Datenschutzanforderung
Technische und organisatorische Maßnahmen des Datenschutzes

Deutsche Telekom Gruppe

Version 5.0
Stand 20.11.2015
Status final

Intern

Erleben, was verbindet.

Inhaltsverzeichnis

Inhaltsverzeichnis 2

1 Einleitung und Zielsetzung 3
1.1 Technische und organisatorische Maßnahmen 3
1.2 Aufbau des Dokuments 4
1.3 Zusammenfassung 4

2 Zutrittskontrolle 4
2.1 Grundsätzliche Anforderungen 4

3 Zugangskontrolle 7
3.1 Grundsätzliche Anforderungen 7
3.2 Maßnahmen am Arbeitsplatz des Anwenders 10

4 Zugriffskontrolle 11
4.1 Grundsätzliche Anforderungen 11

5 Weitergabekontrolle 13
5.1 Grundsätzliche Anforderungen 13
5.2 Transport über Netze 14
5.3 Logischer Zugang zu Systemen 15
5.4 Schnittstellen 16
5.5 Speicherung und Aufbewahrung 17
5.6 Sicherer Versand von Daten 18
5.7 Sichere Löschung, Entsorgung und Vernichtung 19

6 Eingabekontrolle 20
6.1 Grundsätzliche Anforderungen 20

7 Auftragskontrolle 21
7.1 Grundsätzliche Anforderungen 21

8 Verfügbarkeitskontrolle 22
8.1 Backup-Konzept 22
8.2 Disaster-Recovery 22

9 Verwendungszweckkontrolle 23
9.1 Grundsätzliche Anforderungen 23

10 Organisationskontrolle 24
10.1 Grundsätzliche Anforderungen 24

11 Anwendbarkeit 25
11.1 Geltungsbereich 25
11.2 Zielgruppen und Adressaten 25
11.3 Umsetzung 26

A Abkürzungsverzeichnis 27

B Mitgeltende Dokumente 27

C Begriffe und Definitionen 27

D Impressum 27

E Änderungshistorie 28

F Anmerkungen und Änderungsvorschläge 28

1 Einleitung und Zielsetzung

In der betrieblichen Praxis der Informations- und Kommunikationstechnik werden technische Sicherheitsmaßnahmen des Datenschutzes und der IT-Sicherheit oft konzeptionell zusammengefasst und umgesetzt. Während die IT-Sicherheit risikoorientiert ist, orientiert sich der Datenschutz vordringlich an den bestehenden gesetzlichen Vorschriften zum Schutz personenbezogener Daten. Die IT-Sicherheit muss über die mögliche Verletzung des Datenschutzes hinaus weitere Bedrohungsszenarien in Betracht ziehen, die für den Datenschützer aber nicht im Fokus stehen, da dieser stets personenbezogene Daten betrachtet. Die verschiedenen Vorgehensweisen ergänzen sich, denn IT-Sicherheit ohne die explizite Berücksichtigung der gesetzlichen und unternehmenspolitischen Anforderungen zum Datenschutz ist unvollständig.

Die Anlage zu § 9 BDSG gibt die aus Sicht des Datenschutzes zu treffenden organisatorischen und technischen Maßnahmen abstrakt vor. Das nachfolgende Anforderungsdokument soll denjenigen, die im Konzern Deutsche Telekom AG damit befasst sind die Anforderungen des Datzenschutzes umzusetzen, transparent machen, welche Maßnahmen gefordert sind und welche optional zu treffen sind. Insoweit konkretisiert dieses Dokument die gesetzlichen Anforderungen.

Die hier vorgestellten Anforderungen werden im Privacy and Security Assessment (PSA) projektbezogen konkretisiert. Soweit bei besonderen Geschäftsmodellen ergänzende Anforderungen erforderlich sind, werden diese im Einzelfall von GPR definiert und sind verbindlich zu beachten.

1.1 Technische und organisatorische Maßnahmen

In der Anlage zu §9, Satz 1, BDSG, „Technische und organisatorische Maßnahmen“ werden die Anforderungen des Datenschutzes methodisch geordnet. Die dort formulierten Anforderungen werden unter den folgenden Begriffen zusammengefasst:

1) Zutrittskontrolle
2) Zugangskontrolle
3) Zugriffskontrolle
4) Weitergabekontrolle
5) Eingabekontrolle
6) Auftragskontrolle
7) Verfügbarkeitskontrolle
8) Verwendungszweckkontrolle
9) Organisationskontrolle

Als achter Punkt des Anforderungskataloges ist „zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können“. Diese Anforderung wird im Folgenden mit dem Begriff „Verwendungszweckkontrolle“ versehen. Unter „Organisationskontrolle“ sind allgemeine Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus zu verstehen, die sich implizit aus § 9 BDSG selbst und aus einer Zusammenschau der Einzelmaßnahmen nach der Anlage zu § 9 BDSG ergeben. Hierzu gehört zum Beispiel die Verpflichtung der an einer Datenverarbeitung beteiligten Mitarbeiter, über die allgemeine Datenschutzverpflichtung hinausgehende Datenschutzschulungen wahrzunehmen.

1.2 Aufbau des Dokuments

Das Dokument ist nach den neun oben genannten Kategorien gegliedert. Zu Beginn steht – soweit vorhanden – das Zitat aus dem BDSG. Anschließend erfolgt eine Erläuterung im Fließtext.

Req n	Das Dokument definiert für alle neun oben genannten Kategorien zwingend einzuhaltende durchnummerierte Anforderungen. Diese sind durch diese Formatierung hervorgehoben.

Im Anschluss an die Anforderung erfolgt eine Erläuterung erneut im Fließtext

Umsetzungsvorschläge
Für die meisten Anforderungen werden alternative oder sich ergänzende Umsetzungsvorschläge gegeben. Dies sind konkret beschriebene mögliche technische oder organisatorische Lösungen zur Erfüllung der Anforderung.

1.3 Zusammenfassung

Geltungsbereich	Zielgruppe	Information	Normierung	Regelungstyp
national	Mitarbeiter der Deutschen Telekom	Leitlinie zur Umsetzung der technischen und organisatorischen Maßnahmen des Datenschutzes	Basiert auf dem BDSG und den Binding Corporate Rules Privacy	Datenschutzanforderung

2 Zutrittskontrolle

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „... Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)".
Mit dem Begriff „Zutritt" ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT- Systeme betrieben und genutzt werden. Dies können z.B. Rechenzentren sein, in denen Web-Server, Applikationsserver, Datenbanken, Mainframes, Speichersysteme betrieben werden und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und Netzverkabelungen befinden und verlegt sind, gehören hierzu.

2.1 Grundsätzliche Anforderungen

Req 100	Festlegung von Sicherheitsbereichen

Der Schutzbedarf eines Gebäudes bzw. Raumes ist festzustellen anhand der darin befindlichen DV-Anlagen sowie ggf. sonstiger Unterlagen auf denen personenbezogene Daten verarbeitet bzw. gespeichert werden.

Req 101	Realisierung eines wirksamen Zutrittsschutzes

Sicherheitsbereiche sowie deren Zutrittspunkte müssen gegen den Zutritt unbefugter Personen durch geeignete technische (z.B. Spezialverglasung, Einbruchmeldesystem, Drehkreuz mit Chipkarte, Vereinzelungsanlage, Schließanlage) oder organisatorische (z.B. Pförtner) Maßnahmen abgesichert werden.

Umsetzungsvorschlag: Einfriedung
Die Absicherung des Geländes kann durch Mauern oder Zäune geschehen. Dabei ist das Gelände nur durch definierte Zutrittsstellen betretbar. Bevor einzelne Räumlichkeiten betreten werden können, in denen sich

datenverarbeitende Systeme befinden, muss in der Regel der Zutritt zum Gebäude oder Gebäudeteil stattfinden. Spätestens an dieser Stelle müssen Kontroll- und Berechtigungsfunktionen implementiert sein, um einen unbefugten Zutritt zu verhindern. Innerhalb des Gebäudes ist zudem der Zutritt zu einzelnen Räumen des IT-Betriebs zusätzlich nach dem Minimalprinzip zu reglementieren.

Umsetzungsvorschlag: Absicherung der Ein- und Ausgänge
Ein- und Ausgänge sind entweder zu bewachen oder dürfen sich nur mit Hilfe von Schlüsseln, elektronischen Karten oder sonstigen Schließsystemen öffnen lassen. Ausnahmen bilden Notausgänge und Fluchtwege. Deren Nutzung muss alarmgesichert sein. Die Alarme müssen zu einer Leitstelle vermittelt werden, die umgehend die Ursache des Alarms ermittelt.

Umsetzungsvorschlag: Zutritt über PIN
Soweit eine Zutrittskontrolle ausschließlich oder zusätzlich durch PIN-Eingabe erfolgt, ist die PIN regelmäßig zu ändern und der Kreis der Personen, denen die PIN bekannt gegeben wird, auf das Need-to-Know Prinzip zu beschränken. Triviale PINs, z.B. 1234, 4711, etc. dürfen nicht als PIN verwendet werden. Soweit technisch möglich, muss die PIN mindestens 5 Stellen umfassen.

Req 102	Protokollierung des Zutritts

Der Zutritt zu Räumen, in denen personenbezogene Daten verarbeitet werden, ist (nach Möglichkeit) zu protokollieren. Die Aufbewahrungsfrist für die Protokollierung richtet sich nach den mit dem Sozialpartner vereinbarten Regelungen. Bei fehlenden Regelungen beträgt die Frist 3 Monate. Geeignete Verfahren zur Missbrauchserkennung und zur anlassbezogenen Auswertung sind mit dem Sozialpartner und dem Datenschutz zu vereinbaren.

Req 104	Festlegung zutrittsberechtigter Personen

Die Voraussetzungen sowie der Kreis der allgemein zutrittsberechtigten Personen müssen festgelegt und die Zutrittsberechtigungen zu sicherheitsrelevanten Bereichen, auf das notwendige Minimum beschränkt werden ("Prinzip der minimalen Berechtigung"). Der Zutritt ist bei fehlender Berechtigung zu verwehren. Zutrittsmittel zu Gebäuden bzw. Räumlichkeiten sind grundsätzlich personengebunden zu vergeben und dürfen nicht an Dritte weitergegeben werden. Die Nutzer sind hierfür zu sensibilisieren.

Umsetzungsvorschlag: Festlegung von Berechtigtengruppen
Die Festlegung der Berechtigungen kann durch Einordnung der Nutzer in bestimmte Gruppen erfolgen. Neben der Festlegung von Nutzergruppen innerhalb der Mitarbeiter, sind auch Berechtigungsgruppen für Fremdfirmen, Berater, Besucher, Wartungs- oder Reinigungsfirmen zu definieren

Req 105	Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus

Ein Prozess zur Beantragung, Genehmigung, Ausgabe, Verwaltung und Rücknahme von Zutrittsmitteln bzw. zum Entzug von Zutrittsrechten (einschl. Schlüssel, Sichtausweise, Transponder, Chipkartenverwaltung etc.) ist einzurichten, zu beschreiben und zwingend anzuwenden. Regelungen und Verfahren zum Sperren von Zutrittsberechtigungen sind zu beschreiben. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Zutrittsmittel und -rechte zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr erforderlichen Räumlichkeiten unverzüglich zu entziehen. Sämtliche mit Sicherheitsaufgaben betraute Personen, insbesondere der Pförtnerdienst, sind über den Weggang und Funktionsänderungen von Mitarbeitern zu unterrichten.

