EUROPEAN DATA PROTECTION SUPERVISOR

# Leitlinien zu personenbezogenen Daten und elektronischer Kommunikation in den EU-Einrichtungen


Dezember 2015

**Zusammenfassung**

Für die meisten Menschen ist elektronische Kommunikation (E-Kommunikation) wie E-Mail, Internet und Telefonie zentraler Bestandteil ihres beruflichen Alltags und ihres Privatlebens.

Heutzutage ist E-Kommunikation für einen effizienten Betrieb der meisten Organisationen von entscheidender Bedeutung, und die Organe und Einrichtungen, Ämter und Agenturen der EU („EU-Einrichtungen“) bilden hier keine Ausnahme.

Diese Leitlinien sollen den EU-Einrichtungen für die Praxis Rat und Anleitung bei der Verarbeitung personenbezogener Daten in der Nutzung von Instrumenten der E-Kommunikation bieten, um zu gewährleisten, dass sie sich an die in der für die EU-Einrichtungen geltenden Datenschutzverordnung (EG) Nr. 45/2001 („Verordnung“) niedergelegten Verpflichtungen halten.

Grundsätzlich verarbeiten Organisationen, die E-Kommunikation praktizieren, die personenbezogenen Daten ihrer Beschäftigten beispielsweise in der Verwaltung von E-Kommunikationsdiensten, bei der Gebührenabrechnung und bei der Überprüfung der rechtmäßigen Nutzung. In den meisten Fällen ist in beschränktem Umfang die private Nutzung dienstlicher Geräte erlaubt, so dass ein Eingriff eines Arbeitgebers in die Nutzung von E-Kommunikation durch Beschäftigte vermutlich auch Aspekte berührt, die unmittelbar mit deren Privatleben zu tun haben.

E-Kommunikation ist also ein vielschichtiges Thema, zu dem eine gewisse Orientierung erforderlich ist. Der Bereich gehört aber auch zu den sich am schnellsten entwickelnden Feldern der Technologie und unterliegt raschem Wandel. Daher gehen diese Leitlinien technologisch neutral an die Thematik heran und schreiben keine konkreten technischen Maßnahmen vor. Stattdessen legen diese Leitlinien klar Gewicht auf die allgemeinen Grundsätze des Datenschutzes, die den EU-Einrichtungen bei der Einhaltung der Datenschutzverordnung helfen werden.

Grundsätzlich wenden sich diese Leitlinien an die Organe und Einrichtungen der EU, doch sind sie möglicherweise auch für alle Personen oder Organisationen hilfreich, die sich für Datenschutz und E-Kommunikation interessieren; die Verordnung weist in vielerlei Aspekten Ähnlichkeiten mit der Datenschutzrichtlinie Richtlinie (EG) 95/46 auf, die in das einzelstaatliche Recht der Mitgliedstaaten sowie in innerstaatliche Vorschriften in Island, Liechtenstein und Norwegen umgesetzt wurde.

**Zusammenfassung der Empfehlungen**

Nachstehend eine Liste der Empfehlungen, auf die in den Leitlinien im Detail eingegangen wird. Der EDSB verwendet diese als Checkliste, wenn er überprüft, ob Sie Ihren in der Verordnung niedergelegten Verpflichtungen nachgekommen sind.

***Empfehlungen für bestimmte Verarbeitungsvorgänge:***

*Für Systemsicherheit und Verkehrsmanagement:*

R1: Legen Sie den Inhalt von Sicherheitsprotokollen und deren Speicherfristen im Einklang mit den Sicherheitsbedürfnissen Ihrer Einrichtung fest.

R2: Daten, die für Zwecke der Sicherheitsüberwachung erhoben wurde, dürfen *nur für diese Zwecke verwendet* werden.

R3: Sorgen Sie dafür, dass die erstellten Statistiken anonym sind.

*Für Gebührenabrechnung und Verwaltung des Haushalts:*

R4: Weisen Sie externe Anbieter an, nach Möglichkeit die Menge der den Einrichtungen für Gebührenabrechnungszwecke bereitgestellten personenbezogenen Daten auf ein Mindestmaß zu senken.

R5: Legen Sie Aufbewahrungsfristen auf der Grundlage der für die Anfechtung von Rechnungen bestehenden Fristen fest.

*Für die rechtmäßige Nutzung von E-Kommunikationsdiensten:*

R6: Verfolgen Sie einen schrittweisen Ansatz bei der Überwachung der rechtmäßigen Nutzung von E-Kommunikationsdiensten.

*Für die Aufzeichnung der Gespräche über eine bestimmte Telefonleitung:*

R7: Legen Sie in einer Verwaltungsmaßnahme genau fest, wie und warum Telefongespräche aufgezeichnet werden müssen.

R8: Unterrichten Sie Anrufer und Mitarbeiter über eine (eventuelle) Aufzeichnung von Telefongesprächen, *bevor* diese erfolgt.

*Für den Zugang zu E-Mails in Abwesenheit des Beschäftigten:*

R9: Ergreifen Sie Vorkehrungen, um möglichst selten aus Gründen der Geschäftskontinuität auf persönliche Mailboxen zugreifen zu müssen.

R10: Erarbeiten Sie eine Strategie für den Zugang zu Mailboxen von Beschäftigten in deren Abwesenheit.

*Für Verwaltungsuntersuchungen und Disziplinarverfahren:*

R11: Sorgen Sie dafür, dass der Zugriff auf E-Kommunikationsdaten durch die Vorschriften für Verwaltungsuntersuchungen und Disziplinarverfahren abgedeckt ist.

R12: Sehen Sie bei der Planung verdeckter Überwachung angemessene Garantien vor.

***Horizontale Empfehlungen, die für alle Verarbeitungsvorgänge gelten:***

R13: Sorgen Sie bei jedem Vorgang, bei dem personenbezogene Daten verarbeitet werden sollen, dafür, dass die Zwecke festgelegt, eindeutig und rechtmäßig sind.

R14: Erheben und verarbeiten Sie nur die Daten, die Sie wirklich benötigen, um Ihren/Ihre festgelegten Zweck(e) zu erreichen.

R15: Legen Sie bei jeder Verarbeitung fest, wie lange die personenbezogenen Daten gespeichert werden.

R16: Sorgen Sie bei jeder Verarbeitung dafür, dass die Daten für den festgelegten Zweck verarbeitet und nicht für Zwecke weiterverarbeitet werden, die mit dem ursprünglichen Zweck unvereinbar sind.

R17: Informieren Sie die betreffenden Personen darüber, wie ihre Daten verarbeitet werden.

R18: Erleichtern Sie den betroffenen Personen die Ausübung ihres Rechts auf Auskunft und Berichtigung.
R19: Steuern Sie die Strategien Ihrer Einrichtung für die Verarbeitung von E-Kommunikationsdaten.
R20: Melden Sie Ihre Verarbeitungen dem Datenschutzbeauftragten.
R21: Seien Sie mit Ihrer Dokumentation und Ihren Meldungen immer auf dem neuesten Stand.
R22: Schaffen Sie ein gut dokumentiertes Verfahren für das Risikomanagement, um Informationen zu schützen.
R23: Nehmen Sie in Verträge mit externen Dienstleistern Datenschutzklauseln auf.
R24: Überwachen Sie Auftragnehmer daraufhin, ob sie die Datenschutzklauseln in ihren Verträgen korrekt anwenden.

# INHALTSVERZEICHNIS

# 1. EINLEITUNG

1 Diese Leitlinien sollen den Organen und Einrichtungen der EU für die Praxis Rat und Anleitung bei der Verarbeitung personenbezogener Daten bei der Nutzung von Instrumenten der E-Kommunikation bieten, um zu gewährleisten, dass sie sich an ihre in der Verordnung niedergelegten Datenschutzverpflichtungen halten.

2 Diese Leitlinien bauen auf vorliegenden Entscheidungen und Stellungnahmen des EDSB (zu Konsultationen durch Behörden, Vorabkontrollen und Beschwerden) sowie auf den Arbeiten der Artikel 29-Datenschutzgruppe auf (in Anbetracht der Tatsache, dass weitgehende Ähnlichkeit zwischen den Begriffen und Konzepten besteht, die in den auf nationaler Ebene und für die EU-Einrichtungen geltenden Vorschriften verwendet werden, schließt sich der EDSB gegebenenfalls und sofern relevant der Auslegung dieser Begriffe und Konzepte durch die Artikel 29-Datenschutzgruppe an). Wo wir keine Stellung beziehen, übernimmt der EDSB die in diesen anderen Dokumenten niedergelegte Auslegung.

3 Grundlage dieser Leitlinien sind langjährige Erfahrungen. Ferner stützen sie sich auf den derzeit geltenden Rechtsrahmen. Es sind zwar Änderungen an den Datenschutzvorschriften für die EU-Einrichtungen absehbar, doch bleibt die hier formulierte Hilfestellung auch weiterhin gültig. Eine Änderung, die im Zuge dieser neuen Vorschriften zu erwarten ist, ist das größere Gewicht der Rechenschaftspflicht, eine Akzentverschiebung, der in diesen Leitlinien bereits Rechnung getragen wird.

4 Bei Beachtung dieser Leitlinien können Sie mit großer Sicherheit davon ausgehen, dass Sie die Vorschriften der Verordnung (EG) Nr. 45/2001 innerhalb des dargestellten Geltungsbereichs einhalten. Der EDSB wird diese Leitlinien als Maßstab für die Beurteilung der Einhaltung der Vorschriften durch Sie verwenden.

5 Wenn Sie diese Leitlinien als Mitarbeiter der IT-Abteilung oder eines anderen Dienstes einer EU-Einrichtung anwenden, ist Ihr erster Ansprechpartner für weitere Hilfestellung der Datenschutzbeauftragte Ihrer Einrichtung. Jedes Organ, jede Einrichtung und Agentur der EU verfügt über mindestens einen solchen Datenschutzbeauftragten, der Ihnen weiterhelfen kann.

6 Diese Leitlinien sind zum einen von besonderem Interesse für behördliche Datenschutzbeauftragte, Datenschutzkoordinatoren, IT-Abteilungen und andere Verwaltungsdienste, könnten zum anderen aber auch alle diejenigen interessieren, die die E-Kommunikationsressourcen der EU-Einrichtungen nutzen (alle Kategorien von Beschäftigten, MdEP, Delegierte von Mitgliedstaaten, Auftragnehmer, Besucher usw.).

## 1.1. Gliederung

7 Diese Leitlinien sind in zwei Teile unterteilt: einen Abschnitt mit allgemeinen Empfehlungen zum Datenschutz bei der Nutzung von E-Kommunikation, und einen

weiteren Abschnitt zu bestimmten Problemen mit eher gezielten Empfehlungen. Beide Abschnitte enthalten bei Bedarf zur Illustration praktische Beispiele.

**Rx: Die Empfehlungen stehen hervorgehoben in Feldern und werden unter dem Feld durch nähere Erläuterungen ergänzt**

8 Bei verpflichtenden Maßnahmen wird in unseren Empfehlungen an der Formulierung deutlich, dass es sich um eine Verpflichtung handelt: „muss“, „tun Sie dieses“, „Sie müssen“ oder andere Befehlsformen.

