Implementierung und Einhaltung erfolgt durch Reviews unter Wahrung der jeweils gültigen nationalen Vorschriften.

Stellung des Datenschutzbeauftragten für die Gesellschaften des Konzerns und Erfüllung der gesetzlichen Aufgaben zum Datenschutz.

Vertretung des Konzerns in allen Angelegenheiten des Datenschutzes nach innen wie nach außen.

II. Zielsetzung (Zweck)

Sicherstellung eines einheitlichen und hohen Datenschutzniveaus im Konzern.

Hinwirken auf die Einhaltung der gesetzlichen, regulatorischen und konzerninternen Anforderungen zum Datenschutz.

III. Aufgaben am externen Markt

- Vertretung der Interessen des Konzerns im Bereich Datenschutz gegenüber Wirtschaft, Verbänden, Politik, obersten Aufsichtsbehörden, Großkunden, Endkunden, Lieferanten und anderen Stakeholdern
- Verbesserung der Wahrnehmung des Datenschutzes bei der Deutschen Telekom in der Öffentlichkeit (Öffentlichkeitsarbeit).

IV. Aufgaben im Konzern

Strategie/Policies/Guidelines

- Ableitung der Datenschutz-Strategie aus der Unternehmensstrategie.
- Strategische, einheitlichen und nachhaltigen Steuerung des Konzerns im Datenschutz.
- Entwicklung, Erlass und Kommunikation von Konzernrichtlinien und Anforderungen zum Datenschutz.
- Herbeiführung der notwendigen Beschlüsse durch die zuständigen Organe und Gremien zur Umsetzung der Datenschutzrichtlinien und -anforderungen im Konzern.

Reviews

- Durchführung von regelmäßigen, bedarfsorientierten oder anlassbezogenen Reviews und Kontrollbesuchen zur Prüfung der regelkonformen und konzerneinheitlichen Ausrichtung im Bereich Datenschutz.
- Regelmäßige Überprüfung der für den Konzern geltenden Rahmenbedingungen im Datenschutz.

Konzernweite Projekte

- Durchführung von konzernweiten strategischen Synergieprojekten im Zusammenhang mit Datenschutzanforderungen, Begleitung von Konzern-Großprojekten oder Projekte zur Einführung von neuen Richtlinien und Anforderungen.

V. Wesentliche Produkte/Leistungen

- Umsetzung der gesetzlichen Aufgaben des Datenschutzbeauftragten.
- Gestaltung und Bereitstellung des Berichtswesens zum Datenschutz an den Konzernvorstand und den Aufsichtsrades Konzerns.
- Risikoberatung, Vorabprüfung bzw. Prüfung und Freigabe von Geschäftsmodellen, Produkten und Personaldatenverarbeitungsmodellen.
- Entwicklung und Bereitstellung von Templates und Muster zur vertraglichen Regelungen und Vorgehensweisen.
- Konzeption und Umsetzung von Mitarbeiter- und Kundensensibilisierungsmaßnahmen.
- Steuerung und Kontrolle der Umsetzung der Datenschutzrichtlinien und –anforderungen im Konzern.
- Kontrollmaßnahmen zur Einhaltung der regulatorischen Rahmenbedingungen durch den Konzern.

VI. Interne/Externe Kunden

Intern (Beispiele)

- Aufsichtsrat und seine Ausschüsse
- Vorstandsvorsitzender, Konzernvorstand und Vorstandsausschüsse
- Konzernbetriebsrat, Betriebsräte und deren Ausschüsse
- Topmanagement im Konzern, insbesondere Leiter der Organisationseinheiten
- Alle Mitarbeiter

Extern (Beispiele)

- Politische Vertreter und Meinungsbildner.
- Nationale und internationale oberste Aufsichtsbehörden zum Datenschutz.
- Institutionen und Gremien aus Wissenschaft, Verbänden, Industrie und Wirtschaft
- Top Management Unternehmenskunden
- Endkunden (Massenmarkt).

3 Privacy Compliance-Risiken

IDW PS 980: Unter Berücksichtigung der Compliance-Ziele werden die Compliance-Risiken festgestellt, die Verstöße gegen einzuhaltende Regeln und damit eine Verfehlung der Compliance-Ziele zur Folge haben können. Hierzu wird ein Verfahren zur systematischen Risikoerkennung und -berichterstattung eingeführt. Die festgestellten Risiken werden im Hinblick auf Eintrittswahrscheinlichkeit und mögliche Folgen analysiert.