Umsetzungsvorschlag Sichtausweise
Für alle Zutrittsberechtigten werden Sichtausweise ausgegeben, mit denen die Zutrittsberechtigten sich im Gebäude als legitimiert ausweisen können.

Umsetzungsvorschlag: Zentrale Schlüsselverwaltung
Alle Schlüssel für ein Gebäude sind für das jeweilige Gebäude zentral zu verwalten. Dabei sind für jeden Schlüssel der ausgegeben wird, mindestens die Person die den Schlüssel erhalten hat und das Ausgabedatum des Schlüssels zu dokumentieren. Die Ausgabe ist vom Empfänger schriftlich zu quittieren. Dies kann z.B. in einer Datenbank oder in Papierform dokumentiert und archiviert werden. Die Vergabe und Rücknahme von Zutrittsmitteln und Berechtigungen ist für 3 Monate über die Rücknahme hinaus revisionssicher zu archivieren. Der Prozess muss sicherstellen, dass ausscheidende Mitarbeiter zwingend den Schlüssel abgeben müssen.

Umsetzungsvorschlag: Verwaltung elektronischer Zutrittsberechtigungen
Die Zutritte über ein elektronisches Schließsystem können in der Regel wesentlich effizienter verwaltet werden, da Berechtigungen in dem System i.d.R. protokolliert werden. Optimal ist eine Kopplung an zentrale Systeme (z.B. zentrale Identity & Accountmanagementsysteme), die über Austritte oder Umzüge von Mitarbeitern informieren können, so dass automatisiert oder teilautomatisiert Aktionen wie Sperrungen der Zutrittsberechtigung erfolgen können.

Req 106 Begleitung von Besuchern und Fremdpersonal

Es müssen schriftlich fixierte Regelungen zum Zutritt für Firmenfremde, wie Gäste oder Lieferanten, existieren. Diese Regelungen beinhalten minimal, dass Firmenfremde Ihren berechtigten Aufenthalt innerhalb der Gebäude jederzeit nachweisen können, z.B. mittels Gästeausweis, Besucherausweis, oder Lieferantenausweis. Namen und Herkunft (Firmenzugehörigkeit, Geschäftsadresse oder Privatadresse) der Personen sind zu protokollieren. Die stichprobenartige Prüfung des berechtigten Aufenthaltes innerhalb der Gebäude ist obligatorisch. Besteht ein erhöhter Schutzbedarf (ab Schutzklasse 3), ist Fremdpersonal zu begleiten bzw. während ihrer Tätigkeit zu beaufsichtigen.

Umsetzungsvorschlag: Regelungen für Reinigungskräfte/Reinigungsfirmen
Es ist zu klären ob eine Reinigung der Räumlichkeiten während der Betriebszeiten und damit unter Aufsicht möglich ist. Bei einer Reinigung außerhalb der Betriebszeiten sind geeignete Regelungen (z.B. Anforderungen an das Reinigungspersonal) zu vereinbaren.

Umsetzungsvorschlag: Regelungen für firmenfremdes Wartungspersonal vor Ort
Die Wartungsarbeiten durch Fremdpersonal vor-Ort müssen so durchgeführt werden, dass nur die beauftragten Arbeiten möglich sind. Dies kann z.B. durch Begleitung oder durch eine genaue Protokollierung/ Aufzeichnung der Tätigkeiten erfolgen. Auf jeden Fall darf nur temporär der Zutritt gewährt werden und nur in die Räume und z.B. nur für die Serverschränke, wo dies erforderlich ist.

Req 107 Überwachung der Räume außerhalb der Betriebszeiten

Das Gebäude bzw. die Räumlichkeiten, in denen sich DV-Anlagen befinden, auf denen personenbezogene oder personenbeziehbare Daten verarbeitet und/oder gespeichert werden, sind außerhalb der regulären Betriebszeiten zu überwachen.

Umsetzungsvorschlag: Kontrollbegehung
Die Überwachung kann sichergestellt werden, indem befugtes Wachpersonal regelmäßige Kontrollbegehungen vornimmt.

Umsetzungsvorschlag: Elektronische Überwachung
Die Überwachung kann auch beispielsweise in Form von Videoüberwachung oder über Bewegungsmelder erfolgen. Beides muss mit einer Meldezentrale verbunden sein.

3 Zugangskontrolle

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „...zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle)...“.
Ergänzend zur Zutrittskontrolle ist es Ziel der Zugangskontrolle zu verhindern, dass DV- Anlagen von Unbefugten benutzt werden, mit denen personenbezogene Daten gespeichert, verarbeitet oder genutzt werden.

3.1 Grundsätzliche Anforderungen

Req 201	Festlegung des Schutzbedarfs

Der Schutzbedarf des IV-Verfahrens richtet sich nach der Kritikalität der in dem IV-Verfahren verarbeiteten Daten bzw. den mit dem unbefugten Zugang verbundenen Risiko. Kann nach erfolgter Zugangskontrolle auf Daten der Datenschutzklasse 3 oder höher zugegriffen werden, dann besteht hoher Schutzbedarf (hohes Datenschutzniveau). Ansonsten ist von niedrigem bis mittlerem Schutzbedarf (mittleres Datenschutzniveau) auszugehen.

Req 202	Zugangsschutz (Authentisierung)

Der Zugang zu DV-Anlagen, auf denen Daten verarbeitet werden, darf erst nach Identifikation und erfolgreicher Authentisierung (z.B. durch Benutzername und Passwort oder Chipkarte/ PIN) der befugten Personen durch dem Stand der Technik entsprechende Sicherheitsmaßnahmen möglich sein. Der Zugang ist bei fehlender Berechtigung entsprechend zu verwehren.
Für niedriges bis mittleres Datenschutzniveau sind einfache Zugangsmechanismen wie Username und Passwort unter einigen zusätzlichen Voraussetzungen zulässig. Für ein hohes Datenschutzniveau ist eine starke Authentisierung (z.B. mittels Chipkarte/Zertifikaten und PIN) erforderlich.

Req 203	Umsetzung sicherer Zugangsverfahren (starke Authentisierung) bei Schutzbedarf „hoch“

Eine starke Authentisierung erfolgt immer auf Basis mehrerer (mindestens zwei) Merkmale wie z.B. Besitz und Wissen oder auf einer einmaligen, dem Nutzer eigenen Eigenschaft (in der Regel biometrische Verfahren).

Umsetzungsvorschlag: Chipkarte mit Zertifikaten und PIN
Im Konzern Deutsche Telekom kann zur Authentisierung auf Smartcards (TIKS-Karten/MyCard) mit Zertifikaten zugegriffen werden. Die Karte mit Zertifikaten und die Eingabe der PIN stellen eine starke Authentisierung dar.

Umsetzungsvorschlag: OneTimePassworte (OTP) + Gerät
Eine starke Authentisierung ist ebenfalls mittels OneTimePassworten möglich, die auf ein bestimmtes Gerät bei Bedarf übertragen werden (z.B. auf ein Handy) oder durch ein Gerät unter Eingabe einer PIN erzeugt werden (SecureID-Karte, OTP auf TIKS-Karte, OTP-Generator-Software auf MDAs,...).

Umsetzungsvorschlag: Einsatz biometrischer Verfahren
Biometrische Verfahren wie z.B. Stimmerkennung, Irisscan, Daumenabdruck und ähnliche stellen, wenn die Verfahren sauber aufgesetzt sind, sichere Authentisierungsverfahren dar. Allerdings wird zurzeit vom breiten Einsatz dieser Techniken abgeraten, da nicht alle Techniken bereits verlässlich sind und außerdem erhebliche Problematiken durch das notwendige Abspeichern persönlicher Merkmale bestehen. Ein sinnvolles Einsatzszenario ist am ehesten dort zu finden, wo beispielsweise ohnehin mit Spracherkennungssystemen (IVR - Interactive Voice Recognition) gearbeitet wird, wie z.B. bei Callcentern/Helpdesk. Dort könnte eine stimmbasierte Authentisierung am ehesten sinnvoll sein.

Umsetzungsvorschlag: Indirekte Anmeldung (z.B. Kerberos)
Wenn ein IV-Verfahren eine indirekte Authentisierung z.B. gegen einen zentralen Verzeichnisdienst wie das Active Directory über das Kerberos- Protokoll durchführt, entspricht das Datenschutzniveau dem des Niveaus der Anmeldung an dem zentralen Verzeichnis-/Authentisierungsdienst. Dieses Verfahren ist also für hohes Datenschutzniveau erst dann praktikabel, wenn die Anmeldung am Active Directory auf Chipkartenanmeldung umgestellt wurde.

Req 204 Umsetzung einfacher Authentisierung per Username Passwort (bis Schutzbedarf „mittel“)

Passworte müssen angemessenen Mindestregeln entsprechen wie z.B. einer minimalen Passwortlänge und Komplexität. Passworte müssen in regelmäßigen Abständen geändert werden. Erstpassworte müssen umgehend geändert werden.

Umsetzungsvorschlag: Indirekte Anmeldung (z.B. Kerberos)
Wenn ein IV-Verfahren eine indirekte Authentisierung z.B. gegen einen zentralen Verzeichnisdienst wie das Active Directory über das Kerberos- Protokoll durchführt, entspricht das Datenschutzniveau dem des Niveaus der Anmeldung an dem zentralen Verzeichnis-/Authentisierungsdienst. Dieses Verfahren ist aktuell für niedriges und mittleres Datenschutzniveau adäquat, da aktuell die Anmeldung am Active Directory auf Username Passwort basiert. Der Vorteil liegt darin, dass die nachfolgenden Passwortregeln im Active Directory bereits implementiert sind und daher übergangen werden können.

Umsetzungsvorschlag: Eigene Nutzer- und Passwortverwaltung
- Die Passworte und Prozesse müssen mindestens die Anforderungen der jeweils aktuellen Konzernrichtlinien erfüllen.
- Die Umsetzung/Einhaltung der Anforderungen an Passwortlänge, Passwortkomplexität und Gültigkeit ist soweit möglich durch technische Einstellungen sicherzustellen.
- Das Passwort darf bei der Eingabe nicht im Klartext auf dem Bildschirm sichtbar sein.
- Das Erstpasswort muss auf sicherem Wege zum Nutzer kommen und/oder dieser mindestens sofort nach erstmaliger Anmeldung aufgefordert werden, dieses zu ändern.