9 Bei Maßnahmen, die als bewährtes Vorgehen empfohlen werden, jedoch nicht vorgeschrieben sind, heißt es „Sie sollten“, „man sollte“ usw.

10 „Kann“, „könnte“ und ähnliche Formulierungen werden bei Maßnahmen verwendet, die freiwillig oder gleichermaßen geeignet sind, das gleiche Ziel zu erreichen.

11 Aus praktischen Erwägungen werden Organe, Einrichtungen, Ämter und Agenturen der EU in diesen Leitlinien als „Einrichtung“, „Ihre Einrichtung“ oder „Ihre Agentur“ bezeichnet, wobei jedoch immer alle Kategorien gemeint sind.

### 1.2. Anwendungsbereich

12 Dem Anwendungsbereich der Verordnung entsprechend gelten diese Leitlinien für alle Verarbeitungen *durch* die EU-Einrichtungen. In den meisten Fällen handelt es sich bei den betroffenen Nutzern um Beschäftigte (im weiteren Sinne des Wortes; dazu gehören beispielsweise auch abgeordnete nationale Sachverständige, Praktikanten und Subunternehmer), doch auch um Personen, die nicht zu den Einrichtungen gehören (z. B. beim Internetzugang für Gäste). Einzelne Vorschriften für verschiedene Personenkategorien mögen voneinander abweichen (z. B. bei Verwaltungsuntersuchungen gegen Personen, die dem Statut unterliegen, und gegen Personen, die dies nicht tun), doch sind sie vom Grundsatz her gleich. Letztendlich kommen die Leitlinien zur Anwendung, wenn *durch* EU-Einrichtungen E-Kommunikationsdaten von allen diesen Kategorien betroffener Personen verarbeitet werden, und dies ungeachtet der Frage, ob EU-Einrichtungen für ihre hochrangigen oder politischen Vertreter eigene oder spezifische Strategien haben.

13 Unter diese Leitlinien fallen die folgenden Arten von E-Kommunikation:

- Telefonie (Festnetz und mobil),
- E-Mail und
- Internet.

14 Gegenstand der Leitlinien ist die Verarbeitung personenbezogener Daten, die durch E-Kommunikation für folgende Zwecke generiert werden:

- Gebührenabrechnung und Verwaltung des Haushalts;
- Sicherheit und Verkehrsmanagement;
- Störfallmanagement und Fehlersuche;

- Überprüfung der rechtmäßigen Nutzung von E-Kommunikationssystemen;
- Aufzeichnung der Gespräche auf bestimmten Telefonleitungen (z. B. Notrufleitungen);
- Zugang zu E-Kommunikationsdaten eines Beschäftigten in dessen Abwesenheit;
- Verwaltungsuntersuchungen und Disziplinarverfahren.

15 Diese Leitlinien gelten NICHT für:

- Identitäts- und Zugangsmanagementsysteme;
- Überwachung durch Videoüberwachung;
- Remote-Sitzungen im Netzwerk der Organisation;
- Systeme für die Überwachung der Nutzeraktivität (wie Überwachung der Produktivität);
- lokale Speicherung (also Speicherung von Dateien auf lokalen Laufwerken);
- Kommunikation zwischen Nutzern sowie zwischen Nutzer und Server im Netzwerk der Organisation (z. B. Instant Messaging zwischen Kollegen, Zugriff auf interne Websites usw.);
- öffentliche Websites der Organisation;
- Verarbeitung personenbezogener Daten von Dritten bei der Nutzung mobiler Geräte.

## 2. EMPFEHLUNGEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN AUS BESONDEREN GRÜNDEN

16 In diesem Abschnitt wird auf spezifische Bedenken wegen der Verarbeitung personenbezogener Daten bei der Nutzung von E-Kommunikation eingegangen und werden diesbezüglich Empfehlungen formuliert. Sie sind zusätzlich zu den allgemeinen Empfehlungen in nachstehendem Abschnitt 3 unten anzuwenden. Die allgemeinen Empfehlungen gelten immer, auch wenn sie nicht ausdrücklich erwähnt werden.

### 2.1. Systemsicherheit und Verkehrsmanagement

17 Möglicherweise benötigt die E-Kommunikation Ihrer Einrichtung eine gewisse Überwachung, damit sichergestellt ist, dass sie wie vorgesehen abläuft. Diese Überwachung umfasst Verarbeitungen, mit denen Folgendes bezweckt wird:

- Gewährleistung der Sicherheit und Stabilität der Systeme;
- Aufdeckung und Verhütung von Angriffen (von innen und außen);
- Gewährleistung des reibungslosen Funktionierens der Systeme;
- Messung der Nutzung.

18 Erforderlich ist vielleicht auch eine gewisse Überwachung der Internetnutzung, um die Funktionalität (Kontrolle) und Sicherheit des Netzwerks zu gewährleisten.

R1: **Legen Sie den Inhalt von Sicherheitsprotokollen und deren Speicherfristen im Einklang mit den Sicherheitsbedürfnissen Ihrer Einrichtung fest**

19 Sie müssen die Internetüberwachung für Zwecke der Sicherheit und des Verkehrsmanagements auf das Maß beschränken, das für die Zwecke der Verarbeitung angemessen und relevant ist (siehe Absatz 95 ff. zur Datenqualität). In der Praxis bedeutet das:

- Nach Möglichkeit Einsatz weniger in die Privatsphäre eindringender Instrumente oder Technologien (wie das Sperren von Websites) und entsprechende Beschränkung der Erstellung von Protokollen;
- Beschränkung der in den Protokollen verzeichneten personenbezogenen Angaben auf das absolut Notwendige;
- Festlegung einer Frist für die Speicherung der Protokolle.

20 Internetzugangsprotokolle beispielsweise enthalten in der Regel (pro Nutzung und pro versuchtem Zugang zum Internet):

- eine Nutzerkennung und IP-Adresse;
- das Volumen der mit dem Internet ausgetauschten Daten;
- Datum und Uhrzeit des Zugangs.

21 Für die gleichen Zwecke ist möglicherweise auch eine Speicherung von E-Mail-Verkehrsdaten erforderlich. Von den EU-Einrichtungen werden am häufigsten die folgenden Felder ausgefüllt; vielleicht ist dies auch eine Anregung für Ihre Einrichtung:

- Von:
- Datum:
- Message-ID:
- An:
- Betr.:
- Versteckter Verteiler:
- Verteiler:
- Inhaltstyp:
- Absender:

22 **Aufbewahrungsfristen**: Personenbezogene Daten dürfen nur so lange, wie es für die Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, gespeichert werden (Artikel 4 Absatz 1 Buchstabe d der Verordnung). Wenn Sie den Zweck und die Art von Daten festgelegt haben, die Sie benötigen, müssen Sie bestimmen, wie lange sie gespeichert werden sollen.

R2: **Daten, die für Zwecke der Sicherheitsüberwachung erhoben wurde, dürfen *nur für diese Zwecke verwendet* werden.**

23 Der allgemeine Grundsatz der **Zweckbindung** (siehe weiter unten Abschnitt 3.4 unten) beschränkt die Weiterverwendung personenbezogener Daten, die mit dem/den ursprünglichen Zweck(en) unvereinbar ist. Bei Sicherheitsprotokollen wird dieser Grundsatz durch Artikel 6 Absatz 2 der Verordnung noch **weiter gestärkt**, der lautet: „Mit Ausnahme zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten *dürfen* personenbezogene Daten, die ausschließlich zur Gewährleistung der Sicherheit oder Kontrolle der Verarbeitungssysteme oder -vorgänge erfasst werden, *für keinen anderen Zweck verwendet werden*." Als Beispiele für die Verwendung für „Sicherheit und Kontrolle" wären Störfallmanagement, Virenscanning, die Analyse von Verstößen und die Erstellung von Statistiken über die Ressourcennutzung zu nennen. Eine Verwendung dieser Protokolle für Zwecke der Mitarbeiterbeurteilung ist nicht zulässig.

24 Ein Beispiel für die Verarbeitung für Zwecke der Sicherheit und Kontrolle ist das E-Mail-Screening zur Entfernung von Viren oder anderer Malware sowie von Spam. Hierbei werden im Wesentlichen E-Mail-Verkehrsdaten (Volumen, Art der angehängten Dateien, E-Mail-Kopfzeilen usw.) gefiltert, doch ist auch ein automatisches Filtern von Inhalten möglich, vor allem bei Spam und der Aufdeckung von vorherbestimmtem Inhalt. Auch wenn die Verarbeitung automatisch mit Hilfe besonderer Software erfolgt, kann doch auch ein manuelles Eingreifen erforderlich sein, wenn der Systemadministrator dies für richtig hält.

***Example 1:*** *Herausfiltern von Spam*

*Ihre Einrichtung filtert eingehende E-Mails, um Spam zu vermeiden. Die Mitarbeiter beklagen jedoch, dass das System bestimmte Spam-Nachrichten (falsch negative) nicht erkennt und einige erwünschte Nachrichten (falsch positive) blockiert.*
*Für eine Feinabstimmung des Systems muss ein Systemadministrator einen Blick auf die von den betreffenden Beschäftigten erwähnten Nachrichten werfen. In diesem Fall kann ein manuelles Eingreifen gerechtfertigt sein, wohingegen im Normalbetrieb Administratoren keinen Einblick in den Inhalt haben, sondern sich auf das automatische Filtern verlassen sollten.*

R3: **Sorgen Sie dafür, dass die erstellten Statistiken anonym sind**

25 Werden Internetzugangsprotokolle (automatisch oder manuell) zur **Erstellung von Statistiken** und zur Bewertung der Internetnutzung durch Ihre Einrichtung weiter ausgewertet (beispielsweise durch den Sicherheitsbeauftragten oder andere Verwaltungsstellen), sollten die Daten **anonymisiert** werden. Bei der Erstellung dieser Statistiken können zwar personenbezogene Daten verarbeitet werden, doch **müssen die Ergebnisse anonym sein**.

### 2.2. Gebührenabrechnung und Verwaltung des Haushalts

26 Es kann sein, dass Ihre Einrichtung personenbezogene Daten für die Gebührenabrechnung und die Verwaltung des Haushalts von E-

Kommunikationsdiensten wie Rechnungen für Telefongespräche mit Einzelgebührennachweis verarbeiten muss.

27 Daten, die zur Überwachung von Gebührenabrechnung und Rechnungen verarbeitet werden, **müssen auf das Notwendige beschränkt werden** (nach dem Grundsatz der Datenqualität, siehe Absatz 95 ff.). Für die Überwachung von Festnetz- und Mobiltelefongesprächen gelten die folgenden Daten im Allgemeinen als angemessen:

- Durchwahlname;
- Durchwahlnummer;
- angerufene Nummern (die drei letzten Stellen sollten aus Datenschutzgründen gelöscht werden, falls der Anbieter diese Option bereithält);
- Datum, Uhrzeit und Dauer der einzelnen Anrufe;
- Rechnungsbeträge;
- Volumen der ausgetauschten Daten (bei mobilem Internetzugang).