Die Risiken in Bezug auf die Compliance-Ziele sind:

- Gesetzliche Anforderungen werden nicht oder zu spät identifiziert
- Die Bestellung eines Datenschutzbeauftragten erfolgt in einzelnen Unternehmensteilen nicht.
- Das öffentliche Verfahrensverzeichnis (§ 4e BDSG) einzelner Unternehmen liegt nicht vor oder ist nicht vollständig.
- Die interne Verarbeitungsliste (§ 4 e, g BDSG) einzelner Unternehmen liegt nicht vor oder ist nicht vollständig.
- Die Datenverarbeitungen setzen nicht alle gesetzlichen Anforderungen um (BDSG, TKG, TMG, SGB u.a.).
- Es sind nicht alle betroffenen Mitarbeiter auf das Datengeheimnis (§ 5 BDSG) bzw. das Fernmeldegeheimnis (§ 88 TKG) verpflichtet.
- Es werden nicht alle Mitarbeiter regelmäßig zum Thema Datenschutz geschult und sensibilisiert (§ 4 g BDSG).
- Es werden nicht alle notwendigen Verträge zur Auftragsdatenverarbeitung (§ 11 BDSG) abgeschlossen.
- Auskunftsanträge von Betroffenen (§ 34 BDSG) werden nicht oder unzureichend beantwortet.
- Bei unrechtmäßiger Kenntniserlangung von personenbezogenen Daten nach (§ 42 a BDSG, § 109a TKG, § 15a TMG) wird nicht oder unzureichend berichtet.

Diese Risiken werden einer Bewertung der Eintrittswahrscheinlichkeit und möglicher Folgen analysiert und daraus werden geeignete Maßnahmen abgeleitet. Es wird ein Maßnahmenplan aufgestellt und die Verantwortlichen zur Umsetzung werden identifiziert.

4 Compliance-Programm

IDW PS 980: Auf der Grundlage der Beurteilung der Compliance-Risiken werden Grundsätze und Maßnahmen eingeführt, die auf die Begrenzung der Compliance-Risiken und damit auf die Vermeidung von Compliance-Verstößen ausgerichtet sind. Das Compliance-Programm umfasst auch die bei festgestellten Compliance-Verstößen zu ergreifenden Maßnahmen. Das Compliance-Programm wird zur Sicherstellung einer personenunabhängigen Funktion des CMS dokumentiert.

4.1 Identifikation gesetzlicher Anforderungen

Die Grundsätze und umzusetzenden Maßnahmen zur Vermeidung von Compliance-Verstößen ergeben sich unmittelbar aus den gesetzlichen Regelungen zum Datenschutz. Besonderes Augenmerk wird daher bei der Deutschen Telekom AG und ihren Konzerngesellschaften auf die kontinuierliche Identifikation geplanter und neu eingeführter gesetzlicher Anforderungen im Datenschutz gelegt.

4.2 Leitlinie zum Datenschutz

Das übergeordnete Ziel der Datenschutzorganisation ist es, ein weltweit einheitlich hohes Datenschutzniveau in allen Konzerngesellschaften zu implementieren. Die identifizierten gesetzlichen und regulatorischen Anforderungen sind als Leitlinien zum Datenschutz im öffentlichen Privacy Code of Conduct (PCoC) zusammengefasst. Der PCoC hat für alle Konzerngesellschaften mit Mehrheitsbeteiligung Rechtsnatur und ist somit bindend. Der PCoC wird künftig abgelöst werden duch Bindung Corporate Rules.

Die Leitlinien zum Datenschutz werden präzisiert in einer Vielzahl von Richtlinien und Datenschutzanforderungen, die für konkrete Anwendungsfälle Handlungsanweisungen für einen datenschutzkonformen Betrieb der Datenverarbeitungen enthalten.

4.3 Schulungen und Awareness

Jeder Beschäftigte muss eine Grundlagenschulung „Verpflichtung auf den Daten- und Informationsschutz“ absolviert haben. Neben der verpflichtenden Grundlagenschulung werden Vertiefungsschulungen zu den Themen Beschäftigtendatenschutz und Kundendatenschutz und Spezialistenschulungen zu konkreten Sachverhalten durchgeführt, beispielsweise für Marketing, die Personalabteilung oder das Rechnungswesen.

4.4 Verpflichtungserklärung

Am Ende der Grundlagenschulung wird jeder Teilnehmer auf das Datengeheimnis nach § 5 BDSG und das Fernmeldegeheimnis nach § 88 TKG verpflichtet.

4.5 Vorgehen bei Regelverstößen

Regelverstöße werden bei der Telekom ohne Ansehen der Person und von Hierarchien verfolgt und ziehen angemessene Sanktionen nach sich.

5 Privacy Compliance-Organisation

IDW PS 980: Das Management regelt die Rollen und Verantwortlichkeiten (Aufgaben) sowie Aufbau- und Ablauforganisation im CMS als integralen Bestandteil der Unternehmensorganisation und stellt die für ein wirksames CMS notwendigen Ressourcen zur Verfügung.

5.1 Konzerndatenschutz

Der Konzerndatenschutzbeauftragte als Leiter des Bereichs Group Privacy (GPR) berichtet direkt an den Vorstand Datenschutz, Recht und Compliance (DRC). Somit ist ein regelmäßiger Austausch GPR mit den weiteren Ressortbereichen gegeben.

Der Konzerndatenschutzbeauftragte wird von allen nationalen Konzerneinheiten als Datenschutzbeauftragter bestellt. Es gibt jedoch begründete Ausnahmen:

- Die Gesellschaft gehört der Telekom zu weniger als 50%
- Die Gesellschaft wäre aufgrund der vorherrschenden Organisationsstruktur mit der Prozessadaption überlastet.
- Ein als kompetent eingestufter Datenschutzbeauftragter ist bereits langjährig für das Unternehmen tätig

Der Bereich GPR gliedert sich in verschiedene Abteilungen, die Beratungsaufgaben wahrnehmen, die Einhaltung der Datenschutzvorgaben im Rahmen von Audits überprüfen und abteilungsübergreifende Steuerfunktionen wahrnehmen. GPR-Mitarbeiter nehmen an einer Vielzahl von internen und externen Gremien teil, um die Interessen des Datenschutzes zu vertreten.