Req 205 Protokollierung des Zugangs

Alle erfolgreichen und abgewiesenen Zugangsversuche müssen protokolliert (verwendete Kennung, Rechner, IP-Adresse) und revisionssicher archiviert werden. Die Aufbewahrungsfrist für die Protokollierung richtet sich nach den mit dem Sozialpartner vereinbarten Regelungen. Bei fehlenden Regelungen ist von 3 Monaten auszugehen. Zur Missbrauchserkennung sind regelmäßig stichprobenartige Auswertungen vorzunehmen.

Req 206 Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk

Das Authentisierungsgeheimnis (z.B. Benutzerkennung und Passwort) darf nie ungeschützt über das Netzwerk übertragen werden.

Umsetzungsvorschlag: Verschlüsselung der Übertragungsstrecke
Zwischen IT-Systemen, z.B. vom Client zum Server, müssen die Credentials deshalb mit Verschlüsselungsverfahren vor unberechtigtem Mitlesen geschützt werden.
Beispiele sind:
- Secure Socket Layer/Transport Layer Security (SSL/TLS) in Verbindung mit validen Zertifikaten bei Web-Anwendungen (auch als https bekannt)
- Secure Shell im administrativen Bereich
- Secure Network Communication (SNC) bei der Kommunikation zwischen SAP-GUI, PAS und AAS
- Secure FTP (SFTP)
- IPSec

Umsetzungsvorschlag: Nutzung von Challenge Response Verfahren
Bei Challenge Response Verfahren wird niemals das eigentliche Authentisierungsgeheimnis übertragen. Es wird vielmehr genutzt, um eine zufällige vom Server gesendete Sequenz (Challenge) zu kodieren, so dass der Server aufgrund der korrekten Codierung auf den Besitz des Geheimnisses schließen kann. Da bei jedem Authentisierungsvorgang eine neue Challenge gesendet wird, kann das ggf. durch einen Angreifer mitgelesene Authentisierungsmerkmal hier nicht zur erneuten Anmeldung genutzt werden.

Req 207 Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen

Nach wiederholter fehlerhafter Authentisierung, muss der Zugang gesperrt werden. Ein Prozess zur Rücksetzung bzw. Entsperrung von gesperrten Zugangskennungen ist einzurichten, zu beschreiben und anzuwenden. Benutzerkennungen, welche über einen längeren Zeitraum nicht genutzt werden (max. 180 Tage), müssen automatisch gesperrt bzw. auf inaktiv gesetzt werden.

Umsetzungsvorschlag: Rücksetzung nach Authentisierung beim Helpdesk
Die Aufhebung einer Sperre kann beispielsweise auf besondere Anforderung und nach hinreichender Authentisierung des entsprechenden Benutzers (z.B. Vorsprache beim Administrator) erfolgen. Hierbei ist zu beachten, dass im Falle einer Passwortrücksetzung nicht einfache, immer gleiche oder erratbare Passworte gesetzt werden.

Umsetzungsvorschlag: Automatisierte Rücksetzung
Wenn sichergestellt werden kann, dass kein Brute-Force Angriff auf die Zugangscredentials möglich ist, können auch automatisierte Mechanismen angewendet werden. Ggf. kann über Nacht oder nach einer bestimmten Zeit eine automatische Entsperrung erfolgen. Der gesperrte Nutzer sollte dabei aber zwingend über die Sperrung informiert werden, damit er mögliche Missbrauchsversuche bemerken kann.

Req 208 Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)

Zugriffspasswörter und/oder Formulareingaben dürfen nicht auf dem Client selbst oder in seiner Umgebung unverschlüsselt/ungeschützt abgelegt werden (z.B. Speicherung im Browser, unverschlüsselte Passworttabellen, Zettel, Haftnotizen, etc.). Die Nutzer sind hierfür zu sensibilisieren.

Umsetzungsvorschlag: Deaktivierung Speicherfunktion für Passwörter und/oder Formulareingaben
Soweit das Betriebssystem bzw. die Anwendung (z.B. der Browser) die Möglichkeit bietet Passwörter und/oder Formulareingaben unverschlüsselt zu speichern, muss die Nutzung dieser Funktion technisch verhindert werden.

Umsetzungsvorschlag: Keine Speicherung von Passwörtern im Klartext
Zugriffspasswörter müssen im System zugriffssicher gespeichert werden und dürfen nicht im Klartext abgelegt werden.

Req 209 Festlegung befugter Personen

Der Kreis der Personen, die befugt Zugang zu DV-Anlagen auf oder mit denen Daten verarbeitet und/oder gespeichert werden, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung im Rahmen der laufenden Betriebsorganisation notwendige Minimum zu beschränken. Zugänge für temporär beschäftigte Personen (Berater, Praktikanten, Auszubildende) müssen individuell vergeben werden. Wieder verwendbare Kennungen (z.B. Berater1, Gast1, etc.) dürfen nicht vergeben werden.

Req 210 Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen

Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen ist einzurichten, zu beschreiben und zwingend anzuwenden. Dieser beinhaltet mindestens einen Beantragungs- und Genehmigungsprozess sowie den Prozess zur Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen.
Die Vergabe von Zugangsberechtigungen darf immer nur für diejenigen DV- Anlagen(-typen) erfolgen, zu welchen der Zugang im Rahmen der Aufgabenwahrnehmung notwendig ist ("Prinzip der minimalen Berechtigung"). Authentifizierungsmedien sowie Zugangskennungen für den Zugang zu DV-Anlagen sind grundsätzlich personengebunden zu vergeben und an ein persönliches Credential (z.B. Passwort, Token, Chipkarte) zu knüpfen (Benutzerkennung). Authentifizierungsmedien und/oder Benutzerkennung/Passwort-Kombination dürfen nicht an Dritte weitergegeben werden. Die Nutzer sind hierfür zu sensibilisieren.
Regelungen und Verfahren zum Sperren und datenschutzgerechten Löschen von Zugangskennungen müssen beschrieben werden. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Authentifizierungsmedien und Zugangsberechtigungen zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr benötigten DV-Anlagen, unverzüglich zu entziehen. Hierbei ist sicherzustellen, dass alle beteiligten Stellen über den Weggang bzw. Funktionsänderungen von Mitarbeitern informiert sind (insb. IT-/Berechtigungsadministration).

Umsetzungsvorschlag: Anschluss an zentrale Verzeichnisse (z.B. Active Directory)
Eine erste Maßnahme wäre, keine eigene Benutzerverwaltung bzw. ein eigenes Directory zu nutzen, sondern auf bestehende zentrale Verzeichnisse wie z.B. das Active Directory zurückzugreifen. So ist bei Ausscheiden des Mitarbeiters aus dem Unternehmen sichergestellt, dass der Zugang lokal nicht mehr möglich ist.

Umsetzungsvorschlag: Papierworkflow und Archivierung
Ein Prozess zum Management von Accounts kann auf der Basis eines Papierworkflows umgesetzt werden. Hierbei müssen Accounts schriftlich beantragt und von den relevanten Genehmigern unterschrieben werden. Erst dann darf ein Account eingerichtet werden. Die Anträge müssen aufbewahrt werden, so dass jederzeit ein Abgleich zwischen bestehenden und beantragten Accounts möglich ist. Dieser Abgleich muss je nach Kritikalität der Anwendung ggf. mehrmals jährlich durchgeführt werden. Der Entzug der Accounts muss dann ebenfalls dokumentiert erfolgen. Dieses Vorgehen empfiehlt sich nur für eine kleinere Anzahl von Usern, da der Aufwand erheblich ist um den Überblick zu behalten.

Umsetzungsvorschlag: Elektronischer Workflow
Optimal ist eine Kopplung an zentrale Systeme (z.B. zentrale Identity & Accountmanagementsysteme oder elektronische Bestellsysteme), die auch über Austritte von Mitarbeitern oder Wechsel in der Aufgabe informieren können, so dass automatisiert oder teilautomatisiert Aktionen wie Sperrungen der Accounts erfolgen können. In diesen elektronischen Workflowsystemen können Beantragungs- und Genehmigungsprozesse effizient abgebildet werden und alles automatisiert dokumentiert werden

3.2 Maßnahmen am Arbeitsplatz des Anwenders

Req 211 Automatische Zugangssperre

Bei mehr als fünf Minuten Inaktivität der Arbeitsstation bzw. des Terminals muss ein kennwortgeschützter Bildschirmschoner mit Hilfe der betriebssystemeigenen Mechanismen automatisch aktiviert werden.

Req 212 Manuelle Zugangssperre

Arbeitsstationen und Terminals sind bei vorübergehendem Verlassen des Arbeitsplatzes gegen unbefugte Nutzung zu schützen (z.B. durch manuelle Aktivierung des kennwortgeschützten Bildschirmschoners, durch Sperrung des Systems über den Task- Manager oder Abmeldung). Die Mitarbeiter sind hierfür zu sensibilisieren.

4 Zugriffskontrolle

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „...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)".
Die Anforderungen der Zugriffskontrolle sind darauf ausgerichtet, dass nur durch Berechtigte auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass die Daten nicht durch Unbefugte manipuliert oder gelesen werden können.

4.1 Grundsätzliche Anforderungen

Req 301 Erstellen eines Berechtigungskonzepts

Ein Berechtigungskonzept (Benutzer- und Administrationsberechtigungen) stellt sicher, dass der Zugriff auf Daten des Systems nur in dem Umfang ermöglicht wird, wie es für die jeweilige Aufgabenerledigung gemäß interner Aufgabenverteilung und Funktionstrennung des Benutzers erforderlich ist. Regelungen und Verfahren zum Anlegen, Ändern und datenschutzgerechten Löschen von Berechtigungsprofilen bzw. Benutzerrollen sind darin zu beschreiben. Aus dem Berechtigungskonzept muss hervorgehen, welche Aufgabenträger Administrationsaufgaben (System, Benutzer, Betrieb, Transport) wahrnehmen und welche Benutzergruppen, welche Aktivitäten im System durchführen können. Verantwortlichkeiten sind geregelt.

Req 302 Umsetzung von Zugriffsbeschränkungen

Mit jeder Zugangsberechtigung muss eine Zugriffsberechtigung verknüpft sein, beispielsweise durch die Verknüpfung mit einer oder mehrere im Berechtigungskonzept definierten Rollen. Jeder Zugangsberechtigte darf nur mit den Anwendungen und innerhalb dieser Anwendungen nur auf die Daten zugreifen, die er zur auftragsgemäßen Bearbeitung des jeweils aktuellen Vorgangs konkret benötigt und die in dem individuellen Berechtigungsprofil eingerichtet sind. Soweit Datenbestände mehrerer Auftraggeber in einer Datenbank gespeichert oder mit einer Datenverarbeitungsanlage verarbeitet werden, sind logische Zugriffseinschränkungen vorzusehen, die ausschließlich auf die Datenverarbeitung für den jeweiligen Auftraggeber ausgerichtet sind (Mandantenfähigkeit). Zudem ist die Datenverarbeitung selbst soweit einzuschränken, dass ausschließlich die minimal erforderlichen Funktionen für die Verarbeitung der personenbezogenen Daten verwendet werden können. Es werden in den Datenverarbeitungsanlagen eindeutige Merkmale eingebaut, die es der zugreifenden Person ermöglicht, zu erkennen, dass es sich um eine authentische Datenverarbeitungsanlage handelt. Zudem muss sich auch der Zugriffsberechtigte gegenüber der Datenverarbeitungsanlage anhand von nachprüfbaren eindeutigen Merkmalen identifizieren und authentisieren lassen, z.B. mittels Ausweislesern an den Terminals.