28 **Nicht erfasst werden müssen für Abrechnungszwecke** hingegen die **Identität der angerufenen Person**, **erfolglose Anrufversuche**, **nicht entgegengenommene Anrufe**, **erhaltene Anrufe** und **spezifische** aufgesuchte **Websites**. Unberührt davon bleibt die mögliche Notwendigkeit, im Telefon selber verpasste/getätigte Anrufe zu erfassen.

R4: **Weisen Sie externe Anbieter an, nach Möglichkeit die Menge der den Einrichtungen für Gebührenabrechnungszwecke bereitgestellten personenbezogenen Daten auf ein Mindestmaß zu senken**

29 Die für Gebührenabrechnung und Verwaltung des Haushalts benötigten Daten werden in der Regel vom E-Kommunikationsanbieter zusammen mit den Rechnungen (für Telefonie) oder von der IT-Infrastruktur Ihrer Einrichtung (für Internet- und E-Mail-Verkehrsdaten) bereitgestellt. Es ist Sache Ihrer Einrichtung, den Anbieter dahingehend anzuweisen, dass in den entsprechenden Rechnungen möglichst wenige Datenkategorien zu finden sind.

30 Nicht alle weiter oben in 2.1 oben erwähnten Datenfelder sind für Gebührenabrechnung und Verwaltung des Haushalts von Belang. So dürften beispielsweise E-Mail-Verkehrsdaten für die Gebührenabrechnung unwichtig sein, wohingegen das Volumen der mit dem Internet ausgetauschten Daten durchaus relevant sein kann, wenn der Zugang über ein Smartphone nach Volumen abgerechnet wird. Gespeichert und verwendet werden sollten nur die Felder, die für Gebührenabrechnung und Verwaltung des Haushalts von Bedeutung sind.

R5: **Legen Sie Aufbewahrungsfristen auf der Grundlage der für die Anfechtung von Rechnungen bestehenden Fristen fest**

31 Der Zeitraum, den Sie für die Speicherung von Gesprächsaufzeichnungen oder anderen Protokollen (Speicherfrist) für Zwecke der Gebührenabrechnung und der Verwaltung des Haushalts vorsehen, sollte nicht länger als der Zeitraum sein, in dem

Rechnungen für Kommunikationsdienste angefochten werden können (siehe Artikel 37 der Verordnung). Die Fristen für die Anfechtung von Rechnungen kann je nach den Verträgen variieren, die Ihre Organisation mit den Anbietern der Kommunikationsdienste abgeschlossen hat, und die Speicherfristen sollten entsprechend festgelegt werden (siehe auch Empfehlung R15).

32 Sollten Sie einige Daten länger speichern müssen, beispielsweise wegen der Finanzvorschriften oder für Rechnungsprüfungszwecke, **sollte der Zugriff** auf die Personen (oder Funktionen) **beschränkt sein**, die unmittelbar mit diesen Bereichen zu tun haben.

33 Die in den beiden vorstehenden Punkten genannten Argumente gelten auch, wenn in Ihrer Einrichtung die Mitarbeiter Kommunikationsausrüstung privat nutzen dürfen und hierfür eine Rechnung erhalten.

34 Verschiedene Einrichtungen können unterschiedliche Methoden zur Identifizierung privater und beruflicher Aktivitäten heranziehen, wie

- nachträgliche Identifizierung und Abrechnung privater Aktivitäten: Eine Einrichtung kann beispielsweise (auf der Grundlage der durchschnittlichen Nutzung durch die Einrichtung in der Vergangenheit) ein bestimmtes Datenverkehrsvolumen für die Einrichtung auf Smartphones festlegen, die Beschäftigen zur Verfügung gestellt werden, und den Nutzern den darüber hinausgehenden Datenverkehr in Rechnung stellen; bei Telefongesprächen können die Mitarbeiter aufgefordert werden, Privatgespräche anzugeben, die dann der Einrichtung zu erstatten sind;
- vorherige Anmeldung von Privatgesprächen bei der Telefonzentrale;
- vorherige Anmeldung bestimmter Anrufkategorien (z. B. Auslandsgespräche oder Gespräche mit Mobiltelefonen) bei der Telefonzentrale und Angabe des beruflichen oder privaten Charakters des Gesprächs;
- Verwendung eines persönlichen PIN-Codes für Privatgespräche.

***Example 2:*** *Erstattung von Kosten für private Telefongespräche*

*Ihre Einrichtung erlaubt die Benutzung von Diensttelefonen für Privatgespräche, sofern diese durch einen persönlichen Code vor dem Wählvorgang als solche gekennzeichnet werden. Am Ende jedes Monats erhalten die Beschäftigten eine Liste ihrer gekennzeichneten Gespräche (wobei die drei letzten Stellen der angerufenen Nummern gelöscht sind) und werden aufgefordert, die entsprechenden Kosten innerhalb eines Monats zu erstatten. Diese Aufzeichnungen werden sechs Wochen aufbewahrt, es sei denn, die Erstattung ist strittig; dann werden sie so lange aufbewahrt, bis der Streit beigelegt ist. Die Beschäftigten werden über diese Regelung (die in einer Strategie niedergelegt ist) bei ihrem Eintritt in die Einrichtung unterrichtet.*

### 2.3. Rechtmäßige Nutzung von E-Kommunikationsdiensten

35 Es kann sein, dass Ihre Einrichtung über Regeln oder eine Strategie für die rechtmäßige Nutzung von E-Kommunikationsressourcen am Arbeitsplatz verfügt. Gegenstand dieser Strategie können Themen wie Internetzugang und Benutzung von

Diensttelefonen für private Zwecke, die Überwachung des Internetzugangs und verbotene Websites sein.

### 2.3.1. Transparenz und Verfahren

36 Die Beschäftigten müssen darüber in Kenntnis gesetzt werden, ob Ihre Einrichtung die private Nutzung der E-Kommunikationsdienste der Einrichtung erlaubt. Diese Informationen sollten zumindest über Ihre Strategie für die rechtmäßige Nutzung (siehe hierzu auch die nachstehenden Abschnitte 3.5 und 3.7 unten über Information und Dokumentation) erteilt werden.

| R6: | **Verfolgen Sie einen schrittweisen Ansatz bei der Überwachung der rechtmäßigen Nutzung von E-Kommunikationsdiensten** |
|---|---|

37 Die Überwachung der rechtmäßigen Nutzung sollte begründet werden und nach einem schrittweisen Ansatz erfolgen. Liegen keine verdächtigen Aktivitäten vor, sollte überhaupt keine Überwachung von Personen durchgeführt werden. Diesem Ansatz entsprechend sollte E-Kommunikation zunächst aggregiert, also personenunspezifisch überwacht werden. Ist es für Ihre Einrichtung erforderlich, individuelle Verhaltensmuster zu überwachen, sollte die Identität der einzelnen Nutzer zunächst maskiert und nur bei Bedarf offengelegt werden.

38 Werden regelwidrige Verhaltensmuster oder Situationen entdeckt (bei Volumen, Umfang oder anderen Aktivitätsindikatoren), kann Ihre Einrichtung die Überwachung schrittweise steigern. So könnte beispielsweise der/den betreffenden Abteilung(en) zunächst eine Warnung dahingehend zugehen, dass eine unangemessene Nutzung von E-Kommunikationsressourcen festgestellt wurde und diese einzustellen ist. Wird die unangemessene Nutzung daraufhin eingestellt, besteht kein Bedarf an einer Überwachung einzelner Personen. Wird sie fortgesetzt, kann die Überwachung intensiviert werden.

39 Die Identifizierung des Nutzers sollte nur erfolgen, wenn ein konkreter Verdacht auf Fehlverhalten (wie unangemessene Nutzung von E-Kommunikationsressourcen) vorliegt, und nach einem festgelegten Verfahren oder im Rahmen einer Verwaltungsuntersuchung (siehe Beispiel 3). Der Verdacht darf nicht allgemeiner Art sein, sondern muss begründet, spezifisch und mit ersten konkreten Beweisen belegt sein. Ihr Datenschutzbeauftragter sollte über alle Fälle unterrichtet werden, in denen Ihre Einrichtung eine individuelle Überwachung in die Wege leiten möchte. In derartigen Fällen sollte(n) die betreffende(n) Person(en) so bald wie möglich informiert werden, sofern nicht eine der Ausnahmen von Artikel 20 der Verordnung greift (siehe weiter unten Abschnitt 2.6 unten über Verwaltungsuntersuchungen).

40 Die Entscheidung, eine individuelle Überwachung vorzunehmen, hat schweres Gewicht, und daher sollten die Beweise, die den Verdacht auf Fehlverhalten begründen, die Notwendigkeit einer individuellen Überwachung, die Grenzen der Untersuchung und die Verhältnismäßigkeit der eingesetzten Mittel insgesamt bewertet und dokumentiert werden. Die Entscheidung über die Überwachung eines

Mitarbeiters sollte von der für das Verfahren oder die Untersuchung zuständigen Behörde auf der entsprechenden Verwaltungsebene und im Einklang mit einer öffentlich zugänglichen Strategie Ihrer Einrichtung über die Nutzung von E-Kommunikationsressourcen gefällt werden.

41 Ihre Einrichtung muss in der Lage sein, alle Schritte in Richtung einer Überwachung zurückzuverfolgen, und für alle damit zusammenhängenden Prozesse sollte ein Prüfpfad aufbewahrt werden. Sollte der EDSB (oder eine andere Stelle) die Notwendigkeit der Überwachung in Frage stellen, sind klare Prüfpfade und dokumentierte Bewertungen der durchzuführenden Maßnahmen das, wonach der EDSB (oder eine andere Stelle) in der Untersuchung suchen wird (siehe auch den nachstehenden Abschnitt über Rechenschaftspflicht unter 3.1 unten).

### 2.3.2. Internetzugang

42 Möglicherweise möchte Ihre Einrichtung eine Liste *verbotener* Websites oder Adressen aufstellen, zu denen der Zugang gesperrt ist, wie Websites, die bekanntermaßen oder vermutlich Malware verbreiten. Vielleicht will sie auch Websites sperren, die nachweislich nicht beruflichen Zwecken dienen, wie Glücksspiel oder Pornographie. Wollen Nutzer eine solche Seite aufrufen, sollten sie darüber informiert werden, dass diese Seite gesperrt ist und warum (also darüber, zu welcher Kategorie sie gehört; es ist nicht erforderlich, vorab eine Liste intern gesperrter Websites bekanntzugeben).

43 Grundsätzlich sollte die Quelladresse der Person(en), die auf die gesperrte Seite zugreifen wollte(n), nicht protokolliert werden, während die Zieladressen (verbotener Seiten) durchaus protokolliert werden können. In der Regel gilt, dass die Erfassung von Quelladressen zum Zweck der Überprüfung der rechtmäßigen Nutzung unterbleiben sollte, solange nicht konkrete Beweise für Sicherheitsprobleme vorliegen, wie ein steiler Anstieg der Zahl der versuchten Verbindungen mit einer gesperrten Website. Dies steht im Einklang mit dem Grundsatz der Datenqualität (siehe Absatz 95).