5.2 Dezentrale Datenschutzorganisation

Der Bereich GPR wird national und international ergänzt durch dezentrale Datenschutzorganisationen. Hierbei übernehmen Mitglieder des jeweiligen Top-Managements der Beteiligungen strategische Datenschutzaufgaben, im mittleren Management sind operative Aufgaben angesiedelt und auf Arbeitsebene wird der Konzerndatenschutz durch Datenschutzkoordinatoren unterstützt.

5.3 PSA-Verfahren

Das Privacy and Security Assessment (PSA)-Verfahren ist ein zentraler Baustein zur Gewährleistung von technischer Sicherheit und Datenschutz bei der Deutschen Telekom. Alle neu erstellten oder geänderten Systeme durchlaufen eine Beurteilung hinsichtlich der Umsetzung eines adäquaten Sicherheits- und Datenschutzniveaus bereits während der Entwicklungs- und Implementierungsprozesse. In-

formationen zum PSA-Verfahren werden einer interessierten Öffentlichkeit über die Webseite der Deutschen Telekom zugänglich gemacht[3].

5.4 Auskunftsersuchen

Der Bereich GPR bearbeitet Anfragen nach dem öffentliches Verfahrensverzeichnis (§ 4 g (2) BDSG) sowie Auskunftsersuchen nach § 34 BDSG. Über die E-Mail-Adresse datenschutz@telekom.de, per Post, Fax oder Anfrage über den Kundenservice gehen entsprechende Kundenanfragen zu Verzeichniseinträgen, unerwünschter Werbung oder Auskunftsersuchen nach §34 BDSG ein.

[3] http://www.telekom.com/psa

6 Privacy Compliance-Kommunikation

IDW PS 980: Die jeweils betroffenen Mitarbeiter und ggf. Dritte werden über das Compliance-Programm sowie die festgelegten Rollen und Verantwortlichkeiten informiert, damit sie ihre Aufgaben im CMS ausreichend verstehen und sachgerecht erfüllen können.

Im Unternehmen wird festgelegt, wie Compliance-Risiken sowie Hinweise auf mögliche und festgestellte Regelverstöße an die zuständigen Stellen im Unternehmen (z.B. die gesetzlichen Vertreter und erforderlichenfalls das Aufsichtsorgan) berichtet werden.

6.1 Verpflichtung auf das Daten- und/oder Fernmeldegeheimnis

Die Verpflichtung auf das Datengeheimnis nach § 5 BDSG und auf das Fernmeldegeheimnis nach § 88 TKG ist sowohl eine gesetzliche Anforderung als auch ein sehr gut geeignetes Mittel, um Compliance einzufordern. Die Verpflichtung wird für alle Mitarbeiter sowie Berater und externe Dienstleister durchgeführt und gilt auch nach Beendigung des Vertrages. Es wird in den Vertragstexten darauf hingewiesen, dass Verstöße gegen das Datengeheimnis mit Freiheits- oder Geldstrafen geahndet werden können.

Mitarbeiter, Berater und Dienstleister verpflichten sich außerdem, den Arbeitgeber bzw. Auftraggeber DTAG umgehend bei Verdacht auf Datenschutzverletzungen, Verletzung der Vertraulichkeit von Daten und anderen Unregelmäßigkeiten zu unterrichten.

Bei externen Mitarbeitern (z.B. Reinigungskräften, Personal im Facility Management oder Beratern) wird über die Einkaufsprozesse eine Verschwiegenheitsklausel in die jeweilige Beauftragung integriert. Berater unterzeichnen zudem routinemäßig, als Bestandteil ihrer Verträge, Sicherheitsregelungen hinsichtlich Zutrittskontrolle, Brandschutz und Vertraulichkeit sowie eine Verpflichtungserklärung auf das Datengeheimnis nach § 5 BDSG und das Fernmeldegeheimnis nach § 88 TKG.

6.2 Schulungen

Ein weiteres Mittel zur Kommunikation von Compliance-Anforderungen ist die Durchführung von Mitarbeiterschulungen (siehe Kapitel „Schulungen und Awareness“ im Abschnitt „Compliance-Programm“).

6.3 Richtlinien zum Datenschutz

Die Leitlinie zum Datenschutz bildet das Rahmenwerk für die Umsetzung eines hohen Datenschutzniveaus innerhalb der Deutschen Telekom. Sie wird ergänzt durch eine Vielzahl von Datenschutzanforderungen, die sich auf konkrete Sachverhalte beziehen, beispielsweise Technische und Organisatori-

sche Maßnahmen nach Anhang zu § 9 BDSG, das Löschen von Kundendaten oder Maßnahmen im Zusammenhang mit Webportalen und Webtracking.