Umsetzungsvorschlag: Verknüpfung von Berechtigungen an Rollen (Role Based Access Control - RBAC)
An die definierten Rollen werden konkrete und genaue Berechtigungen geknüpft. Dies sind beispielsweise lesende oder schreibende Rechte auf bestimmte Datensätze oder Auslösen bestimmter Aktionen und Prozesse in dem IV-Verfahren.

Umsetzungsvorschlag: Authentisierung einzelner kritischer Transaktionen mittels TAN
Eine weitere sehr sichere Möglichkeit ist es, dass bestimmte kritische Transaktionen innerhalb des IV-Verfahrens nur nach erneuter Authentisierung mittels einer TAN (Transaktionsnummer) aus einer Liste gestartet werden. Dieses Verfahren ist aus dem Online Banking bekannt. Damit wird sichergestellt, dass allein der Zugang mit den entsprechenden Berechtigungen noch keine massenhafte und ggf. missbräuchliche Nutzung des IV-Verfahrens ermöglicht.

Umsetzungsvorschlag: Zusätzliche Authentisierung einzelner Transaktionen durch Geheimnis des Kunden
Eine weitere sehr sichere Methode ist es, z.B. für IV-Verfahren, die in der Interaktion mit dem Kunden bedient werden, einzelne Transaktionen durch den Kunden zu autorisieren. Dies kann z.B. erfolgen, indem der Kunde ein nur ihm bekanntes Merkmal an den Bearbeiter gibt und dieser dieses zur Authentisierung des einzelnen Zugriffs nutzt. Besser ist es noch, wenn beispielsweise der Start einer Transaktion den Versand einer Einmal-PIN auf das Handy des Kunden auslöst. Der Kunde teilt dem Bearbeiter die PIN mit und dieser Authentisiert damit den Zugriff auf die Transaktion. Vorteil bei Letzterem ist, dass es sich um ein Einmalpasswort handelt und der Kunde dem Bearbeiter nicht sein Geheimnis verraten muss. Ziel dieser Methoden ist es, sicher zu stellen, dass ein Bearbeiter nicht missbräuchlich Transaktionen mit den Kundendaten aufruft. Diese Verfahren sind z.B. für den Kundenkontakt am Point of Sale (POS) oder im Callcenter geeignet.

Umsetzungsvorschlag: Reduktion des Zugriffs auf die für die Transaktion notwendigen Daten
Während einer Transaktion dürfen nur die für diese Transaktion erforderlichen Daten angezeigt werden. Dies gilt insbesondere bei Suchfunktionen. Es dürfen nur äußerst sparsam Wildcards genutzt werden und die Menge der auszugebenden Daten muss deutlich beschränkt sein.

Req 303 Vergabe minimaler Berechtigungen

Der Umfang der Berechtigungen, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung notwendige Minimum zu beschränken. Soweit bestimmte Funktionen ohne Verlust der Qualität der Datenverarbeitung zeitlich beschränkbar sind, sind Zugriffe auf die personenbezogene Daten und Berechtigungen zeitlich zu begrenzen.

Req 304 Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen

Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen und deren Prüfung ist einzurichten, zu beschreiben und zwingend anzuwenden. Regelungen und Verfahren zum Erteilen/Entziehen von Berechtigungen bzw. der Zuweisung von Benutzerrollen sind zu beschreiben. Umgesetzt werden müssen die Zugriffsrechte durch die Rechteverwaltung des IT-Systems. Berechtigungen sind an eine persönliche Benutzerkennung und an einen Account zu knüpfen. Dies schließt den Einsatz von mehreren Personen genutzten Gruppenkennungen/- passwörtern aus. Bei der Vergabe der Berechtigungen bzw. Zuweisung von Benutzerrollen dürfen immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip"). Dabei ist sicherzustellen, dass die im System abgebildete Funktionstrennung nicht durch kumulierte Berechtigungen aufgehoben wird. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Zugriffsrechte zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr benötigten DV- Anlagen und Speicherbereichen unverzüglich zu entziehen. Hierbei ist sicherzustellen, dass alle beteiligten Stellen über den Weggang bzw. Funktionsänderungen von Mitarbeitern informiert sind (insb. IT-/Berechtigungsadministration). Die Dokumentationen sind 3 Monate aufzubewahren.

Umsetzungsvorschlag: Papierworkflow und Archivierung
Ein Prozess zum Management von Rollen/Berechtigungen kann auf der Basis eines Papierworkflows umgesetzt werden. Hierbei müssen Rollen/Berechtigungen schriftlich beantragt und von den relevanten Genehmigern unterschrieben werden. Erst dann darf eine Rolle/Berechtigung eingerichtet werden. Die Anträge müssen aufbewahrt werden, so dass jederzeit ein Abgleich zwischen bestehenden und beantragten Rollen/ Berechtigungen möglich ist. Dieser Abgleich muss je nach Kritikalität der Anwendung ggf. mehrmals jährlich durchgeführt werden. Der Entzug der Rolle/Berechtigung muss dann ebenfalls dokumentiert erfolgen. Dieses Vorgehen empfiehlt sich nur für eine kleinere Anzahl von Usern, da der Aufwand erheblich ist.

Umsetzungsvorschlag: Elektronischer Workflow
Optimal ist eine Kopplung an zentrale Systeme (z.B. zentrale Identity & Accountmanagementsysteme oder elektronische Bestellsysteme), die auch über Austritte von Mitarbeitern oder Wechsel in der Aufgabe informieren können, so dass automatisiert oder teilautomatisiert Aktionen wie Entzug der Rollen/Berechtigungen erfolgen

können. In diesen elektronischen Workflowsystemen können Beantragungs- und Genehmigungsprozesse effizient abgebildet werden und alles automatisiert dokumentiert werden

Req 305 Vermeidung der Konzentration von Funktionen

Sowohl in Applikationen als auch im administrativen Bereich ist eine Konzentration von Funktionen zu vermeiden. Es ist zu vermeiden, dass durch eine geeignete Konzentration von verschiedenen Rollen bzw. Zugriffsrechten auf eine Person diese in der Kombination eine übermächtige Gesamtrolle erhalten kann und dadurch Kontrollmöglichkeiten ausgeschaltet werden. Beispielsweise kann ein Datenbank-Administrator, der gleichzeitig Anwender der Applikation ist, Transaktionen durch direkte Zugriffe auf das Datenbankmanagementsystem manipulieren oder Daten einsehen, die nicht seiner Rolle entsprechen. Insbesondere gilt dies für die Protokollierungstechniken für die Zugriffe auf personenbezogene Daten. Hier dürfen nicht dieselben Personen das Protokollierungssystem administrieren, deren unerlaubte Zugriffe ggf. erkannt werden sollen.

Req 306 Protokollierung des Datenzugriffs

Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen müssen protokolliert (Benutzerkennung, Transaktionsdetails) werden. Die Aufbewahrungsfrist für die Protokollierung richtet sich nach den mit dem Sozialpartner vereinbarten Regelungen. Bei fehlenden Regelungen ist von 3 Monaten auszugehen. Geeignete Verfahren zu Missbrauchserkennung und zur anlassbezogenen Auswertung sind mit dem Sozialpartner und dem Datenschutz zu vereinbaren.

5 Weitergabekontrolle

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „...zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer 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 (Weitergabekontrolle)“.

5.1 Grundsätzliche Anforderungen

Req 401 Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen

Es ist festzulegen welche Stellen/Personen an wen, welche Daten übermitteln dürfen und auf welchem Übertragungsweg dies geschehen soll.

Umsetzungsvorschlag: Dokumentation
Es wird schriftlich (z.B. in einer Verfahrensanweisung) festgelegt, an welche Stellen eine Übermittlung erlaubt ist und auf welchen Übermittlungswegen dies geschehen darf. Die kann durch eine datenbezogene Kommunikationsmatrix erfolgen.

Req 402 Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland

Sollte eine Weitergabe von Daten ins Ausland erfolgen sind die gesetzlichen Einschränkungen vorab zu prüfen. Hier ist insbesondere die Übermittlung in Länder außerhalb der Europäischen Union grundsätzlich nur unter zusätzlichen Bedingungen (z.B. EU –Standardvertragsklauseln) und nicht für alle Klassen von Daten möglich. Grundsätzlich ist zu beachten, dass bereits ein Zugriff aus anderen Ländern eine Übermittlung darstellt. Dies ist sowohl auf Ebene Entwicklung, Test oder Betrieb sowie auf Anwendungs-/ Nutzerebene eine relevante Fragestellung.

Req 403 Protokollierungen jeder Übermittlung oder einer repräsentativen Auswahl

Für jedes IT-/NT-System, in dem personenbezogene Daten übermittelt werden, ist eine Protokollierung der Übermittlung notwendig. In welcher Form (vollständig oder beispielweise beschreibend nach Art der Daten/ Sender und Empfänger) hängt im Einzelfall davon ab, ob die Protokollierung in einem vertretbaren Aufwand möglich ist, wer die Daten mit wem (Übermittlung zwischen zwei vertrauenswürdigen Instanzen?) austauscht und wie die Übermittlung stattfindet (verschlüsselt/unverschlüsselt). Die Aufbewahrungsfrist für die Protokollierung richtet sich nach den mit dem Sozialpartner vereinbarten Regelungen. Bei fehlenden Regelungen ist von 3 Monaten auszugehen. Geeignete Verfahren zu Missbrauchserkennung und zur Anlassbezogenen Auswertung sind mit dem Sozialpartner und dem Datenschutz zu vereinbaren.

5.2 Transport über Netze

Req 404 Sichere Datenübertragung zwischen Server und Client

Die Übertragung personenbezogener Daten zwischen Clients und Servern muss generell verschlüsselt erfolgen. Ausnahmen davon sind für Daten bis einschließlich Datenschschutzklasse 2 zulässig und nur, wenn die Übertragung innerhalb des Intranets der Deutschen Telekom erfolgt. Datenübertragungen zwischen Client und Servern die das Intranet der Deutschen Telekom verlassen, dürfen nur verschlüsselt erfolgen.