### 2.3.3. Nutzung des Telefons

44 Möglicherweise möchte Ihre Einrichtung die rechtmäßige Nutzung von Diensttelefonen oder Mobiltelefonen daraufhin überwachen, ob die Telefone im Übermaß privat genutzt werden oder ob Beschäftigte in betrügerischer Absicht private Telefongespräche nicht angeben.

45 Es gibt eine ganze Reihe gleichermaßen zuverlässiger Möglichkeiten, die private Nutzung anzugeben. Nachträgliche Anmeldungen privater Gespräche oder Eingabe eines Codes für private Gespräche sind Beispiele im Bereich Diensttelefone (siehe vorstehenden Abschnitt 34 oben).

46 Die Überwachung mutmaßlicher Unregelmäßigkeiten bei der Angabe privater Telefongespräche durch Ihre Organisation muss sich auf objektive Kriterien stützen. Grundsätzlich sollte die Einrichtung keine allgemeinen, systematischen oder

zufälligen Kontrollen von Rechnungen vornehmen. Die Überprüfung sollte auf Rechnungen über einen Betrag jenseits einer vorab festgelegten Grenze beschränkt sein, die mit Blick auf den Durchschnittsverbrauch pro Beschäftigtem und die wahrgenommenen spezifischen Aufgaben als überhöht gelten könnten. Dieses Limit sollte in der Strategie der EU-Einrichtung erwähnt und klar benannt werden.

***Example 3:*** *Strategie für die private Nutzung von für berufliche Zwecke zur Verfügung gestellten Mobiltelefonen*

*Ihre Einrichtung stattet einige Mitarbeiter mit Mobiltelefonen für berufliche Zwecke aus, die in seltenen Fällen auch für private Anrufe genutzt werden dürfen.*
*In der Strategie, die Beschäftigten übergeben wird, die für berufliche Zwecke ein Handy beantragen, heißt es, dass in begrenztem Umfang eine private Nutzung erlaubt ist und besonders auf Roaming zu achten ist. In der Strategie ist auch eine Obergrenze für eine durchschnittliche Monatsrechnung festgelegt; wird diese Obergrenze überschritten, wird der Nutzer umgehend mit einer (vom System generierten) Textnachricht informiert und kann er aufgefordert werden, die Privatgespräche anzugeben und die über der Obergrenze liegenden zu erstatten. Wird die Obergrenze drei Monate in Folge überschritten, kann der Dienstvorgesetzte des Beschäftigten unterrichtet werden.*

47 Wurde die Obergrenze überschritten, sollte dem Beschäftigten Möglichkeit zu einer Erklärung gegeben werden, bevor irgendwelche Maßnahmen ergriffen werden. In dieser Phase sollte die Führungsebene noch keinen Zugriff auf die Rechnung mit Einzelgebührennachweis haben. Sind die Erklärungen nicht überzeugend und besteht nach wie vor ein begründeter Verdacht auf Missbrauch, kann eine Verwaltungsuntersuchung eingeleitet werden.

48 In diesem Fall sollte der Beschäftigte umgehend über die Verwaltungsuntersuchung in Kenntnis gesetzt werden, sofern nicht eine der Ausnahmen gemäß Artikel 20 der Verordnung greift (siehe hierzu auch weiter unten Abschnitt 113 unten). In der Überprüfungsphase kann der Beschäftigte aufgefordert werden, bestimmte auf der Rechnung stehende Privattelefongespräche zu begründen, die problematisch sind.

### 2.4. Aufzeichnung von Gesprächen auf bestimmten Telefonleitungen

49 Vielleicht möchte Ihre Einrichtung eingehende Anrufe für bestimmte Telefonnummern aufzeichnen, beispielsweise für Notrufleitungen oder Hotlines für Whistleblower. Die Aufzeichnung kann für einen oder mehrere Zwecke erforderlich sein, wie die Überprüfung des Inhalts einer Nachricht, damit die Mitarbeiter der Hotline angemessen reagieren können, oder für Schulungszwecke.

***Example 4:*** *Aufzeichnung von Notrufleitungen*

*Ihre Einrichtung hat eine spezielle Telefonleitung für Notrufe eingerichtet. Die Anrufe auf dieser Leitung werden aufgezeichnet. Der für die Anrufe zuständige Mitarbeiter kann die Nachricht mehrmals abhören und sie als Nachweis operativer Tätigkeiten speichern. Dies kann erforderlich sein, um den Inhalt der Nachricht abzuklären, Beweise für eventuell folgende Gerichtsverfahren oder Verwaltungsmaßnahmen zu sichern oder Mitarbeiter in ihrer Fortbildung zu unterstützen. Die Verfahren sind in einem von Ihrem Direktor gebilligten Dokument festgelegt; überall in der Einrichtung sind Plakate angebracht, auf denen über die Existenz der Hotline und über die Tatsache, dass Anrufe aufgezeichnet werden, informiert wird.*

50 Im Einklang mit dem Grundsatz der Verhältnismäßigkeit dürfen EU-Einrichtungen nicht *alle* über die Telefonzentrale oder einzelne Abteilungen ein- oder ausgehenden Anrufe aufzeichnen. Lediglich in Ausnahmefällen kann eine allgemeine Aufzeichnung der bei einer bestimmten Abteilung (weniger auf einer bestimmten Telefonleitung) eingehenden Anrufe als notwendig erachtet werden. Ihre Einrichtung muss auf jeden Fall belegen können, warum die Aufzeichnung dieser Anrufe für die Wahrnehmung ihrer Aufgaben (einschließlich operativer Tätigkeiten) *erforderlich* ist. Für nähere Informationen siehe die Fälle des EDSB 2005-0376 und 2006-0102, abrufbar auf unserer Website.

R7: **Legen Sie in einer Verwaltungsmaßnahme genau fest, wie und warum Telefongespräche aufgezeichnet werden müssen**

51 Die Einzelheiten der Aufzeichnung (welche Telefonleitungen, Speicherfristen, Zwecke, für die die Aufzeichnungen weiter verwendet werden dürfen usw.) sind, wenn keine spezifische Rechtsgrundlage besteht, auf der angemessenen Ebene in Verwaltungsmaßnahmen festzulegen.

52 Zur Rechtfertigung der Aufzeichnung von Anrufen genügt jedoch nicht allein die Aussage, die Aufzeichnung sei *erforderlich*, damit Ihre Einrichtung *ihre Aufgaben wahrnehmen* kann und/oder für ihre *Verwaltung und ihr Funktionieren* (Artikel 5 Buchstabe a und Erwägungsgrund 27 der Verordnung (EG) Nr. 45/2001). Es sind noch ergänzende Informationen zu dokumentieren. Dabei sollte erfasst werden, warum Aufzeichnungen bei diesen konkreten Leitungen erforderlich sind; zu den möglichen Gründen gehören die Sensitivität des erbrachten Dienstes, ihr hochtechnischer Charakter, die Volatilität der ausgetauschten Informationen, der eventuelle Bedarf an einem Zugang dazu in der Zukunft und eine hohe Wahrscheinlichkeit einer Streitigkeit.

53 Erfolgt die Aufzeichnung nicht kontinuierlich, sondern nur unter ganz bestimmten Umständen, wenn beispielsweise die Alarmstufe angehoben wird, muss in der Dokumentation auch das Verfahren für die Entscheidung darüber geregelt sein, wann mit der Aufzeichnung zu beginnen ist.

R8: **Unterrichten Sie sowohl Anrufer als auch Mitarbeiter über eine eventuelle Aufzeichnung von Telefongesprächen, *bevor* diese erfolgt**

54 Anrufer sind im Vorhinein darüber zu unterrichten, dass ihr Anruf aufgezeichnet wird/werden könnte. Am besten geschieht dies mit einer aufgezeichneten Ansage, bevor ein Mitarbeiter den Anruf entgegennimmt (bei Leitungen, bei denen der Faktor Zeit entscheidend ist - wie bei Notrufleitungen - können andere Möglichkeiten erwogen werden). Dieser Hinweis sollte auch gut sichtbar neben der Telefonnummer in allen Telefonverzeichnissen wie beispielsweise auf der Website der Einrichtung angebracht werden. Auch die mit diesen Telefonleitungen arbeitenden Beschäftigten sind zu informieren. Dies könnte z. B. über einen Datenschutzhinweis in unmittelbarer Nähe des Telefons und/oder in der Einweisung bei Aufnahme der Tätigkeit geschehen.

55 Eine Sprachnachricht oder eine Nachricht auf einem Anrufbeantworter könnte als Einwilligung in die Bearbeitung der hinterlassenen Nachricht gelten. Sie bedeutet allerdings nicht eine Einwilligung in irgendeine weitere Verarbeitung.

56 Whistleblowing-Hotlines gehören zu den sensibelsten Kategorien aufgezeichneter Telefonleitungen. Da es bei ihnen um mutmaßliche kriminelle Aktivitäten oder anderes schweres Fehlverhalten geht, sollten Whistleblowing-Leitungen mit Bedacht eingeführt werden, wenn sich ihre Notwendigkeit ausreichend belegen lässt. Für nähere Informationen siehe bitte die Stellungnahme 01/2006 der Artikel 29-Datenschutzgruppe und die in der Vorbereitung befindlichen Leitlinien des EDSB zum Thema Whistleblowing.

### 2.5. Zugang zu E-Mails in Abwesenheit des Mitarbeiters

57 Es kann vorkommen, dass Ihre Einrichtung aus Gründen der Geschäftskontinuität Zugang zum Inhalt von Mailboxen von Beschäftigten in deren Abwesenheit haben möchte. Dabei kann es sich beispielsweise um Beschäftigte handeln, die langfristig in Urlaub sind, die Einrichtung verlassen haben oder verstorben sind.

58 Da in der Regel in beschränktem Umfang eine private Nutzung erlaubt ist, könnte ein solcher Zugang, auch wenn er möglicherweise gerechtfertigt ist, doch einen Eingriff in das Recht auf Privatsphäre bedeuten.

R9: **Ergreifen Sie Vorkehrungen, um möglichst selten aus Gründen der Geschäftskontinuität auf persönliche Mailboxen zugreifen zu müssen**

59 Um möglichst wenig Zugang zu persönlichen Mailboxen in Abwesenheit von Beschäftigten zu benötigen, müssen Sie dafür sorgen, dass wichtige E-Mails auch an anderer Stelle zugänglich sind. Einige Beispiele:

a. Die Mitarbeiter könnten angewiesen werden, alle wichtigen E-Mails in elektronischen Fallakten wie in Dokumenten- oder Fallmanagementsystemen zu speichern oder die Korrespondenz auf Papier aufzuheben;

b. es könnten funktionale Mailboxen für bestimmte Referate/Dienststellen/Sektoren eingerichtet werden, die für alle zuständigen Beschäftigten zugänglich sind. Empfänger könnten dann aufgefordert werden, alle betriebsbezogene Korrespondenz in diese Mailboxen zu kopieren;

c. Mitarbeiter, die die Einrichtung verlassen, könnten angewiesen werden, vollständige Übergabevermerke vorzulegen.