Die Dokumente enthalten klare Vorgaben zu den rechtlichen Rahmenbedingungen und Anforderungen an den Umgang mit personenbezogenen Daten. Die gesetzlichen Anforderungen und die Anforderungen der Datenschutz-Leitlinie werden in den Datenschutzanforderungen fachlich konkret formuliert und geben den betroffenen Bereichen im Konzern umfangreiche Handlungsvorschläge und Hilfestellungen an die Hand, um die Anforderungen des Datenschutzes umzusetzen.

6.4 Auftragsdatenverarbeitung

Die Prüfung, ob ein Vertrag zur Auftragsdatenverarbeitung (ADV) abgeschlossen werden muss, ist als Routine-Schritt in den Einkaufsprozessen etabliert. Der Einkauf ist die zentrale Stelle zur Ablage der ADV-Verträge mit externen Unternehmen. GPR stellt für die operativen Bereiche eine Reihe von Vertragskonstellationen aktuelle ADV-Vorlagen zur Verfügung.

6.5 Öffentlicher Transparenzbericht

Ein weiteres Element der Compliance – Kommunikation ist der jährlich veröffentlichte Transparenzbericht „Datenschutz und Datensicherheit“[4]. Darin werden aktuelle Datenschutz-Themen des Unternehmens und gesellschaftlich relevante Fragestellungen diskutiert. Im Bericht findet sich auch eine Aufzählung der bei der Telekom aufgetretenen Datenschutz-Probleme und der eingeleiteten Maßnahmen.

[4] Datenschutzbericht 2013 (http://www.telekom.com/static/-/212804/3/datenschutzbericht-2013-si)

7 Compliance-Überwachung und Verbesserung

IDW PS 980: Angemessenheit und Wirksamkeit des CMS werden in geeigneter Weise überwacht. Voraussetzung für die Überwachung ist eine ausreichende Dokumentation des CMS. Werden im Rahmen der Überwachung Schwachstellen im CMS bzw. Regelverstöße festgestellt, werden diese an das Management bzw. die hierfür bestimmte Stelle im Unternehmen berichtet. Die gesetzlichen Vertreter sorgen für die Durchsetzung des CMS, die Beseitigung der Mängel und die Verbesserung des Systems.

7.1 Audits

Die Einhaltung der Leitlinie zum Datenschutz und der Datenschutz-Anforderungen wird durch eine Vielzahl von Audits überprüft. Die Auditplanung erfolgt auf Basis von Risikoanalysen zur Identifikation kritischer Datenverarbeitungen. Die Ergebnisse der Audits und die Nachverfolgung der daraus resultierenden Maßnahmen werden mit Hilfe einer Audit-Datenbank dokumentiert und gesteuert.

Ein wichtiges Element sind Basis-Datenschutzaudits, die der Ermittlung des aktuellen Datenschutzniveaus in einer Organisation anhand der Beantwortung von Fragen an Mitarbeiter dienen. Sie werden jährlich durchgeführt. Für den BDSA werden im Allgemeinen etwa 30% der Mitarbeiter einer Organisation zufällig ausgewählt. Je nach Größe des betroffenen Organisationsbereichs wird die Größe der Stichprobe manuell angepasst, damit die Ergebnisse statistisch relevant und damit vergleichbar sind. In Bereichen mit weniger als 40 Mitarbeitern werden 100% der Mitarbeiter befragt, in Bereichen mit mehreren tausend Mitarbeitern können auch weniger als 30% der Mitarbeiter für die Befragung ausgelost werden. Das Top-Management des betroffenen Bereichs sowie der Konzernvorstand werden durch den Konzerndatenschutzbeauftragten über die Ergebnisse des BDSA informiert, ferner werden Gespräche über daraus abzuleitende Maßnahmen (z.B. Nachschulungen) und deren Umsetzung geführt.

Weiterhin werden System-Audits, Organisations-Audits und verschiedene Audits im Rahmen des PSA-Verfahrens durchgeführt. Darüber hinaus werden anlassbezogene Audits ad hoc durchgeführt, sobald der Bedarf weiterer, nicht geplanter Prüfungen erkannt und für sinnvoll erachtet wird. Beispiele solcher Audits sind Abnahmeaudits von IT-Systemen oder Untersuchungen zu Datenschutzvorfällen.

7.2 Übersicht über die Datenverarbeitungen

Die Datenverarbeitungen der Unternehmen der Deutschen Telekom werden von den Betreibern gemäß § 4 d, e, g (2) BDSG in einem so genannten internen Verfahrensverzeichnis aufgeführt.

7.3 Behandlung von Datenschutzvorfällen

Innerhalb der Leitlinie zum Datenschutz ist festgelegt, dass der Datenschutzbeauftragte des jeweiligen Unternehmens unverzüglich über Verstöße (auch schon bei Verdacht auf Verstoß) gegen Datenschutzbestimmungen oder die Leitlinie zu informieren ist. 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.

Datenschutzvorfälle werden zeitnah berichtet und alle relevanten Stellen werden informiert. Es werden ferner Sofortmaßnahmen initiiert und dauerhafte Lösungen abgeleitet. Meldungen gehen auf verschiedenen Wegen ein. Sie können über die öffentlich und intern kommunizierte Mailadresse datenschutz@telekom.de bekannt werden, aber auch telefonisch, im persönlichen Gespräch, über Fax, Brief oder über Mailadressen von Mitarbeitern des Konzerndatenschutzes.