Umsetzungsvorschlag: Verschlüsselung der Übertragungsstrecke
Zwischen Client und Server, kann die Übertragung beispielsweise wie folgt geschützt werden:

- Secure Socket Layer/Transport Layer Security (SSL/TLS) in Verbindung mit validen Zertifikaten bei Web-Anwendungen (auch als https bekannt)
- Secure Shell
- Secure Network Communication (SNC) bei der Kommunikation zwischen SAP-GUI, PAS und AAS
- Secure FTP (SFTP)
- IPSec
- VPN-Technologien
- RPC mit Verschlüsselungsoption RC4
- SFTP
- SQLNet mit Advanced Security Option (ASO).
- XML Dateien verschlüsseln mit XML Encryption bei SOAP-Protokollen

Req 405 Sicherung der Übertragung im Backend

Werden personenbezogene Daten innerhalb des Backends zwischen einzelnen Systemen ausgetauscht, so ist genau zu betrachten, wie die einzelnen Verbindungen gegen unbefugten Zugriff geschützt sind. Verlassen die Daten nicht den gesicherten Bereich des Rechenzentrums und kann ausgeschlossen werden, dass beispielsweise die Administratoren der Netzkomponenten die Daten abfangen können, dann kann auf die Verschlüsselung der Übertragungsstrecke bis Datenschutzklasse 2 verzichtet werden. Daten der Datenschutzklasse 3 oder höher sind beim Transport zu verschlüsseln. Sobald die Daten über längere Strecken (beispielsweise zu einem anderen Rechenzentrum) übertragen werden, ist die Verschlüsselung des Transports zwingend notwendig.

Umsetzungsvorschlag: Verschlüsselung der Übertragungsstrecke
Zwischen Client und Server, kann die Übertragung beispielsweise wie folgt geschützt werden:

- Secure Shell
- Secure FTP (SFTP)
- IPSec
- VPN-Technologien
- RPC mit Verschlüsselungsoption RC4
- SFTP

- SQLNet mit Advanced Security Option (ASO).
- XML Dateien verschlüsseln mit XML Encryption bei SOAP-Protokollen

Req 406 Übertragung zu externen Systemen

Werden personenbezogene Daten zu externen Systemen (außerhalb des Bereichs der Deutschen Telekom) übertragen, ist eine Verschlüsselung ab Datenschutzklasse 2 generell erforderlich.

Umsetzungsvorschlag: Verschlüsselung der Übertragungsstrecke
Zwischen Client und Server, kann die Übertragung beispielsweise wie folgt geschützt werden:

- Secure Shell
- Secure FTP (SFTP)
- IPSec
- VPN-Technologien
- RPC mit Verschlüsselungsoption RC4
- SFTP
- SQLNet mit Advanced Security Option (ASO).
- XML Dateien verschlüsseln mit XML Encryption bei SOAP-Protokollen
- E-Mail Verschlüsselung mittels S/MIME oder PGP

5.3 Logischer Zugang zu Systemen

Req 407 Risikominimierung durch Netzseparierung

Um das Risiko zu mindern, dass personenbezogene Daten, die zwischen IT-Systemen weitergegeben werden, auf dem Netz mitgelesen werden, müssen für diese IT-Systeme Netzsegmente gebaut werden. Solche Netzsegmente können mit Hilfe von Switches und Routern konfiguriert werden. Datenpakete, egal auf welcher Ebene, verlassen und erreichen die IT-Systeme in diesen Segmenten nur über definierte Schnittstellen, an denen weitere Maßnahmen der Weitergabekontrolle ergriffen werden können. Diese Segmentierung muss mindestens eine Trennung zwischen Frontend- und Backendsystemen vorsehen. Innerhalb des Backends wird eine sinnvolle Segmentierung ebenfalls dringend empfohlen.

Umsetzungsvorschlag: Schutz der Backendsysteme
Die Backendsysteme müssen in einem eigenen Netzsegment stehen, dass gegenüber jeglichen Netzen, aus denen zugegriffen werden kann getrennt ist. Das gilt für die Nutzung z.B. aus dem Telekom Netz heraus ebenso wie für die Nutzung beispielsweise über Partnernetze oder aus dem Internet. Gleiches gilt auch für betriebliche Netzsegmente (Backup, Monitoring usw.) und administrative Netze.

Umsetzungsvorschlag: Segmentierung innerhalb der Backendsysteme
Innerhalb des Backends sollte eine Trennung ebenfalls erfolgen. Die jeweils sinnvolle Architektur kann sich stark unterscheiden. Generell sind die Backendsysteme eines IV-Verfahrens von den Backendsystemen anderer IV-Verfahren zu separieren, soweit keine gemeinsamen Ressourcen genutzt werden. Auch innerhalb der Backendarchitektur des IV-Verfahrens ist eine Separierung beispielsweise der Webserver von den Applikations- und Datenbankservern sinnvoll.

Req 408 Implementation von Sicherheitsgateways an den Netzübergabepunkten

Die IT-/NT-Systeme, auf denen personenbezogene Daten verarbeitet werden, sind durch dem aktuellen Stand der Technik entsprechende Maßnahmen (i.d.R. Firewalls) vor unerwünschten Zugriffen oder Datenströme sowohl aus dem eigenen wie auch aus anderen Netzen zu schützen. Unabhängig davon, ob es sich um Netzwerk-/Hardware-Firewalls oder ergänzend dazu um hostbasierte Firewalls handelt, müssen diese dauerhaft aktiviert sein. Jedwede Deaktivierung oder Umgehung der Funktionen durch den Anwender muss dabei wirksam

ausgeschlossen werden. Das Regelwerk muss so aufgesetzt werden, dass alle Kommunikationsbeziehungen außer den notwendigen automatisch geblockt werden.

Umsetzungsvorschlag: Firewalls, IP-Filter
Der Verkehr zwischen den Netzübergabepunkten kann je nach eingesetzten Protokollen mit Hilfe von einfachen IP-Paketfiltern realisiert werden. Hierbei sind vom Ansatz „any-any-deny" ausgehend nur die erforderlichen Kommunikationsbeziehungen freizuschalten. Dies gilt in alle Netze, auch die administrativen oder betrieblich notwendigen Netze. Für erhöhten Schutz oder wenn Protokolle mit dynamischen Portzuweisungen genutzt werden, können entsprechende Firewalls genutzt werden.

Umsetzungsvorschlag: Netzwerk Intrusion Prevention Systeme (NIPS)
Der Einsatz von netzwerkbasierten Intrusion Prevention Systemen macht in Kombination mit IP-Filtern Sinn. Das NIPS analysiert dabei die erlaubten Kommunikationsbeziehungen auf vermeintlichen Angriffsverkehr und blockiert diesen. Der Einsatz dieser Systeme ist für besonders hohe Datenschutzanforderungen sinnvoll.

Umsetzungsvorschlag: Einsatz von Proxies/ Loadbalancern mit IP-Filtern
Der Einsatz von dedizierten Loadbalancern oder Proxies zusammen mit einem Schutz durch IP-Filter kann den Einsatz einer Firewall ersetzen und bietet ebenfalls einen hohen Schutz. Voraussetzung ist, dass die Proxies/ Loadbalancer ebenfalls gehärtet und sicher konfiguriert sind.

Req 409 Härtung der Backendsysteme

Die Backendsysteme müssen gehärtet werden, damit ein unbefugter Angreifer nicht aufgrund von Schwachstellen im System sich unbefugten Zugriff auf die Systeme und Daten verschaffen kann. Dazu gibt es neben den Security Requirements der DTAG weitere allgemeingültige Best Practices. Bei einer Systemhärtung sind mindestens die folgenden Punkte zu beachten:

- aktueller Patchstand
- alle nicht benötigten Softwareelemente sind zu deinstallieren
- alle nicht benötigten Dienste sind zu deinstallieren/ deaktivieren
- alle benötigten Dienste sind nach Möglichkeit auf die Interfaces zu binden, wo sie benötigt werden
- nicht benötigte voreingestellte Dienstkonten sind zu löschen und voreingestellte Passworte zu ändern

Umsetzungsvorschlag: Aufsetzen von neuen Systemen nach gehärteten Standards
Neu aufzusetzende Systeme sollen nach Standardpolicies aufgesetzt werden, die den jeweiligen Härtungsrichtlinien der IT-Security entsprechen

Umsetzungsvorschlag: Durchsetzen der Härtung durch Automatismen (z.B. Group Policies)
Um eine zentrale Umsetzung und Aktualisierung der Härtungsmaßnahmen sicherzustellen, können Automatismen genutzt werden. Im Umfeld Windows Server kann z.B. durch entsprechende Active Directory Policies ein Hardening sichergestellt werden. Auch andere telekominterne Tools wie z.B. SIUX können verwendet werden.

5.4 Schnittstellen

Req 410 Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder

Alle Schnittstellen zu anderen IV-Verfahren sind zu dokumentieren. Diese Dokumentation muss mindestens die folgenden Informationen beinhalten:

- alle personenbezogenen Datenfelder
- Richtung der Übermittlung (Import/ Export)
- der jeweilige Verwendungszweck für die Übermittlung
- das IV-Verfahren/ die Schnittstelle, an das die Daten exportiert werden
- Art der Authentisierung der Schnittstelle

- Schutz der Übertragung (z.B. Verschlüsselung)

Insbesondere sind auch Import- und Exportschnittstellen aus bzw. in Dateien zu beschreiben und wie deren Verwendung technisch oder organisatorisch geschützt wird. Auch Datenmigrationen sind entsprechend als Schnittstelle zu beschreiben.

Umsetzungsvorschlag: Dokumentation im Datenschutzkonzept
Da die Informationen über die Schnittstellen essentieller Bestandteil eines Datenschutzkonzepts sind, ist die Dokumentation in diesem Rahmen zwingend.

Req 411 Umsetzung einer Maschine-Maschine-Authentsierung

Werden personenbezogene Daten zwischen IT-/NT-Systemen ausgetauscht, dann sollte jedes System über eine eindeutige und verifizierbare elektronische Identität verfügen. Damit kann das Risiko begrenzt werden, dass nicht autorisierte Systeme stellvertretend agieren und personenbezogene Daten empfangen bzw. einen autorisierten Empfänger vortäuschen können.

Umsetzungsvorschlag: SSL-Zertifikate
In der Praxis kann dies beispielsweise mit Hilfe valider SSL-Server-Zertikate erreicht werden. Dabei ist darauf zu achten, dass Zertifikate auslaufen und erneuert werden müssen. Hier müssen geeignete Mechanismen dafür sorgen, dass dies rechtzeitig erfolgen kann, sonst wird die Kommunikation abrupt gestoppt.

Umsetzungsvorschlag: Kennung und Passwort
Die Nutzung von Kennung und Passwort ist nicht zu empfehlen, da hier grundlegende Mechanismen wie Passwortwechselzyklen eingehalten werden müssen. Wenn diese Anforderungen analog Nutzerpassworten erfüllt werden können, kann die Umsetzung auch so erfolgen.