60 Mit derartigen Maßnahmen ist ein Zugang zu persönlichen Mailboxen seltener erforderlich. Es kann jedoch trotz alledem ein Zugang zu einer persönlichen Mailbox erforderlich sein.

R10: **Erarbeiten Sie eine Strategie für den Fall, dass ein Zugang zu Mailboxen von Beschäftigten in deren Abwesenheit erforderlich ist**

61 Das Verfahren für den Zugang zu Mailboxen von Beschäftigten in deren Abwesenheit sollte in einer Strategie festgelegt sein. Diese Strategie kann Teil des allgemeinen Regelwerks für Ihre Einrichtung sein und kann auch den Zugang zu Papierakten abdecken.

62 Die Beschäftigten müssen über diese Strategie in Kenntnis gesetzt werden, und zwar sowohl allgemein, beispielsweise bei Aufnahme ihrer Tätigkeit in Ihrer Einrichtung, vielleicht mit Hilfe der Strategie für die Nutzung von E-Mails, als auch in spezifischen Fällen, wenn Ihre Einrichtung plant, auf ihre E-Mail-Accounts zuzugreifen. Dem Nutzer sollte dieser Zugriff unter Angabe der Notwendigkeit, der Dringlichkeit, der Art und des Umfangs der benötigten Informationen genau erläutert werden. Neben den Informationen, die dem Beschäftigten gemäß Artikel 12 zu geben sind (siehe Abschnitt 108), müssen die Nutzer auch etwas über ihr Recht auf Widerspruch gemäß Artikel 18 der Verordnung erfahren.

63 Ist ein Kontaktieren der Person(en) unmöglich oder erfordert es einen unverhältnismäßigen Aufwand, müssen sie nicht informiert werden (Artikel 12 Absatz 2).

64 Ist trotz der in Absatz 59 vorgeschlagenen Maßnahmen ein Zugang noch immer erforderlich, kann Ihre Einrichtung auf die Mailbox im Einklang mit Ihrer Strategie zugreifen.

65 Der Zugriff auf E-Mails ist jedoch nur unter bestimmten Voraussetzungen und bei bestimmten Garantien zulässig. Die E-Mail-Strategie Ihrer Einrichtung muss klare Regeln enthalten, nach denen ein Zugang zu E-Mails in solchen Fällen erlaubt ist. Der Zugriff sollte stufenweise ablaufen, indem beispielsweise zunächst nach bestimmten Schlüsselwörtern und Betreff-Zeilen gesucht wird, bevor an den Inhalt von Nachrichten herangegangen wird; ferner sollte der behördliche Datenschutzbeauftragte informiert werden und sollten Protokolle aufbewahrt werden, mit denen sich die Rechtmäßigkeit des Zugangs belegen lässt.

***Example 5:*** *Zugriff auf eine Mailbox, nachdem ein Mitarbeiter die Organisation verlassen hat*

*Die Vorschriften Ihrer Einrichtung besagen, dass Mitarbeiter allen relevanten Schriftwechsel in einem Dokumentenverwaltungssystem abzuspeichern haben. Dazu zählen interne E-Mails an und von Vorgesetzten über die Billigung von Dokumenten und andere Informationen, die künftige Sachbearbeiter benötigen werden. Da auch Übergabevermerke vorhanden sind, ist es eher unwahrscheinlich, dass aus Gründen der Geschäftskontinuität ein Zugang zur Mailbox des früheren Mitarbeiters tatsächlich erforderlich ist.*
*Ist er jedoch erforderlich, wird der ehemalige Mitarbeiter nach Möglichkeit informiert. Um zu vermeiden, dass private Inhalte offengelegt werden, werden die Mitarbeiter angewiesen, ihren privaten Schriftverkehr in einem entsprechend gekennzeichneten Ordner zu sammeln; auf diese Weise lässt sich das Problem leicht umgehen. Im Einklang mit den Regeln Ihrer Einrichtung werden ihre Mailboxen zwei Monate nach ihrem Ausscheiden gelöscht.*

66 Die Einwilligung ist keine geeignete Rechtsgrundlage für den Zugang zu Mailboxen in der oben beschriebenen Situation. Der Zugriff auf ein E-Mail-Account erfolgt vielmehr aus Gründen der Geschäftskontinuität und weil er für erforderlich und verhältnismäßig gehalten wird. Siehe für nähere Informationen die Stellungnahme 15/2011 der Artikel 29-Datenschutzgruppe, S. 13, und die Stellungnahme 08/2001 der Artikel 29-Datenschutzgruppe, S. 3.

67 Ein Zugang kann auch erforderlich sein für Familienangehörige schwer erkrankter Mitarbeiter; wird ein solcher Zugang für die Wahrung lebenswichtiger Interessen des betreffenden Mitarbeiters benötigt, kann er mit den entsprechenden Garantien gewährt werden.

## 2.6. Verwaltungsuntersuchungen und Disziplinarverfahren

### 2.6.1. Zugang zu E-Kommunikationsdaten

68 E-Kommunikationsdaten können wichtige Beweismittel in Verwaltungsuntersuchungen und Disziplinarverfahren sein, beispielsweise E-Mails, die zeigen, dass die Vertraulichkeit nicht gewahrt wurde, Internetzugangsprotokolle, die auf Pflichtversäumnis hindeuten, usw.

69 Dieser Abschnitt befasst sich mit internen Untersuchungen in den EU-Einrichtungen gemäß dem Statut; die Lage mag sich anders darstellen bei anderen Untersuchungstätigkeiten, die auf anderen Teilen des EU-Rechts fußen, wie Untersuchungen durch die GD WETTBEWERB der Europäischen Kommission.

70 Die weiterreichenden Datenschutzimplikationen von Verwaltungsuntersuchungen und Disziplinarverfahren werden in den Leitlinien des EDSB vom 23. April 2010 zur Verarbeitung personenbezogener Daten bei Verwaltungsuntersuchungen und Disziplinarverfahren untersucht.

71 In diesem Abschnitt ist der für die Verarbeitung Verantwortliche die für die Untersuchung zuständige Stelle (das IDOC für die Europäische Kommission) und

nicht der für die Verarbeitung Verantwortliche des E-Kommunikationssystems, aus dem die Daten gewonnen werden (wie die GD DIGIT).

72 Eine individuelle Auswertung der E-Kommunikation sollte nur vorgenommen werden, wenn *begründeter Verdacht* auf Missbrauch besteht. Der Verdacht erregende Sachverhalt muss nicht so konkret sein wie ein Sachverhalt, der eine Verurteilung oder Anklageerhebung rechtfertigen würde. Ein begründeter Verdacht müsste jedoch auf Tatsachen oder Informationen beruhen, die einen objektiven Beobachter vermuten lassen, dass die betreffende Person möglicherweise eine Straftat begangen hat (siehe EGMR, Murray ./. Vereinigtes Königreich (14310/88) Urteil vom 28. Oktober 1994, Randnrn. 55-63).

R11: **Sorgen Sie dafür, dass der Zugriff auf E-Kommunikationsdaten durch die Vorschriften für Verwaltungsuntersuchungen und Disziplinarverfahren abgedeckt ist**

73 Wie und wann Untersuchungsbeauftragte Zugriff auf E-Kommunikationsdaten erhalten können, muss in den internen Vorschriften Ihrer Einrichtung für Verwaltungsuntersuchungen und Disziplinarverfahren festgelegt werden.

74 Der Zugriff auf E-Kommunikationsdaten muss erforderlich sein und zum Zweck der Untersuchung in einem angemessenen Verhältnis stehen. Die mit der Untersuchung beauftragte Stelle (wie das IDOC) sollte Erforderlichkeit und Verhältnismäßigkeit konkret bewerten und dabei genau die mutmaßliche Straftat bestimmen und festlegen, mit welchem Aufwand an Personal, Material und Zeit die Durchsuchung durchzuführen ist. Diese Bewertung sollte vor der Untersuchung ordnungsgemäß dokumentiert werden, damit im Fall einer Anfechtung eine Überprüfung durch Gerichte oder die Verwaltung möglich ist.

### 2.6.2. Verdeckte Überwachung

75 Unter bestimmten Umständen möchte Ihre Einrichtung vielleicht verdeckte Überwachung anwenden, also die Speicherung detaillierter Protokolle aller Aktivitäten eines bestimmten Beschäftigten ohne dessen Wissen, um Beweise für kriminelles Verhalten zu sammeln.

76 Vorgeschlagene Verfahren für verdeckte Überwachung müssen mit einer stichhaltigen Begründung und einer Folgenabschätzung versehen werden und sind einer Vorabkontrolle zu unterziehen. Der Grund hierfür ist, dass solche Verfahren die Verarbeitung personenbezogener Daten über mutmaßliche Straftaten und eine Beurteilung der verdächtigten Person(en) beinhalten, womit sowohl Artikel 27 Absatz 2 Buchstabe a als auch Buchstabe b der Verordnung zum Tragen kommen. In seiner Vorabkontrollstellungnahme kann der EDSB bei Bedarf spezifische Datenschutzgarantien anordnen.

R12: **Sehen Sie bei der Planung verdeckter Überwachung angemessene Garantien vor**

77 Grundsätzlich fällt die Vorabkontrollstellungnahme des EDSB positiv aus; allerdings müssen alle folgenden Bedingungen erfüllt sein:

- Die verdeckte Überwachung ist erforderlich für die Untersuchung einer schweren Straftat in einer rechtlichen Untersuchung oder einer von der Polizei eines EU-Mitgliedstaats, anderen zuständigen Strafverfolgungsbehörden oder von einschlägigen Untersuchungsstellen der EU autorisierten Untersuchung;
- der Einsatz der verdeckten Überwachung steht im Einklang mit dem Gesetz und wurde offiziell genehmigt i) durch einen Richter oder einen anderen Beamten, der kraft Gesetzes des Mitgliedstaats, der den Einsatz der verdeckten Überwachung in Ihrer Einrichtung beantragt hat, entsprechend befugt ist, oder ii) durch das zuständige oberste Entscheidungsgremium (wie Exekutivausschuss oder Vorstand) Ihrer Einrichtung nach Maßgabe der schriftlichen und öffentlich zugänglichen Strategie Ihrer Einrichtung in Bezug auf den Einsatz der verdeckten Überwachung;
- es wird ein Register aller solcher Genehmigungen und Fälle verdeckter Überwachung geführt. Dieses Register muss auf Verlangen Ihres Datenschutzbeauftragten und des EDSB zur Überprüfung vorgelegt werden;
- die Überwachung erfolgt im Hinblick auf ihren Aufwand an Material, Personal und Zeit gezielt und unter der Voraussetzung, dass
    a. es für eine erfolgreiche Untersuchung des Falls keine Alternative zur verdeckten Überwachung gibt, und
    b. die daraus resultierenden Vorteile größer sind als die Verletzung der Privatsphäre der beobachteten Personen.