Alle Datenschutzvorfälle werden im Auftragsmanagement-Tool erfasst, gesteuert und dokumentiert. Wenn erforderlich, werden die Betroffenen und die Aufsichtsbehörden informiert, ferner wird im nächsten Transparenzbericht informiert.

7.4 Dokumentation und Maßnahmenverfolgung

Sämtliche Dokumentation und Maßnahmenverfolgung wird mit Hilfe eines Auftragsmanagement-Tools“) durchgeführt.

7.5 Berichtswesen

Der Bereich Konzerndatenschutz berichtet regelmäßig an den Vorstand DRC, darunter auch Kennzahlen zum Compliance Management. Die Compliance-Ziele werden durch geeignete Key Performance Indicators (KPI) hinsichtlich der Zielerreichung überwacht.

7.6 Kontinuierliche Verbesserung

Um die kontinuierliche Überprüfung und Verbesserung des Compliance Management Systems zu gewährleisten, ist dieses in das interne Qualitätsmanagement-System des Konzerndatenschutzes integriert.

ANLAGE 2: ALLGEMEINE AUFTRAGSBEDINGUNGEN FÜR WIRTSCHAFTSPRÜFER UND WIRTSCHAFTSPRÜFUNGSGESELLSCHAFTEN IN DER FASSUNG VOM 1. JANUAR 2002

Allgemeine Auftragsbedingungen
für
Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften
vom 1. Januar 2002

1. Geltungsbereich

(1) Die Auftragsbedingungen gelten für die Verträge zwischen Wirtschaftsprüfern oder Wirtschaftsprüfungsgesellschaften (im nachstehenden zusammenfassend „Wirtschaftsprüfer genannt) und ihren Auftraggebern über Prüfungen, Beratungen und sonstige Aufträge, soweit nicht etwas anderes ausdrücklich schriftlich vereinbart oder gesetzlich zwingend vorgeschrieben ist.

(2) Werden im Einzelfall ausnahmsweise vertragliche Beziehungen auch zwischen dem Wirtschaftsprüfer und anderen Personen als dem Auftraggeber begründet, so gelten auch gegenüber solchen Dritten die Bestimmungen der nachstehenden Nr. 9.

2. Umfang und Ausführung des Auftrages

(1) Gegenstand des Auftrages ist die vereinbarte Leistung, nicht ein bestimmter wirtschaftlicher Erfolg. Der Auftrag wird nach den Grundsätzen ordnungsmäßiger Berufsausübung ausgeführt. Der Wirtschaftsprüfer ist berechtigt, sich zur Durchführung des Auftrages sachverständiger Personen zu bedienen.

(2) Die Berücksichtigung ausländischen Rechts bedarf - außer bei betriebswirtschaftlichen Prüfungen - der ausdrücklichen schriftlichen Vereinbarung.

(3) Der Auftrag erstreckt sich, soweit er nicht darauf gerichtet ist, nicht auf die Prüfung der Frage, ob die Vorschriften des Steuerrechts oder Sondervorschriften, wie z. B. die Vorschriften des Preis-, Wettbewerbsbeschränkungs- und Bewirtschaftungsrechts beachtet sind; das gleiche gilt für die Feststellung, ob Subventionen, Zulagen oder sonstige Vergünstigungen in Anspruch genommen werden können. Die Ausführung eines Auftrages umfasst nur dann Prüfungshandlungen, die gezielt auf die Aufdeckung von Buchfälschungen und sonstigen Unregelmäßigkeiten gerichtet sind, wenn sich bei der Durchführung von Prüfungen dazu ein Anlass ergibt oder dies ausdrücklich schriftlich vereinbart ist.

(4) Ändert sich die Rechtslage nach Abgabe der abschließenden beruflichen Äußerung, so ist der Wirtschaftsprüfer nicht verpflichtet, den Auftraggeber auf Änderungen oder sich daraus ergebende Folgerungen hinzuweisen.

3. Aufklärungspflicht des Auftraggebers

(1) Der Auftraggeber hat dafür zu sorgen, daß dem Wirtschaftsprüfer auch ohne dessen besondere Aufforderung alle für die Ausführung des Auftrages notwendigen Unterlagen rechtzeitig vorgelegt werden und ihm von allen Vorgängen und Umständen Kenntnis gegeben wird, die für die Ausführung des Auftrages von Bedeutung sein können. Dies gilt auch für die Unterlagen, Vorgänge und Umstände, die erst während der Tätigkeit des Wirtschaftsprüfers bekannt werden.

(2) Auf Verlangen des Wirtschaftsprüfers hat der Auftraggeber die Vollständigkeit der vorgelegten Unterlagen und der gegebenen Auskünfte und Erklärungen in einer vom Wirtschaftsprüfer formulierten schriftlichen Erklärung zu bestätigen.

4. Sicherung der Unabhängigkeit

Der Auftraggeber steht dafür ein, daß alles unterlassen wird, was die Unabhängigkeit der Mitarbeiter des Wirtschaftsprüfers gefährden könnte. Dies gilt insbesondere für Angebote auf Anstellung und für Angebote, Aufträge auf eigene Rechnung zu übernehmen.