Umsetzungsvorschlag: IP-/Port-Filter
Wenn die Kommunikation zwischen zwei Systemen über vertrauenswürdige Netze erfolgt, so dass ein IP-Spoofing mit großer Wahrscheinlichkeit ausgeschlossen werden kann, dann ist die Begrenzung des Zugriffs auf die Schnittstelle per IP-/ Port-Filterung möglich. Der IP-/Port-Filter ist dabei optimalerweise am System implementieren.

5.5 Speicherung und Aufbewahrung

Req 412 Sichere Ablage von Daten

Zur sicheren Ablage personenbezogener Daten der Datenschutzklasse 3 oder höher ist eine verschlüsselte Datenablage vorzusehen. Dies gilt auch für etwaige Backups.

Umsetzungsvorschlag: Verschlüsselte Datenbanken
Die Speicherung personenbezogener Daten der Datenschutzklasse 3 oder höher in einer Datenbank kann durch Verschlüsselungsmechanismen der Datenbank abgesichert werden.

Umsetzungsvorschlag: Verschlüsselung in der Applikation
Personenbezogene Daten der Datenschutzklasse 3 oder höher, können auch im Rahmen der Applikation verschlüsselt werden, so dass in die Datenbank nur diese extra verschlüsselten Inhalte neben den unkritischen Klartextdaten abgelegt werden.

Umsetzungsvorschlag: Verschlüsselte Dateisysteme
Eine weitere Möglichkeit ist die Nutzung verschlüsselter Dateisysteme, wobei auch hier der Schlüssel zum Entschlüsseln nicht beispielsweise dem Systemadministrator direkt zugänglich sein darf.

Req 413 Automatisierte Löschung temporärer Zwischenspeicher

Temporäre Zwischenspeicher (z.B. der Browsercache oder der TEMP-Ordner des Betriebssystems) sind so zu konfigurieren, dass Ihre Inhalte sofern möglich unmittelbar bei jedem Beenden oder aber spätestens beim Start der Anwendung (z.B. des Browsers) bzw. des Betriebssystems automatisiert gelöscht werden.

Req 414 Zugriff auf lokale Zwischenspeicher

Jeder Zugriff auf etwaige lokal abgelegte Zwischenspeicher oder Datenbanken, die personenbezogene Daten enthalten, ist unzulässig. und sofern möglich technisch zu verhindern.

Req 415 Gesicherte Speicherung auf mobilen Datenträgern

Die Speicherung auf mobilen Datenträgern ist aufgrund des hohen Verlustrisikos zu vermeiden. Sollte eine Speicherung dennoch unumgänglich sein, so ist die Nutzung zu regeln und die Verschlüsselung der Daten auf dem Medium muss technisch sichergestellt sein. Nicht mehr benötigte Daten sind umgehend datenschutzgerecht zu löschen. Die verwendete Hardware ist zudem gegen Verlust/Diebstahl zu schützen (Nutzung von Kabelschlössern, geeignete verschließbare Transportbehältnisse,...).

Req 416 Einführung eines Prozesses zur Datenträgerverwaltungen

Es muss eine qualifizierte Datenträgerverwaltung existieren. Die Verwaltung der Datenträger muss dokumentieren, wie viele Datenträger mit personenbezogenen Daten für welche Aufgaben und Verarbeitungen erstellt wurden und wo diese bis zur Vernichtung gelagert werden. Über den Bestand der Datenträger ist regelmäßig eine Bestandskontrolle durchzuführen. Eine Lagerung der erstellten Datenträger in einem kontrollierten Sicherheitsbereich ist bei personenbezogenen Daten obligatorisch. Darüber hinaus wird die Anfertigung von Kopien von Datenträgern dokumentiert und für einen Zeitraum von 3 Monaten ab Beendigung des Auftrages oder der Tätigkeit aufbewahrt.

Req 417 Sichere Datenträgeraufbewahrung

Die bereitgestellten oder abgerufenen personenbezogenen Daten sind in Sicherheitsschränken, z.B. Datasafes aufzubewahren, soweit der Auftrag oder die Datenverarbeitung an sich eine Gewährleistung der Verfügbarkeit erfordert.

5.6 Sicherer Versand von Daten

Req 418 Einführung und Umsetzung von Versandvorschriften

Sollen personenbezogene Daten versendet werden, so sind diese gegen unbefugten Zugriff zu sichern.

Umsetzungsvorschlag: Verschlüsselte Datenträger
Werden Datenträger versendet, so sind diese zu verschlüsseln. Der Zugang zu den verschlüsselten Daten muss mindestens durch ein komplexes Passwort geschützt sein, dass dem Empfänger auf einem alternativen sicheren Weg mitgeteilt wird. Mittels der Verschlüsselung ist damit sichergestellt, dass auf dem Transportweg oder bei Verlust kein unbefugter Zugriff erfolgen kann.

Umsetzungsvorschlag: Sicherung des Versandweges
Werden Informationen durch Transportunternehmen im Klartext übermittelt (z.B. unverschlüsselte Datenträger oder in Dokumentenform), so dürfen die Daten nur nach vorheriger Authentisierung des Transportunternehmens (Deutsche Post AG, Spediteur, Kurierdienst, Taxifahrer, etc.), notfalls durch telefonische Rückversicherung beim Transportunternehmen, herausgegeben werden. Außerdem sind zuverlässige Transportmechanismen mit dokumentierter Empfangsbestätigung und manipulationssichere Verpackungen zu verwenden. Soweit sehr

große Datenbestände im Klartext transportiert werden (> 250.000 Datensätze) ist eine Begleitung des Transportes obligatorisch. Nach dem Transport sind die übermittelten Daten auf Vollständigkeit und Unversehrtheit zu prüfen.

5.7 Sichere Löschung, Entsorgung und Vernichtung

Req 419 Prozess zur Sammlung und Entsorgung

Ein Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von Datenträgern und Informationsträgern in Papierform ist einzurichten und zu beschreiben. Dabei werden Regelungen und Verfahren zur sicheren Sammlung und internen Weitergabe sowie zu Lagerung, Transport und Vernichtung unter Berücksichtigung medientypischer Eigenarten in einer Organisationsrichtlinie/Verfahrensanweisung beschrieben. Das datenschutzgerechte Vernichten bzw. Löschen ist arbeitsplatz- und zeitnah durchzuführen, um ein Zwischenlagern der Datenträger weitgehend zu vermeiden. Dadurch wird auch der Personenkreis, der mit den Datenträgern umgeht, eingeschränkt und die Sicherheit erhöht. Alternative Entsorgungswege sind organisatorisch auszuschließen. Die Mitarbeiter sind hierfür regelmäßig zu sensibilisieren.

Umsetzungsvorschlag: Sichere Entsorgung von Papierdaten
Kleinmengen können über einen örtlichen Reißwolf/Multishredder (z.B. sog. „One- 4-All-Geräte“) mit Partikelschnitt (z.B. Kreuzschnitt) vernichtet werden, der mindestens die Anforderungen der Sicherheitsstufe P-3 nach DIN 66399 erfüllt. Jedes Gerät muss der Norm entsprechend gekennzeichnet sein.

Umsetzungsvorschlag: Sammelstellen
Soweit eine Zwischenlagerung erforderlich ist, sind die Datenträger und Informationsträger vor unbefugter Entnahme bzw. Zugriff zu schützen. Soweit hierfür allgemeinzugängliche Sammelbehälter eingesetzt werden, so müssen diese (z.B. durch Nummernfolge oder über ein Barcodesystem) eindeutig identifizierbar sein, über einen sicheren Schließmechanismus verfügen und gegen unbefugte Mitnahme gesichert sein.

Umsetzungsvorschlag: Weitergabe von Geräten/Datenträgern
Bei der Ausmusterung oder Weitergabe von Geräten mit eingebauten Datenträgern (z.B. PC/Notebook, Multifunktionskopierer, Faxgeräten) ist aus Sicherheitsgründen vor der Weitergabe an externe Stellen oder Firmen darauf zu achten, dass die internen Speicher zuvor datenschutzgerecht gelöscht werden.

Umsetzungsvorschlag: Austausch oder externe Reparatur von defekten Geräten /Datenträgern
Gehen bei Reparaturmaßnahmen defekte Geräte mit eingebauten Datenträgern (z.B. PC/Notebook, Multifunktionskopierer, Faxgeräten) mit dem Ziel des Austausches oder der Reparatur an externe Firmen und sind die darauf enthaltenen Daten nicht verschlüsselt, so sind die enthaltenen Datenträger vor der Übergabe nach Möglichkeit sicher zu löschen. Ist dies im Ausnahmefall nicht möglich (z.B. weil kein Zugriff auf das Gerät mehr möglich ist und/oder die Datenträger nicht ausgebaut werden können) oder der Datenträger selbst defekt ist und keine geeignete Löscheinrichtung zur Verfügung steht, so darf die Herausgabe nur im Rahmen eines datenschutzrechtlichen Unterauftragsverhältnisses erfolgen.

Req 420 Einführung datenschutzgerechter Lösch- und Zerstörungsverfahren

Unverschlüsselte Datenträger müssen aus Sicherheitsgründen vor deren internen Wiederverwendung (z.B. Wechsel des Hauptnutzers) oder Weitergabe an externe Stellen datenschutzgerecht gelöscht werden. Die Formatierung ist als sicheres Löschverfahren ungeeignet. Es müssen andere sichere Lösch-/ Zerstörungsverfahren gewählt werden, die eine Rekonstruktion der Daten nur mit hohem Aufwand erlauben.

Umsetzungsvorschlag: Mehrfaches Überschreiben
Eine für personenbezogene Daten bis einschließlich Datenschutzklasse 2 ausreichende physikalische Löschung kann nur erreicht werden, indem der komplette Datenträger mehrfach überschrieben wird. Die Überschreibprozedur muss bei personenbezogenen Daten bis zur Datenschutzklasse 2 aus mindestens zwei,

und bei personenbezogenen Daten ab der Datenschutzklasse 3 oder höher, aus mindestens drei Durchläufen bestehen. Beim zweiten Durchlauf muss ein zum ersten Durchlauf komplementäres Datenmuster (Bit-Folge) verwendet werden. Für den dritten Durchlauf sind Zufallsdaten anzuwenden.
Bei Datenträgern nach dem aktuellen Stand der Technik kann auch einmaliges Überschreiben ausreichend sein, wenn ein aktuelles Verfahren (z.B. Zufallsmuster) zur einmaligem Überschreiben gewählt wird. Ob diese Voraussetzungen gegeben sind, ist im Einzelfall zu prüfen, ansonsten sind die Verfahren zum mehrmaligen Überschreiben, die an den Datenschutzklassen ausgerichtet sind anzuwenden.
Datenträger, bei denen die Löschung bzw. das sichere Überschreiben nicht möglich ist (z.B. DVD/CD, defekte Datenträger) müssen vernichtet werden.