### 2.6.3. Forensische Sicherung des Inhalts des Computers oder anderer Geräte

78 Computer-Forensik lässt sich definieren als das technologische Verfahren für die Überprüfung von Computersystemen und ihrer Inhalte im Hinblick auf die Erfassung, Analyse und Vorlage elektronischer Beweismittel vor Gericht, die rechtlich fundiert sind und auf deren Stichhaltigkeit und Integrität vertraut werden kann. Mit den Techniken der Computer-Forensik ist es auch möglich, verborgene, verloren gegangene, beschädigte oder (aus Versehen oder absichtlich) gelöschte Daten wieder zu finden, die für Untersuchungen von Belang sein können.

79 Am häufigsten kommt die Computer-Forensik während einer Untersuchung durch Stellen wie das Europäische Amt für Betrugsbekämpfung (OLAF) oder durch einzelstaatliche Behörden in strafrechtlichen Ermittlungen zum Einsatz. Daher ist für die meisten Einrichtungen die Frage, ob und wie Computer-Forensik eingesetzt werden soll, weitgehend hypothetischer Natur. Der Vollständigkeit halber und weil einige Aspekte der Computer-Forensik in Verbindung zu diesen Leitlinien für E-Kommunikation stehen, wird an dieser Stelle auf sie eingegangen.

80 Da die Computer-Forensik in die Privatsphäre eindringt, sollte sie nur als letztes und notwendiges Mittel angesehen werden. Aus dem gleichen Grund bedarf es für ihren

Einsatz einer soliden Rechtsgrundlage (EU-Verträge oder ein auf ihrer Grundlage angenommener Rechtsakt).

81 In manchen Fällen benötigen die Ermittler möglicherweise eine forensische Gesamtabbildung des Zielgeräts (wie Telefone, PC, Laptops und andere mobile Geräte usw.) und weniger bestimmte E-Mails oder Dokumente. Eine forensische Abbildung kann erforderlich sein, um die Integrität der erhobenen Beweismittel zu erhalten. Darüber hinaus müssen die Ermittler je nach den Gegebenheiten vielleicht komplexe Durchsuchungen und Überprüfungen des beschlagnahmten Materials durchführen, die nicht vor Ort erledigt werden können. Ob ein solcher Bedarf besteht, hängt letztendlich von den konkreten Fakten des Einzelfalls ab.

82 Die Aneignung des gesamten Inhalts eines Zielgeräts ist *per definitionem* ein Eingriff in die Privatsphäre. Als Untersuchungsinstrument darf sie daher nur in Ausnahmefällen und dort erfolgen, wo es unbedingt notwendig ist. Ermittler sollten forensische Abbildungen nicht systematisch nutzen. Es sollten spezifische Garantien zum Schutz der Personen vor drohendem Missbrauch formuliert werden. Es sollten neben den allgemeinen, in vorstehendem Abschnitt 2.6.2 oben untersuchten Bedingungen insbesondere folgende Bedingungen erfüllt sein:

- Die untersuchende Stelle (z. B.OLAF) sollte vor Einleitung einer Untersuchung Notwendigkeit und Verhältnismäßigkeit bewerten und diese Bewertung angemessen dokumentieren (ähnlich wie Abschnitt 74). Sie sollte insbesondere nachweisen können, dass die Abbildung erforderlich ist, dass also mit einer anderen Methode der Sachverhalt nicht erfolgreich festgestellt werden könnte oder diese Feststellung deutlich schwieriger wäre;
- Abbildungen oder Kopien von Computern sollten nur hergestellt werden, wenn ein konkreter Verdacht auf einen hinreichend schweren Verstoß besteht, der durch konkrete erste Beweismittel gestützt wird;
- forensische Abbildungen sollten nicht bei geringfügigen Straftaten angefertigt werden, bei denen nur wenige Informationen erhoben werden müssen; ferner nicht bei geringfügigen Forderungen oder in anderen Fällen, in denen der potenzielle Nutzen der Untersuchung in keinem Verhältnis zum potenziellen Eingriff in das Privatleben stünde;
- der Inhalt des kopierten Geräts sollte gezielt ausgewertet werden. Es sollten automatisierte Prozesse und Suchverfahren genutzt werden, beispielsweise nach Schlüsselwörtern, um für den Fall relevante Daten zu identifizieren, die dann extrahiert werden und in die Untersuchungsakte eingehen. Jede Maßnahme muss zu einem nachvollziehbaren Prüfpfad führen;
- die betreffenden Personen sollten die Möglichkeit erhalten, auf Antrag beim Kopieren des Inhalts anwesend zu sein (in manchen Fällen können möglicherweise zum Schutz der Untersuchung Einschränkungen gemäß Artikel 20 zum Tragen kommen - siehe weiter unten die Punkte 113 und 114 unten), oder die Protokolldateien der an den Daten vorgenommenen Handlungen zu prüfen. Des Weiteren sind sie über ihr Recht auf Widerspruch zu informieren.

## 3. ALLGEMEINE EMPFEHLUNGEN FÜR PERSONENBEZOGENE INFORMATIONEN UND E-KOMMUNIKATION

### 3.1. Legen Sie Rechenschaft ab!

83 Rechenschaftspflicht bedeutet, dass Organisationen ihren Datenschutzverpflichtungen nachzukommen haben und auch in der Lage sein müssen, dies nachzuweisen.

84 Die Rechenschaftspflicht ist nicht auf E-Kommunikationsdaten beschränkt, sondern gilt für alle Vorgänge, bei denen personenbezogene Informationen verarbeitet werden.

85 Jede Organisation, die personenbezogene Daten erhebt, verwendet und speichert (gemeinhin bezeichnet als Verarbeitung), ist dafür verantwortlich, dass die Datenschutzvorschriften eingehalten werden und muss über diese Einhaltung Rechenschaft ablegen.

86 EU-Einrichtungen verarbeiten personenbezogene Daten aus zahlreichen Gründen; die Einstellung von Bediensteten und die Vergabe von Aufträgen, die Beurteilung von Bediensteten, die Erhebung von Gesundheitsdaten in Patientenakten, die Einrichtung von Zeitmanagementsystemen, CCTV und der Zugang für Besucher zu EU-Gebäuden sind nur einige Beispiele hierfür. Daher sind EU-Einrichtungen für die Einhaltung der in der Verordnung. niedergelegten Datenschutzvorschriften verantwortlich und müssen entsprechend Rechenschaft ablegen.

87 Generell gilt, dass Einrichtungen auf transparente Weise und klar darlegen, wie sie die personenbezogenen Daten im Zusammenhang mit E-Kommunikation und Überwachung von E-Kommunikation verarbeiten. Sie müssen ihre entsprechenden Strategien dokumentieren und dafür sorgen, dass die Nutzer von diesen Kenntnis haben. Das Recht auf Schutz der Privatsphäre besteht auch am Arbeitsplatz, und Menschen müssen darauf hingewiesen werden, wenn sie überwacht werden. Einrichtungen können nicht einfach davon ausgehen, dass die Mitarbeiter Bescheid wissen.

88 Am einfachsten kann eine Einrichtung ihrer Rechenschaftspflicht nachkommen, wenn sie die Datenschutzimplikationen neuer Prozesse schon bei deren Entwurf berücksichtigt (**eingebauter Datenschutz**). Unterschiedliche Verarbeitungsvorgänge und unterschiedliche Technologien erfordern unterschiedliche Garantien. Durch eine Einbeziehung ihres behördlichen Datenschutzbeauftragten schon in die frühen Phasen des Prozesses kann wertvoller Rat und wertvolle Orientierung eingeholt werden.

89 Nachstehend eine Liste der wichtigsten zu bedenkenden Aspekte:

a. **Festlegung des Zwecks:** Was wollen Sie erreichen und warum?

b. **Rechtmäßigkeit:** Dürfen Sie das tun?

c. **Zweckbindung und Sicherheit:** Wie gewährleisten Sie, dass die personenbezogenen Daten nur für den eigentlichen Zweck verwendet werden?

d. **Rechte der betroffenen Person:** Wie informieren Sie die betreffenden Personen und wie stellen Sie sicher, dass sie ihre Rechte ausüben können

(beispielsweise Datenschutzerklärungen, Ad-Hoc-Information, Auskunft und Berichtigung, mögliche Einschränkungen)?

e. **Dokumentation und Meldungen:** Wie dokumentieren Sie ihre Vorgehensweise und wie halten Sie die Dokumentation auf dem neuesten Stand?

90 In den folgenden Unterabschnitten wird näher auf die einzelnen Fragen eingegangen.

### 3.2. Warum müssen Sie E-Kommunikationsdaten verarbeiten und wie gehen Sie dabei vor?

R13: **Sorgen Sie bei jedem Vorgang, bei dem personenbezogene Daten verarbeitet werden sollen, dafür, dass die Zwecke festgelegt, eindeutig und rechtmäßig sind**

91 Bevor Sie personenbezogene Daten verarbeiten, müssen Sie den **Zweck festlegen**, für den Sie sie verarbeiten müssen. Dieser Zweck muss **festgelegt, eindeutig und rechtmäßig** sein. Diese Analyse fußt auf dem operativen Bedarf Ihrer Einrichtung und muss in den entsprechenden Strategien dokumentiert sein (siehe weiter unten Abschnitt 3.7).

92 Der/die Zweck(e) muss/müssen genau festgelegt sein, damit die betroffenen Personen verstehen, weshalb ihre Daten verarbeitet werden. Die Erläuterungen müssen klar und knapp sein. Allzu ausführliche Beschreibungen (wie zur Verbesserung der Nutzererfahrung) reichen ohne nähere Erläuterung nicht aus. Näheres hierzu in der Stellungnahme 03/2013 der Artikel 29-Datenschutzgruppe zur Zweckbindung, S. 15-16.

93 Eine **eindeutige** Erläuterung des Zwecks/der Zwecke gewährleistet, dass alle an der Verarbeitung Beteiligten wissen, was mit ihren Daten geschieht (und was nicht).

94 **Rechtmäßige** Zwecke sind solche, die „mit dem Gesetz in Einklang“ stehen. In der Praxis bedeutet dies, dass eine geeignete Rechtsgrundlage (siehe nachstehenden Abschnitt 3.3 unten) vorhanden sein muss und die anderen datenschutzrechtlichen Vorschriften eingehalten werden müssen (wie spezifische Vorschriften für spezifische Datenkategorien). Näheres hierzu in der Stellungnahme 03/2013 der Artikel 29-Datenschutzgruppe zur Zweckbindung, S. 19-20.