5. Berichterstattung und mündliche Auskünfte

Hat der Wirtschaftsprüfer die Ergebnisse seiner Tätigkeit schriftlich darzustellen, so ist nur die schriftliche Darstellung maßgebend. Bei Prüfungsaufträgen wird der Bericht, soweit nichts anderes vereinbart ist, schriftlich erstattet. Mündliche Erklärungen und Auskünfte von Mitarbeitern des Wirtschaftsprüfers außerhalb des erteilten Auftrages sind stets unverbindlich.

6. Schutz des geistigen Eigentums des Wirtschaftsprüfers

Der Auftraggeber steht dafür ein, daß die im Rahmen des Auftrages vom Wirtschaftsprüfer gefertigten Gutachten, Organisationspläne, Entwürfe, Zeichnungen, Aufstellungen und Berechnungen, insbesondere Massen- und Kostenberechnungen, nur für seine eigenen Zwecke verwendet werden.

7. Weitergabe einer beruflichen Äußerung des Wirtschaftsprüfers

(1) Die Weitergabe beruflicher Äußerungen des Wirtschaftsprüfers (Berichte, Gutachten und dgl.) an einen Dritten bedarf der schriftlichen Zustimmung des Wirtschaftsprüfers, soweit sich nicht bereits aus dem Auftragsinhalt die Einwilligung zur Weitergabe an einen bestimmten Dritten ergibt.
Gegenüber einem Dritten haftet der Wirtschaftsprüfer (im Rahmen von Nr. 9) nur, wenn die Voraussetzungen des Satzes 1 gegeben sind.

(2) Die Verwendung beruflicher Äußerungen des Wirtschaftsprüfers zu Werbezwecken ist unzulässig; ein Verstoß berechtigt den Wirtschaftsprüfer zur fristlosen Kündigung aller noch nicht durchgeführten Aufträge des Auftraggebers.

8. Mängelbeseitigung

(1) Bei etwaigen Mängeln hat der Auftraggeber Anspruch auf Nacherfüllung durch den Wirtschaftsprüfer. Nur bei Fehlschlagen der Nacherfüllung kann er auch Herabsetzung der Vergütung oder Rückgängigmachung des Vertrages verlangen; ist der Auftrag von einem Kaufmann im Rahmen seines Handelsgewerbes, einer juristischen Person des öffentlichen Rechts oder von einem öffentlich-rechtlichen Sondervermögen erteilt worden, so kann der Auftraggeber die Rückgängigmachung des Vertrages nur verlangen, wenn die erbrachte Leistung wegen Fehlschlagens der Nacherfüllung für ihn ohne Interesse ist. Soweit darüber hinaus Schadensersatzansprüche bestehen, gilt Nr. 9.

(2) Der Anspruch auf Beseitigung von Mängeln muß vom Auftraggeber unverzüglich schriftlich geltend gemacht werden. Ansprüche nach Abs. 1, die nicht auf einer vorsätzlichen Handlung beruhen, verjähren nach Ablauf eines Jahres ab dem gesetzlichen Verjährungsbeginn.

(3) Offenbare Unrichtigkeiten, wie z. B. Schreibfehler, Rechenfehler und formelle Mängel, die in einer beruflichen Äußerung (Bericht, Gutachten und dgl.) des Wirtschaftsprüfers enthalten sind, können jederzeit vom Wirtschaftsprüfer auch Dritten gegenüber berichtigt werden. Unrichtigkeiten, die geeignet sind, in der beruflichen Äußerung des Wirtschaftsprüfers enthaltene Ergebnisse in Frage zu stellen, berechtigen diesen, die Äußerung auch Dritten gegenüber zurückzunehmen. In den vorgenannten Fällen ist der Auftraggeber vom Wirtschaftsprüfer tunlichst vorher zu hören.

9. Haftung

(1) Für gesetzlich vorgeschriebene Prüfungen gilt die Haftungsbeschränkung des § 323 Abs. 2 HGB.

(2) Haftung bei Fahrlässigkeit, Einzelner Schadensfall

Falls weder Abs. 1 eingreift noch eine Regelung im Einzelfall besteht, ist die Haftung des Wirtschaftsprüfers für Schadensersatzansprüche jeder Art, mit Ausnahme von Schäden aus der Verletzung von Leben, Körper und Gesundheit, bei einem fahrlässig verursachten einzelnen Schadensfall gem. § 54 a Abs. 1 Nr. 2 WPO auf 4 Mio. € beschränkt; dies gilt auch dann, wenn eine Haftung gegenüber einer anderen Person als dem Auftraggeber begründet sein sollte. Ein einzelner Schadensfall ist auch bezüglich eines aus mehreren Pflichtverletzungen stammenden einheitlichen Schadens gegeben. Der einzelne Schadensfall umfaßt sämtliche Folgen einer Pflichtverletzung ohne Rücksicht darauf, ob Schäden in einem oder in mehreren aufeinanderfolgenden Jahren entstanden sind. Dabei gilt mehrfaches auf gleicher oder gleichartiger Fehlerquelle beruhendes Tun oder Unterlassen als einheitliche Pflichtverletzung, wenn die betreffenden Angelegenheiten miteinander in rechtlichem oder wirtschaftlichem Zusammenhang stehen. In diesem Fall kann der Wirtschaftsprüfer nur bis zur Höhe von 5 Mio. € in Anspruch genommen werden. Die Begrenzung auf das Fünffache der Mindestversicherungssumme gilt nicht bei gesetzlich vorgeschriebenen Pflichtprüfungen.