Umsetzungsvorschlag: Physikalischer Zerstörung
Die Vernichtung erfolgt durch physikalische Zerstörung der Informationsträger (Zerkleinerung oder Stoffumwandlung) und kann etwa durch fachgerechtes Shreddern erfolgen, aber auch thermische Verfahren wie Verbrennen oder Einschmelzen sind geeignet. Für die Vernichtung von z.B. Papier und Kunststoffen sind mindestens die Anforderungen an den Grad der Vernichtung gemäß Sicherheitsstufe 3 nach DIN 66399 zugrunde zu legen. Magnetische oder optische Datenträger (wie z.B. Magnetbänder, Disketten, Identifikationskarten mit Magnetstreifen, CD/DVD), können analog nach den gleichen Mindeststandards physikalisch vernichtet werden.

Umsetzungsvorschlag: Magnetische Neutralisierung
Magnetische Datenträger können alternativ zur physikalischen Zerstörung auch magnetisch neutralisiert werden. Die Mindestanforderungen für z.B. Magnetbänder, Disketten, Identifikationskarten mit Magnetstreifen etc. ergeben sich aus der DIN 66399 (Löschen von schutzbedürftigen Daten auf magnetischen Datenträgern). Analog hierzu können auch die Daten auf Fest- und Wechselplatten statt durch physikalische Zerstörung durch geeignete Löschgeräte (Degausser) mittels starken Magneten vernichtet werden.

Umsetzungsvorschlag: Vertraulichkeit durch Verschlüsselung
Die Vertraulichkeit von Informationen auf elektronischen Datenträgern kann auch dadurch gewahrt bleiben, dass die Daten auf den Datenträgern verschlüsselt werden und der Zugriff auf die Informationen erst nach einer Authentifizierung des Nutzers möglich ist (z.B. mit SmartCard/Token und Passwort). Ein Vernichten/Löschen der verschlüsselten Datenträger ist dann nicht erforderlich.

Req 421 Führung von Löschprotokollen

Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit personenbezogenen Daten ist zu protokollieren. Die Protokolle sind 3 Monate revisionssicher zu archivieren.

6 Eingabekontrolle

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: "... zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)".

6.1 Grundsätzliche Anforderungen

Req 501 Protokollierung der Eingaben

Die Eingaben personenbezogener Daten in die Datenverarbeitungsanlage müssen protokolliert werden. Die Aufbewahrungsfrist für die Protokollierung richtet sich nach den mit dem Sozialpartner vereinbarten Regelungen. Bei fehlenden Regelungen ist von 3 Monaten auszugehen. Geeignete Verfahren zu Missbrauchserkennung und zur anlassbezogenen Auswertung sind mit dem Sozialpartner und dem Datenschutz zu vereinbaren.

Req 502 Dokumentation der Eingabeberechtigungen

Es muss dokumentiert sein, welche Person aufgrund ihrer Aufgabenstellung befugt und verantwortlich ist, Eingaben in der Datenverarbeitungsanlage vorzunehmen

7 Auftragskontrolle

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „...zu gewährleisten, dass personen–bezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)“.

7.1 Grundsätzliche Anforderungen

Req 601 Erstellung eines Vertrags zur Auftragsdatenverarbeitung (ADV)

Wenn personenbezogene Daten im Auftrag durch andere Stellen (auch andere Legaleinheiten innerhalb des Unternehmens) erhoben, verarbeitet oder genutzt werden, so ist ein ADV-Vertrag abzuschließen. Hierbei müssen die von GPR bereitgestellten Muster verwendet werden (datenschutz.telekom.de).

Req 602 Weisungserteilung und -entgegennahme

Es muss sichergestellt werden, dass die auf Seiten des Auftragnehmers zur Entgegennahme und Ausführung von Weisungen des Auftraggebers befugten Personen durch den Auftragnehmer verbindlich spezifiziert und z.B. in einer Weisungsmatrix dokumentiert werden. Der Auftragnehmer teilt dem Auftraggeber die zur Entgegennahme von Weisungen befugten Personen nach Auftragserteilung sowie im Falle von Änderungen umgehend mit. Sie haben sich bei der Entgegennahme von Weisungen bzw. bei der Ausübung ihrer Befugnisse gegenüber den beim Auftraggeber zuständigen Stellen zu legitimieren.

Req 603 Regelungen/Beschränkungen der Auftragsausführung

Es muss sichergestellt werden, dass durch den Auftragnehmer nur die Arbeiten durchgeführt werden, die in der zu erstellenden Leistungsbeschreibung enthalten sind. Alle darüber hinaus gehenden Arbeitsschritte müssen vorher dezidiert mit der zuständigen Stelle auf Seiten des Auftraggebers abgesprochen und schriftlich freigegeben werden. Der terminliche Ablauf der Auftragsausführung muss vorab zwischen Auftraggeber und Auftragnehmer abgestimmt werden. Der Auftraggeber muss verfahrenstechnisch eine Kontrolle der elektronischen und papiergebundenen Aufträge sicherstellen. Das „Vier-Augen-Prinzip“ für die Genehmigung und für die Kontrolle von Aufträgen und Arbeitsergebnissen ist anzuwenden. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen, wenn Fehler festgestellt werden oder anderen Unregelmäßigkeiten beim Umgang mit Daten des Auftraggebers. Der Auftragnehmer wird diese unverzüglich beheben. Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Daten, Unterlagen und Betriebsmittel erfolgen.

Req 604 Protokollierung der Auftragsausführung durch den Auftragnehmer

Es muss vereinbart werden, dass der Auftragnehmer durch eine geeignete Dokumentation die lückenlose Nachvollziehbarkeit der einzelnen im Rahmen der Auftragsausführung erforderlichen Arbeitsschritte gewährleistet und auf Anforderung belegen kann, dass der jeweilige Auftrag strikt nach den Weisungen des Auftraggebers durchgeführt wurde (Mindestangaben: Auftraggeber/Kunde, Aktion/Teilauftrag, genaue Spezifikation der Verarbeitungsschritte/-parameter, Bearbeiter, Termine, ggf. Empfänger). Die Protokolle sind 3 Monate revisionssicher zu archivieren.

8 Verfügbarkeitskontrolle

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „...zu gewährleisten, dass personen–bezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)“.

8.1 Backup-Konzept

Req 701 Backup-Konzept

Um die Verfügbarkeit der Daten auch im Notfall sicherzustellen, müssen die Daten regelmäßig gesichert werden. Zu diesem Zweck muss ein Backup-Konzept erstellt werden, das befugte Mitarbeiter in die Lage versetzt, sämtliche Mittel für die Wiederherstellung der Daten so zu nutzen, dass die Daten nach einem Vorfall in angemessener Zeit wieder zur Verfügung stehen.

Umsetzungsvorschlag: Erstellung eines Backup-Konzepts
Das Backup-Konzept soll Auskunft geben können über:

- Speicherort der Daten im Normalbetrieb
- Ein Bestandsverzeichnis der gesicherten Daten
- Art und Umfang der Datensicherung (Vollbackup/ inkrementelles Backup, Tages- oder Wochenbackup, verschlüsseltes Backup, ...)
- Das Verfahren zur Datensicherung und zur Rekonstruktion der gesicherten Daten und
- Den Ort der Aufbewahrung (Hinweis auf erforderliche Zutrittsmittel)

Das Backup-Konzept, muss zudem regelmäßig auf Aktualität geprüft werden, d.h. es muss sichergestellt werden, dass nur solche Daten gespeichert werden, die zu Weiterbetrieb des IT-/NT-Systems notwendig sind.

Umsetzungsvorschlag: Regelmäßige Durchführung von Datensicherungen
In dem Backup-Konzept sollte zudem festgelegt werden nach welchem Schema regelmäßig Backups stattfinden. Der erstellte Zeitplan muss unbedingt eingehalten werden. Es müssen verantwortliche Personen festgelegt werden, die den termingerechten Ablauf des Backups sicherstellen. Es muss zudem regelmäßig überprüft werden ob das Rückspielen der Daten (Notfallübungen) vollständig und innerhalb der Zeitvorgaben möglich ist.

Umsetzungsvorschlag: Sichere Aufbewahrung von Backup-Daten
Für die Aufbewahrung der Daten gelten die gleichen Anforderungen und Sicherheitsstandards wie im laufenden Betrieb, d.h. es muss beispielsweise sichergestellt werden, dass die Anforderungen aus dem Zutrittsschutz, Zugangs- Zugriffschutz umgesetzt wurden. Ebenso sind die Daten nach den geltenden Datenschutzrichtlinien zu vernichten/zu löschen wenn diese nicht mehr benötigt werden.

8.2 Disaster-Recovery

Req 702 Notfallplan

Der Auftragnehmer ist darauf zu verpflichten, den Auftraggeber über jede Störung (z.B. vorsätzlicher Angriff intern/extern) und Außerbetriebnahme der Datenverarbeitung schnellstmöglich zu informieren. Liegen Anzeichen für eine Störung vor, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Notfallplan erforderlich, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen, insb. auch auf Seite des Auftraggebers, über den Vorfall zu unterrichten sind.

Req 703 Regelmäßige Prüfung der Notfalleinrichtungen

Es muss eine regelmäßige Prüfung der Notfalleinrichtungen wie z.B. Notstromaggregate und Überspannungsschutzeinrichtungen sowie eine permanente Überwachung der Betriebsparameter stattfinden.

9 Verwendungszweckkontrolle

In der Anlage zu §9 Satz 1 des Bundesdatenschutzgesetzes heißt es: „... zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können".

9.1 Grundsätzliche Anforderungen

Req 801 Datensparsamkeit beim Umgang mit personenbezogenen Daten

Es dürfen nur solche Daten erhoben, gespeichert oder verarbeitet werden, die unmittelbar dem eigentlichen Zweck dienen, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses zwingend notwendig sind. Dieser Zweck darf sich in keinem nachgelagerten Schritt der Verarbeitung, auch nicht nach einer Übermittlung ändern.

Umsetzungsvorschlag: Beschreibung des Verwendungszwecks der erhobenen Daten
Um die Datensparsamkeit schon bei der Datenerhebung sicherzustellen, ist der Verwendungszweck jeden Datums schon bei der Erhebung zu beschreiben. Daten die keinen zur Erfüllung der Aufgabe definierten Verwendungszweck haben, dürfen auch nicht verwendet werden. Dies gilt auch für die Verwendung von Daten bei denen der Verwendungszweck nachträglich entfallen ist, bspw. durch Kündigung oder durch einen Tarifwechsel.

Req 802 Getrennte Verarbeitung verschiedener Datensätze

Regelungen und Maßnahmen zur Sicherstellung der getrennten Verarbeitung (Speicherung, Veränderung, Löschung und Übertragung etc.) und/oder Lagerung von Daten und/oder Datenträgern mit unterschiedlichen Verwendungszwecken sind zu dokumentieren und anzuwenden.