R14: **Erheben und verarbeiten Sie nur die Daten, die Sie wirklich benötigen, um Ihren/Ihre festgelegten Zweck(e) zu erreichen**

95 Nachdem Sie den Zweck der Verarbeitung festgelegt und die Rechtmäßigkeit nachgewiesen haben, müssen Sie sich mit der **Qualität der Daten** beschäftigen. Der Grundsatz der **Datenminimierung** besagt, dass Sie nur die Daten verarbeiten dürfen, die Sie für das Erreichen des festgelegten Zwecks benötigen. Artikel 4 Absatz 1 Buchstabe c der Verordnung: verarbeitete personenbezogene Daten „müssen den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und dürfen nicht darüber hinausgehen“.

96 Das heißt, dass Sie festlegen müssen, welche Informationen Sie für das Erreichen des angestrebten Zwecks benötigen. Sind Daten hierfür nicht erforderlich, dürfen Sie sie nicht verarbeiten. Sie dürfen personenbezogene Daten nicht einfach erheben oder speichern, weil sie irgendwann später nützlich sein *könnten*. Werden solche Daten für mehrere Zwecke gespeichert, stellen Sie sicher, dass die Beteiligten nur Zugriff auf die Daten haben, die sie für ihre Aufgabe im Verarbeitungsprozess benötigen. So benötigt beispielsweise ein Mitarbeiter eines IT-Helpdesks für die Beantwortung von Nutzeranfragen Zugang zu bestimmten Nutzerprotokollen; ein Prüfer oder Sicherheitsbeauftragter benötigt diesen Zugang nicht.

R15: **Legen Sie bei jeder Verarbeitung fest, wie lange die personenbezogenen Daten gespeichert werden**

97 **Aufbewahrungsfristen:** Häufig müssen Organisationen personenbezogene Informationen für bestimmte Zwecke (HR, rechtliche Angelegenheiten usw.) aufbewahren. Wenn Sie den Zweck und die Qualität der Daten festgelegt haben, die Sie benötigen, müssen sie bestimmen, wie lange sie gespeichert werden sollen. **Aufbewahrungsfristen** müssen nach der Devise **„so lang wie nötig, so kurz wie möglich“** und unter Berücksichtigung des Zwecks/der Zwecke der Verarbeitung festgelegt werden. (Artikel 4 Absatz 1 Buchstabe d der Verordnung: Personenbezogene Daten „dürfen nur so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, gespeichert werden“).

98 Werden die gleichen Daten für verschiedene Zwecke gespeichert, sollten entsprechende Einschränkungen beim Zugriff gelten. So benötigen Mitarbeiter des IT-Helpdesks beispielsweise Zugriff auf neuere Protokolldateien für die Fehlerbeseitigung, während Prüfer eher ältere Protokolldateien brauchen; der Zugriff auf Dateien für die Verwaltung oder die Prüfung eines Dienstes muss auf die Bedürfnisse des jeweiligen Dienstes zugeschnitten sein.

99 Müssen nur einige der personenbezogenen Daten für einen längeren Zeitraum gespeichert werden, müssen Sie die nicht mehr benötigten Daten löschen (z. B. Aufbewahrung bestimmter Protokolle für einen festgelegten Zeitraum, hingegen Aufbewahrung von Daten zum Nutzer-Account so lange, wie der Account aktiv ist).

### 3.3. Ist das legal?

100 Die Verarbeitung personenbezogener Daten muss sich auf einen der in Artikel 5 der Verordnung genannten rechtlichen Gründe stützen.

101 Die Grundlage für den Großteil der Verarbeitungen von E-Kommunikationsdaten dürfte das **öffentliche Interesse** (Artikel 5 Buchstabe a) sein, das auch „die Verarbeitung personenbezogener Daten einschließt, die für die Verwaltung und das Funktionieren dieser Organe und Einrichtungen erforderlich ist“ (Erwägungsgrund 27). Die meisten spezifischen Rechtsgrundlagen sollten in den internen Vorschriften Ihrer Einrichtung zur Definition von „Verwaltung und

Funktionieren“ zu finden sein, während Artikel 37 der Verordnung spezifische Vorschriften für Verkehrs- und Gebührenabrechnungsdaten enthält.

102 Ein weiteres Kriterium, das über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten entscheidet, ist die **Einwilligung** der betroffenen Personen (Artikel 5 Buchstabe d). Die Einwilligung muss jedoch ohne Zwang gegeben worden sein, und es dürfen bei Verweigerung der Einwilligung keine tatsächlichen oder potenziellen Nachteile entstehen. Näheres hierzu in der Stellungnahme 15/2011 der Artikel 29-Datenschutzgruppe zur Definition von Einwilligung.

103 Im Beschäftigungskontext dürfte es aufgrund des Machtungleichgewichts zwischen Arbeitgeber und Beschäftigtem unwahrscheinlich sein, dass die Einwilligung als Rechtsgrundlage gilt. Müsste beispielsweise Ihre Einrichtung in Abwesenheit eines Beschäftigten auf dessen Mailbox zugreifen, wäre die Einwilligung des Beschäftigten keine geeignete Rechtsgrundlage. Dieser Zugriff erfolgte stattdessen aus Gründen der Geschäftskontinuität im öffentlichen Interesse. Auch Anrufe bei Notrufnummern können aufgezeichnet werden, damit die Mitarbeiter den Anruf erneut abhören können, falls er beim ersten Mal nur schwer verständlich war, und dann die erforderliche Hilfe auf den Weg bringen können; Anrufer und Angerufener können der Aufzeichnung zugestimmt haben oder auch nicht.

> ***Example 6:*** *Internes Telefonverzeichnis der Mitarbeiter: Notwendigkeit gegen Einwilligung*
>
> *Ein internes Telefonverzeichnis mit Namen, Stellenbezeichnung, E-Mail-Adresse, Telefon- und Büronummer usw. kann „für das Funktionieren“ einer Einrichtung erforderlich sein (Artikel 5 Buchstabe a und Erwägungsgrund 27 der Verordnung). Ohne ein solches Telefonverzeichnis könnte eine Organisation kaum reibungslos funktionieren. Diese Notwendigkeit genügt als Grund für die Anlage eines Verzeichnisses. Die Einwilligung der Mitarbeiter ist zwar nicht erforderlich, doch müssen sie informiert werden siehe weiter unten Abschnitt 3.5**Error! Reference source not found.**.*
> *Das Telefonverzeichnis muss nicht unbedingt Fotos der Mitarbeiter enthalten; Fotos spielen keine wesentliche Rolle für das reibungslose Funktionieren der Organisation. Im vorliegenden Fall ist die Einwilligung die geeignete Rechtsgrundlage; Sie können nicht alle Mitarbeiter zwingen, ein Foto von sich einzustellen.*

### 3.4. Personenbezogene Daten dürfen nur für den festgelegten Zweck verwendet werden

R16: **Sorgen Sie bei jeder Verarbeitung dafür, dass die Daten für den festgelegten Zweck verarbeitet und nicht für Zwecke weiterverarbeitet werden, die mit dem ursprünglichen Zweck unvereinbar sind**

104 Die **Zweckbindung** gehört zu den zentralen Grundsätzen des Datenschutzes. Dieser Grundsatz dient dem Schutz von Personen, indem die Verwendung ihrer personenbezogenen Daten auf vorab festgelegte Zwecke beschränkt wird, mit

Ausnahme der Verwendung unter strengen Voraussetzungen und mit geeigneten Garantien. Näheres hierzu in der Stellungnahme 03/2013 der Artikel 29-Datenschutzgruppe zur Zweckbindung.

105 Mitunter mag eine Änderung des Zwecks zulässig sein, wenn es in Ihren internen Vorschriften so vorgesehen ist und der neue mit dem ursprünglichen Zweck vereinbar ist. Eine mit diesem Zweck nicht kompatible Verwendung ist nur zu den Bedingungen von Artikel 20 der Verordnung möglich.

> ***Example 7:*** *Zweckbindung und IT-Protokolle*
>
> *Eine EU-Einrichtung speichert zur Gewährleistung der Funktionsfähigkeit und Sicherheit ihrer Systeme Protokolle von Internetverbindungen. Eine der Aufgaben des IT-Systemadministrators besteht darin, zu überwachen, dass das System funktioniert. Zu diesem Zweck benötigt er Zugriff auf diese Protokolldateien, darunter die Websites, die von Mitarbeitern jeden Tag aufgerufen werden.*
> *Der Leiter eines anderen Referats verlangt nun vom Systemadministrator, die Protokolldateien eines bestimmten, seiner Aufsicht unterstellten Mitarbeiters an ihn weiterzuleiten, da er vermutet, dass der Betreffende viel Zeit auf Websites mit Freizeitangeboten und in sozialen Netzwerken verbringt und damit seine Arbeitspflichten vernachlässigt.*
> *Mit der Speicherung von Protokolldateien soll gewährleistet werden, dass die Systeme korrekt laufen, sollen Störfälle ermittelt werden und soll darauf reagiert werden. Sie sollen Vorgesetzten nicht bei der Kontrolle ihrer Mitarbeiter helfen. Der IT-Administrator hat dieses Ansinnen zurückzuweisen.*
> *Wenn hingegen eine Verwaltungsuntersuchung des Verhaltens des betreffenden Mitarbeiters im Einklang mit den geltenden internen Vorschriften eingeleitet worden ist und der Antrag vom Untersuchungsgremium kommt, kann eine Änderung des Zwecks erlaubt sein.*

106 Sie müssen besondere Sorgfalt darauf verwenden, die Sicherheit der erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten zu gewährleisten. Organisationen müssen angemessene technische und organisatorische Maßnahmen zur Sicherung der Daten ergreifen, um den Risiken für die betreffenden Personen Rechnung zu tragen. Das bedeutet unter anderem, dass ein Verfahren für das Management von Informationsrisiken bestehen muss. Weitere Informationen weiter unten im Abschnitt 3.8.1.

## 3.5. Das Recht auf Information

R17: **Informieren Sie die betreffenden Personen darüber, wie ihre Daten verarbeitet werden**

107 Generell gilt, dass Sie die betreffenden Personen darüber informieren müssen, wie ihre Daten verarbeitet werden, **bevor** die Verarbeitung anläuft.

108 Das Minimum der zu erteilenden Informationen ist in den Artikeln 11 und 12 der Verordnung festgelegt. Die betreffenden Personen müssen Folgendes erfahren:

a. Wer ist für die Verarbeitung verantwortlich (Identität des für die Verarbeitung Verantwortlichen);

b. welchem Zweck dient die Erhebung, Speicherung und Verwendung der Daten;

c. an wen werden die Daten weitergegeben/wer kann auf die Daten zugreifen;

d. wenn die Daten bei der betroffenen Person erhoben werden: ist die Bereitstellung von Daten vorgeschrieben oder fakultativ? Wenn sie vorgeschrieben ist: Welche Folgen hat es, wenn sie nicht bereitgestellt werden?

e. Wenn die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben werden: Woher stammen sie dann? Welche Art von Daten soll verarbeitet werden? Dies gilt beispielsweise für die Protokollierung von Aktivitäten auf IT-Systemen: Da die Nutzer nicht wissen, was protokolliert wird, müssen sie darüber informiert werden. Andererseits ist es in einem Auswahlverfahren nicht erforderlich, alle im Bewerbungsformular abgefragten Datenkategorien in der Datenschutzerklärung zu wiederholen, da die Person ja weiß, welche Angaben sie gemacht hat; hier reicht ein einfacher Hinweis auf den „Inhalt des Bewerbungsformulars“.

f. Aufklärung der betroffenen Person(en) über ihr Recht auf Auskunft über ihre Daten und deren Berichtigung; hier sollte darüber informiert werden, wie Auskunft zu erlangen ist, und sollten die Kontaktdaten der Person angegeben werden, an die man sich zu wenden hat.

g. alle anderen Informationen, mit denen eine Verarbeitung in Treu und Glauben gewährleistet wird, wie

   i. die Rechtsgrundlage der Verarbeitung;

   ii. die Speicherfrist für die Daten;

   iii. das Recht, sich an den EDSB zu wenden.