(3) Ausschlußfristen

Ein Schadensersatzanspruch kann nur innerhalb einer Ausschlußfrist von einem Jahr geltend gemacht werden, nachdem der Anspruchsberechtigte von dem Schaden und von dem anspruchsbegründenden Ereignis Kenntnis erlangt hat, spätestens aber innerhalb von 5 Jahren nach dem anspruchsbegründenden Ereignis. Der Anspruch erlischt, wenn nicht innerhalb einer Frist von sechs Monaten seit der schriftlichen Ablehnung der Ersatzleistung Klage erhoben wird und der Auftraggeber auf diese Folge hingewiesen wurde.

Das Recht, die Einrede der Verjährung geltend zu machen, bleibt unberührt. Die Sätze 1 bis 3 gelten auch bei gesetzlich vorgeschriebenen Prüfungen mit gesetzlicher Haftungsbeschränkung.

52001
1/2002

10 Ergänzende Bestimmungen für Prüfungsaufträge

(1) Eine nachträgliche Änderung oder Kürzung des durch den Wirtschaftsprüfer geprüften und mit einem Bestätigungsvermerk versehenen Abschlusses oder Lageberichts bedarf, auch wenn eine Veröffentlichung nicht stattfindet, der schriftlichen Einwilligung des Wirtschaftsprüfers. Hat der Wirtschaftsprüfer einen Bestätigungsvermerk nicht erteilt, so ist ein Hinweis auf die durch den Wirtschaftsprüfer durchgeführte Prüfung im Lagebericht oder an anderer für die Öffentlichkeit bestimmter Stelle nur mit schriftlicher Einwilligung des Wirtschaftsprüfers und mit dem von ihm genehmigten Wortlaut zulässig.

(2) Widerruft der Wirtschaftsprüfer den Bestätigungsvermerk, so darf der Bestätigungsvermerk nicht weiterverwendet werden. Hat der Auftraggeber den Bestätigungsvermerk bereits verwendet, so hat er auf Verlangen des Wirtschaftsprüfers den Widerruf bekanntzugeben.

(3) Der Auftraggeber hat Anspruch auf fünf Berichtsausfertigungen. Weitere Ausfertigungen werden besonders in Rechnung gestellt.

11. Ergänzende Bestimmungen für Hilfeleistung in Steuersachen

(1) Der Wirtschaftsprüfer ist berechtigt, sowohl bei der Beratung in steuerlichen Einzelfragen als auch im Falle der Dauerberatung die vom Auftraggeber genannten Tatsachen, insbesondere Zahlenangaben, als richtig und vollständig zugrunde zu legen; dies gilt auch für Buchführungsaufträge. Er hat jedoch den Auftraggeber auf von ihm festgestellte Unrichtigkeiten hinzuweisen.

(2) Der Steuerberatungsauftrag umfaßt nicht die zur Wahrung von Fristen erforderlichen Handlungen, es sei denn, daß der Wirtschaftsprüfer hierzu ausdrücklich den Auftrag übernommen hat. In diesem Falle hat der Auftraggeber dem Wirtschaftsprüfer alle für die Wahrung von Fristen wesentlichen Unterlagen, insbesondere Steuerbescheide, so rechtzeitig vorzulegen, daß dem Wirtschaftsprüfer eine angemessene Bearbeitungszeit zur Verfügung steht.

(3) Mangels einer anderweitigen schriftlichen Vereinbarung umfaßt die laufende Steuerberatung folgende, in die Vertragsdauer fallenden Tätigkeiten:

a) Ausarbeitung der Jahressteuererklärungen für die Einkommensteuer, Körperschaftsteuer und Gewerbesteuer sowie der Vermögensteuererklärungen, und zwar auf Grund der vom Auftraggeber vorzulegenden Jahresabschlüsse und sonstiger, für die Besteuerung erforderlicher Aufstellungen und Nachweise

b) Nachprüfung von Steuerbescheiden zu den unter a) genannten Steuern

c) Verhandlungen mit den Finanzbehörden im Zusammenhang mit den unter a) und b) genannten Erklärungen und Bescheiden

d) Mitwirkung bei Betriebsprüfungen und Auswertung der Ergebnisse von Betriebsprüfungen hinsichtlich der unter a) genannten Steuern

e) Mitwirkung in Einspruchs- und Beschwerdeverfahren hinsichtlich der unter a) genannten Steuern.

Der Wirtschaftsprüfer berücksichtigt bei den vorgenannten Aufgaben die wesentliche veröffentlichte Rechtsprechung und Verwaltungsauffassung.

(4) Erhält der Wirtschaftsprüfer für die laufende Steuerberatung ein Pauschalhonorar, so sind mangels anderweitiger schriftlicher Vereinbarungen die unter Abs. 3 d) und e) genannten Tätigkeiten gesondert zu honorieren.