Umsetzungsvorschlag:
Beispiele für solche Maßnahmen sind:

- Umsetzung und Dokumentation einer Funktionstrennung (z.B. Vier- Augen-Prinzip, Closed- Shop-Betrieb)
- Vorhandensein von Richtlinien und Arbeitsanweisungen
- Vorhandensein von Verfahrensdokumentation
- Umsetzung von Regelungen zur Programmierung
- Regelungen zur System- und Programmprüfung
- Umsetzung eines Abstimm- und Kontrollsystems
- Vorhandensein von Stellenbeschreibungen

Req 803 Regelmäßige Verwendungszweckkontrolle und Löschung

Die verantwortliche Stelle (der Anforderer) muss regelmässig überprüfen, ob die zu einer Person gespeicherten Daten noch erforderlich sind. Wenn diese Zweckbindung nicht mehr gegeben ist, sind die entsprechenden Daten zu löschen. Zur Umsetzung ist ein dokumentiertes Verfahren (Löschkonzept) zu etablieren.

Umsetzungsvorschlag:
Die technischen und fachlichen Einzelheiten zur regelmäßigen Überprüfung des Verwendungszwecks und der automatisierten Löschung sind in einem standardisierten Löschkonzept festzulegen (ein Template ist unter datenschutz.telekom.de abrufbar). Diese Überprüfung ist so zu gestalten, dass die maximale zulässige Speicherdauer der Daten nicht überschritten wird. Eine Überprüfung, ob die Daten grundsätzlich noch erforderlich sind muss mindestens jährlich stattfinden. Dieses Verfahrensweise gilt für alle personenbezogene Daten mit denen im Konzern umgegangen wird, insbesondere Kunden- und Beschäftigtendaten.

10 Organisationskontrolle

10.1 Grundsätzliche Anforderungen

Req 901 Umsetzung und Kontrolle geeigneter Prozesse

Für die Verarbeitung von Daten im Unternehmen müssen Prozesse und Arbeitsabläufe definiert sein. Die Umsetzung und Einhaltung der Prozesse ist zu kontrollieren.

Req 902 Umsetzung von Schulungsmaßnahmen

Alle Personen, die mit personenbezogenen Daten umgehen oder sonst an der Auftragsdurchführung beteiligt sind (z.B. sofern vereinbart Wartungsunternehmen, Datenvernichter) sind nachweislich zu folgenden Themenkomplexen zu unterweisen:

- Grundsätze des Datenschutzes, einschließlich den technisch- organisatorischen Maßnahmen
- Pflicht zur Wahrung des Datengeheimnisses und Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse einschließlich Vorgängen des Auftraggebers (BDSG §5)
- Ordnungsgemäßer und sorgfältiger Umgang mit Daten, Datenträgern und sonstigen Unterlagen
- Fernmeldegeheimnis (Verpflichtung nach §88 TKG)
- soweit erforderlich spezielle weitere Verschwiegenheitspflichten
- soweit erforderlich spezielle Hinweise, die sich aus der vertraglichen Vereinbarung und dem vorliegenden Katalog der Mindestvorgaben ergeben können.

Die Unterweisung hat durch geeignete und dem Auftrag angemessene Maßnahmen zu erfolgen und ist mindestens alle zwei Jahre, bei Bedarf (z.B. Änderung der Auftragsumstände oder gesetzlicher Bestimmungen) jedoch auch in kürzeren Abständen, zu wiederholen.

Req 903 Verpflichtung auf das Daten- und Fernmeldegeheimnis

Alle Personen, die mit personenbezogenen Daten umgehen (insbesondere auch Firmenfremde wie z.B. Gäste, Lieferanten) sind nachweislich auf das Daten- und ggf. auch auf das Fernmeldegeheimnis bzw. weitere Verschwiegenheitsverpflichtungen zu verpflichten.

Req 904 Regelungen zur internen Aufgabenverteilung

Die im Zusammenhang mit der Leistungserbringung bzw. dem DV/IT-Einsatz wahrzunehmenden Funktionen sind festzulegen. Zu unterscheiden sind hier zwei Ebenen:

- Die erste Ebene besteht aus den Funktionen, die die Leistungserbringung bzw. den IT-Einsatz ermöglichen oder unterstützen (z.B. Arbeitsvorbereitung, Datennachbereitung, Operating, Programmierung, Netzadministration, Rechteverwaltung, Revision).
- Die zweite Ebene besteht aus den Funktionen, die die zur Leistungserbringung bzw. Aufgabenerfüllung bereitstehenden IT-/NT- Systeme anwenden (z.B. Fachverantwortlicher, IT-Anwendungsbetreuer, Datenerfasser, Sachbearbeiter, Zahlungsanordnungsbefugter).

Req 905	Beachtung von Funktionstrennung und -zuordnung

Eine Funktionstrennung ist festzulegen, zu dokumentieren und zu begründen, d.h. welche Funktionen nicht miteinander vereinbar sind, also auch nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Vorgaben hierfür können aus den Aufgaben selbst, den Anforderungen dieser Vereinbarung (insb. dem Katalog der Mindestvorgaben sowie ergänzender Standards) oder aus gesetzlichen Bestimmungen resultieren. Grundsätzlich sind dabei operative Funktionen nicht mit kontrollierenden Funktionen vereinbar. Nach der Festlegung der einzuhaltenden Funktionstrennung erfolgt Zuordnung der Funktionen zu Personen.

Req 906	Einführung einer geeigneten Vertreterregelung

Im Rahmen der Aufgaben- und Funktionsverteilung sind Vertreterregelungen ebenfalls zu berücksichtigen und zu dokumentieren.

Req 909	Aufnahme in das Verfahrensverzeichnis

Bei IV-Verfahren ist sicherzustellen, dass die in nach §4e Satz 1 Nr.1 BDSG genannten Angaben in die internen Verfahrensverzeichnisse aller das Verfahren nutzenden deutschen Legaleinheiten aufgenommen werden.

Umsetzungsvorschlag:
Anforderungen aus §4e (Inhalt der Meldepflicht):
1. Name oder Firma der verantwortlichen Stelle
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,

In fast allen Konzernunternehmen wird dies durch das Bestandsführungssystem CAPE der Telekom-IT sichergestellt. Um die gesetzlich erforderlichen Daten zu erfassen ist in CAPE zwingend der Workflow zu IRON/NOR zu durchlaufen. Konzernunternehmen, die nicht alle IV-Verfahren in CAPE führen, haben GPR eine vergleichbare Dokumentation über alle genutzten IV-Verfahren quartalsweise im Adobe Acrobat Format (pdf) zur Verfügung zu stellen.

11 Anwendbarkeit

11.1 Geltungsbereich

Diese Leitlinie stellt die Umsetzung geltender datenschutzrechtlicher Vorschriften für die Telekom Gruppe in Deutschland dar. Diese Vorschriften entstammen im Wesentlichen der EG Datenschutzrichtlinie, dem Bundesdatenschutzgesetz, dem Telekommunikationsgesetz und dem Telemediengesetz.

11.2 Zielgruppen und Adressaten

Zielgruppe dieser Leitlinie sind alle Beschäftigten der Deutschen Telekom AG und Konzerngesellschaften, die mit bestehenden Systemen und in Einrichtungen der Deutschen Telekom AG arbeiten. Mitarbeiter die an neuen Projekten arbeiten nutzen die verbindlichen Datenschutzanforderungen (SDSK) des PSA-Verfahrens.

11.3 Umsetzung

Diese Leitlinie wird durch den Konzerndatenschutzbeauftragte (L GPR) für die Umsetzung in den nationalen Konzerngesellschaften freigegeben. Sie sind ein Hilfsmittel für die Fachbereiche zur Gewährleistung der Datenschutz – Compliance.

Bei der Umsetzung ist das jeweils vorrangige deutsche Recht (insbesondere das Bundesdatenschutzgesetz und das Betriebsverfassungsgesetz, das internationale und supra-nationale Recht sowie die bestehenden kollektivrechtlichen Regelungen und Beteiligungsrechte der zuständigen Arbeitnehmervertretungen zu beachten.

A Abkürzungsverzeichnis

Abkürzung	Bedeutung
GPR	Group Privacy
BDSG	Bundesdatenschutzgesetz
PSA	Privacy and Security Assessment Verfahren
SDSK	Standardisiertes Datenschutz und Sicherheitskonzept

B Mitgeltende Dokumente

Auf die folgenden Dokumente wird hingewiesen:
Binding Corporate Rules Privacy (BRCP)
Konzernrichtlinie „IT-/NT-Sicherheit“

C Begriffe und Definitionen

Begriff	Bedeutung
IT-/NT-System	Der Begriff entspricht der Definition in der Konzernrichtlinie „IT-/NT-Sicherheit“
Backend	Unter Backend versteht man die Hintergrundsysteme, die ohne direkte Endnutzerkommunikation (Fontend) (inter)agieren. Dies sind beispielsweise aktive Netzelemente, externe Speichersysteme (Cloud), Rechenzentren, etc.)

D Impressum

Herausgeber

Deutsche Telekom AG
Vorstandsbereich Datenschutz, Recht und Compliance
Group Security Policy / Group Privacy
Friedrich-Ebert-Allee 140, 53113 Bonn, Deutschland

Dateiname	Dokumentennummer	Dokumententyp
Anforderungen_techn-orga_Maßnahmen_Datenschutz v5-0 fin.docx	91133	Datenschutzanforderung

Version	Stand	Status
5.0	20.11.2015	final

Fachlicher Ansprechpartner

Group Privacy
http://datenschutz.telekom.de

Freigegeben von

Leiter Group Privacy
Dr. Claus Dieter Ulmer

Bonn, Januar 2016

Zusammenfassung

Diese Vorlage dient zur Erstellung von Leitlinien und Datenschutzanforderungen der Group Privacy.

Schlagwörter (Taxonomiebegriffe)

Datenschutz übergreifend, TOM, Schulungen Datenschutz, Datenschutz für GBS, übergreifende Regelungsdokumente, Kundendaten, Mitarbeiterdaten, Fokusdokumente TSI, Fokusdokumente TDG, nationale Datenschutzdokumente, Datenschutzhinweise, ...

E Änderungshistorie

Version	Stand	Ansprechpartner	Änderungen / Kommentar
2.0	17.07.2012	Andreas Link	Erstellung der Nachfolgeversion zu 1.3
4.0	05.02.2014	Andreas Link	Einheitliche Versionen für alle TOM Dokumente, Einpflegen von Aktualisierungen
5.0	20.11.2015	Andreas Link	Aktualisierung versch. Requirements

Hinweis: Gültig ist grundsätzlich die in myDMS aktuell hinterlegte Version des Dokuments (http://mydms.telekom.de).

F Anmerkungen und Änderungsvorschläge

Bitte richten Sie Anmerkungen und Änderungsvorschläge an die in der Änderungshistorie unter „Ansprechpartner“ angeführte E-Mail-Adresse, bitte unter Angabe des kompletten Titels des Dokuments und einer möglichst präzisen Beschreibung der Anmerkung.