(5) Die Bearbeitung besonderer Einzelfragen der Einkommensteuer, Körperschaftsteuer, Gewerbesteuer, Einheitsbewertung und Vermögensteuer sowie aller Fragen der Umsatzsteuer, Lohnsteuer, sonstigen Steuern und Abgaben erfolgt auf Grund eines besonderen Auftrages. Dies gilt auch für

a) die Bearbeitung einmalig anfallender Steuerangelegenheiten, z. B. auf dem Gebiet der Erbschaftsteuer, Kapitalverkehrsteuer, Grunderwerbsteuer,

b) die Mitwirkung und Vertretung in Verfahren vor den Gerichten der Finanz- und der Verwaltungsgerichtsbarkeit sowie in Steuerstrafsachen und

c) die beratende und gutachtliche Tätigkeit im Zusammenhang mit Umwandlung, Verschmelzung, Kapitalerhöhung und -herabsetzung, Sanierung, Eintritt und Ausscheiden eines Gesellschafters, Betriebsveräußerung, Liquidation und dergleichen.

(6) Soweit auch die Ausarbeitung der Umsatzsteuerjahreserklärung als zusätzliche Tätigkeit übernommen wird, gehört dazu nicht die Überprüfung etwaiger besonderer buchmäßiger Voraussetzungen sowie die Frage, ob alle in Betracht kommenden umsatzsteuerrechtlichen Vergünstigungen wahrgenommen worden sind. Eine Gewähr für die vollständige Erfassung der Unterlagen zur Geltendmachung des Vorsteuerabzuges wird nicht übernommen.

12. Schweigepflicht gegenüber Dritten, Datenschutz

(1) Der Wirtschaftsprüfer ist nach Maßgabe der Gesetze verpflichtet, über alle Tatsachen, die ihm im Zusammenhang mit seiner Tätigkeit für den Auftraggeber bekannt werden, Stillschweigen zu bewahren, gleichviel, ob es sich dabei um den Auftraggeber selbst oder dessen Geschäftsverbindungen handelt, es sei denn, daß der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Wirtschaftsprüfer darf Berichte, Gutachten und sonstige schriftliche Äußerungen über die Ergebnisse seiner Tätigkeit Dritten nur mit Einwilligung des Auftraggebers aushändigen.

(3) Der Wirtschaftsprüfer ist befugt, ihm anvertraute personenbezogene Daten im Rahmen der Zweckbestimmung des Auftraggebers zu verarbeiten oder durch Dritte verarbeiten zu lassen.

13. Annahmeverzug und unterlassene Mitwirkung des Auftraggebers

Kommt der Auftraggeber mit der Annahme der vom Wirtschaftsprüfer angebotenen Leistung in Verzug oder unterläßt der Auftraggeber eine ihm nach Nr. 3 oder sonst wie obliegende Mitwirkung, so ist der Wirtschaftsprüfer zur fristlosen Kündigung des Vertrages berechtigt. Unberührt bleibt der Anspruch des Wirtschaftsprüfers auf Ersatz der ihm durch den Verzug oder die unterlassene Mitwirkung des Auftraggebers entstandenen Mehraufwendungen sowie des verursachten Schadens, und zwar auch dann, wenn der Wirtschaftsprüfer von dem Kündigungsrecht keinen Gebrauch macht.

14. Vergütung

(1) Der Wirtschaftsprüfer hat neben seiner Gebühren- oder Honorarforderung Anspruch auf Erstattung seiner Auslagen; die Umsatzsteuer wird zusätzlich berechnet. Er kann angemessene Vorschüsse auf Vergütung und Auslagenersatz verlangen und die Auslieferung seiner Leistung von der vollen Befriedigung seiner Ansprüche abhängig machen. Mehrere Auftraggeber haften als Gesamtschuldner.

(2) Eine Aufrechnung gegen Forderungen des Wirtschaftsprüfers auf Vergütung und Auslagenersatz ist nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen zulässig.

15. Aufbewahrung und Herausgabe von Unterlagen

(1) Der Wirtschaftsprüfer bewahrt die im Zusammenhang mit der Erledigung eines Auftrages ihm übergebenen und von ihm selbst angefertigten Unterlagen sowie den über den Auftrag geführten Schriftwechsel zehn Jahre auf.

(2) Nach Befriedigung seiner Ansprüche aus dem Auftrag hat der Wirtschaftsprüfer auf Verlangen des Auftraggebers alle Unterlagen herauszugeben, die er aus Anlaß seiner Tätigkeit für den Auftrag von diesem oder für diesen erhalten hat. Dies gilt jedoch nicht für den Schriftwechsel zwischen dem Wirtschaftsprüfer und seinem Auftraggeber und für die Schriftstücke, die dieser bereits in Urschrift oder Abschrift besitzt. Der Wirtschaftsprüfer kann von Unterlagen, die er an den Auftraggeber zurückgibt, Abschriften oder Fotokopien anfertigen und zurückbehalten.

16. Anzuwendendes Recht

Für den Auftrag, seine Durchführung und die sich hieraus ergebenden Ansprüche gilt nur deutsches Recht.