109 Diese Informationen sollten den betreffenden Personen in einer **klaren und leicht verständlichen Sprache** gegeben werden.

110 Sie sollten dies im Wege **einer oder mehrerer Datenschutzerklärung(en)** tun, da die Informationen in Strategiedokumenten zum Konzept Ihrer Einrichtung bei der Verarbeitung von E-Kommunikationsdaten nicht ausdrücklich für die Personen verfasst wurden, deren Daten verarbeitet werden sollen. Ein einfacher Hinweis auf diese Strategiedokumente ist zur Information dieser betroffenen Personen nicht besonders geeignet.

111 Je kürzer die Datenschutzerklärung ist, desto eher wird sie gelesen. In den meisten Fällen dürfte eine Seite genügen, um die erforderlichen Informationen zu vermitteln. Eine weitere Möglichkeit sind **Hinweise „in Schichten“** mit einer kurzen Zusammenfassung, die auf die Vollfassung verweist.

112 **Nicht ausreichend ist die Einstellung von Datenschutzerklärungen in das Intranet der Einrichtung.** Sie müssen die betreffenden Personen aktiv informieren. Bei neuen Mitarbeitern hat es sich bewährt, diese Informationen in ihrem Begrüßungspaket unterzubringen; eine weitere Möglichkeit sind Pop-up-Bildschirme bei ihrer ersten Anmeldung auf ihren Computern.

> ***Example 8:*** *Informationen über die Regeln für die Nutzung von IT-Ressourcen*
>
> *Eine Einrichtung bietet ihren Mitarbeitern die üblichen IKT-Dienste an (Telefone, Mailboxen, Internetzugang auf Desktop-Computern, WiFi usw.), Besucher können sich über den Gastzugang in das WiFi einloggen.*
> *Die Mitarbeiter werden über die geltenden Regeln in ihren Begrüßungspaket beim Eintritt in die Einrichtung unterrichtet, das ein Exemplar des Strategiedokuments und eine kurze, einseitige Datenschutzerklärung enthält (alle diese Dokumente können natürlich auch im Intranet der Einrichtung eingesehen werden). Bei einer Änderung an der Strategie werden die Mitarbeiter mit einer per E-Mail verbreiteten Zusammenfassung der Änderungen informiert. Die Strategie enthält Regeln dafür, wie und wann die Einrichtung auf die Mailboxen ihrer Beschäftigten in deren Abwesenheit zugreifen darf. Kommen diese gezielten Verfahren zum Einsatz, werden die betroffenen Mitarbeiter außerdem einzeln unterrichtet.*
> *Da nur wenige dieser Verarbeitungen für Besucher von Belang sind, kann hier die Unterrichtung anders erfolgen, beispielsweise durch eine Datenschutzerklärung in dem Informationsblatt mit den WiFi-Zugangscodes für Gäste und/oder über eine Weiterleitung zur Datenschutzerklärung bei der ersten Verbindung mit dem Netzwerk.*

113 Mitunter gibt es gute Gründe dafür, jemanden nicht unverzüglich über die Verwendung seiner Daten zu informieren, beispielsweise in der Anfangsphase einer Verwaltungsuntersuchung. Die Datenschutzverordnung lässt dies unter bestimmten, in Artikel 20 aufgelisteten Bedingungen zu. Für nähere Informationen siehe die Leitlinien des EDSB zu den Rechten natürlicher Personen, S. 26ff.

114 Als Beispiele wären die Verhinderung und Untersuchung von Straftaten zu nennen. Möchte eine Einrichtung eine solche Einschränkung anwenden, ist genau zu dokumentieren, warum dies erforderlich ist. In Fällen, in denen derartige Einschränkungen erforderlich sind, kann in den Durchführungsbestimmungen zum Datenschutz in der Einrichtung die Anhörung des Datenschutzbeauftragten verlangt werden.

***Example 9:*** *Einschränkung des Rechts auf Information*

*Ein Mitarbeiter steht in dem Verdacht, mehrere Stunden des Arbeitstags mit dem Besuch von Glücksspiel-Websites zu verbringen.*
*Die Strategie für den Zugang zu IT-Ressourcen besagt, dass Protokolldateien für den Internetzugang für Verwaltungsuntersuchungen und Disziplinarverfahren verwendet werden dürfen.*
*Im Einklang mit den geltenden Vorschriften wird eine Verwaltungsuntersuchung des Verhaltens des Mitarbeiters eingeleitet. Eine sofortige Unterrichtung des Mitarbeiters würde die Untersuchung ernsthaft behindern, da er vermutlich sein Verhalten für die Dauer der Untersuchung ändern und damit alle Bemühungen zunichte machen würde, Beweise für sein Pflichtversäumnis zu sammeln.*
*Unter diesen Umständen mag ein Aufschub der Unterrichtung gerechtfertigt sein. Der Leiter der Untersuchung hat zu dokumentieren, welche der Ausnahmen gemäß Artikel 20 der Verordnung zur Anwendung kommt und warum ihre Anwendung erforderlich ist. Ist die Einschränkung irgendwann nicht mehr erforderlich, ist der Mitarbeiter darüber zu unterrichten.*

### 3.6. Recht auf Auskunft und Berichtigung

R18: **Erleichtern Sie den betroffenen Personen die Ausübung ihres Rechts auf Auskunft und Berichtigung**

115 Natürliche Personen (auch als betroffene Personen bezeichnet) haben gemäß Artikel 13 und 14 der Verordnung das **Recht auf Auskunft über sie betreffende personenbezogene Daten und auf deren Berichtigung**. Ihre Einrichtung muss lediglich über die diese Person betreffenden Informationen Auskunft geben; aufgrund dieser Rechte ist Ihre Einrichtung **nicht verpflichtet, Daten zu speichern, die sie andernfalls nicht gespeichert hätte.**

116 Die Angaben, die Sie bereitstellen müssen, sind im Einzelnen in den Leitlinien des EDSB zu den Rechten natürlicher Personen ab S. 9 aufgeführt. Zusammengefasst müssen Sie angeben,

a. ob die personenbezogenen Daten des Antragstellers verarbeitet werden;

b. Einzelheiten zur Verarbeitung, beispielsweise in einer Datenschutzerklärung sowie gegebenenfalls weiteren Informationen;

c. welche Daten verarbeitet werden und von wem sie stammen;

d. die Logik aller automatisierten Entscheidungsprozesse. z. B.: Übersteigt die Rechnung für Ihr dienstliches Mobiltelefon 200 EUR, werden Sie verwarnt. Übersteigt die Rechnung zwei Monate in Folge 200 EUR, wird Ihr Dienstvorgesetzter informiert.

117 Die **im Gesetz festgelegte Frist für die Beantwortung** eines Antrags auf **Auskunft oder Berichtigung** nach der Datenschutzverordnung beträgt drei Monate; in den Durchführungsbestimmungen für den Datenschutz in Ihrer Einrichtung können

allerdings kürzere Fristen festgelegt sein. Wenn Sie sich nicht sicher sind, besprechen Sie sich mit dem Datenschutzbeauftragten.

118 Ist eine Berichtigung durch die Änderung von Daten nicht möglich (weil z. B. die Integrität von Protokolldateien gewahrt werden muss), sollte(n) die Person(en) dokumentieren können, dass sie damit nicht einverstanden ist/sind.

119 Ausnahmen von diesen Rechten sind in Artikel 20 der Datenschutzverordnung geregelt. Für nähere Informationen siehe die Leitlinien des EDSB zu den Rechten natürlicher Personen, S. 26ff.

***Example 10:*** *Zugang zu Informationen*

*Eine Einrichtung erlaubt ihren Mitarbeitern die Nutzung von Diensttelefonen für private Anrufe unter der Bedingung, dass diese Anrufe durch Verwendung eines bestimmten Codes gekennzeichnet werden. Die Gebühren für diese Anrufe werden von dem betreffenden Mitarbeiter entrichtet.*
*Die für die Erhebung dieser Daten verwendete Anwendung ermöglicht den Mitarbeitern, über einen Link in das Intranet der Einrichtung ihre eigene Liste angemeldeter Anrufe zu überprüfen. Stellt der Mitarbeiter einen Fehler fest, kann er mit Hilfe eines Kontaktformulars die zuständige Stelle auffordern, die erforderlichen Berichtigungen vorzunehmen.*

### 3.7. Dokumentieren Sie, was Sie tun

R19: **Steuern Sie die Strategien Ihrer Einrichtung für die Verarbeitung von E-Kommunikationsdaten**

120 Bei der Rechenschaftspflicht geht es darum, verantwortungsvoll das Richtige auf reproduzierbare Weise zu tun. Ein zentrales Element der Rechenschaftspflicht sind sorgfältig ausgearbeitete und klug gesteuerte Strategien.

121 Mit Hilfe solcher Strategien erkennen Einrichtungen, wie die in diesen Leitlinien formulierten Empfehlungen umzusetzen sind, beispielsweise die Empfehlungen betreffend den Grundsatz der Zweckbindung, die Grundsätze der Datenqualität und die Unterrichtung aller Personen, deren personenbezogene Daten verarbeitet werden.

122 Diese Strategien sind regelmäßig zu überprüfen und bei Bedarf zu ändern.

R20: **Melden Sie Ihre Verarbeitungen dem behördlichen Datenschutzbeauftragten**

123 Die Verordnung enthält **spezifische Dokumentationspflichten**. Gemäß Artikel 25 haben Sie alle Verarbeitungen Ihrem Datenschutzbeauftragten zu melden, der Ihnen ein auszufüllendes Meldungsformular vorlegt. Sie müssen die Meldung bei ihm einreichen, *bevor* die Verarbeitung anläuft, so dass er Sie noch beraten, Verbesserungen anregen und bei Bedarf beim EDSB eine Meldung zur Vorabkontrolle einreichen kann.

124 Darüber hinaus **müssen bestimmte risikobehaftete Verarbeitungen dem EDSB** zur Vorabkontrolle **gemeldet** werden; im Bereich E-Kommunikation betrifft dies im Wesentlichen die Verarbeitung bestimmter besonderer Datenkategorien, die in

Artikel 27 Absatz 2 Buchstabe a der Verordnung aufgeführt sind, und Verarbeitungen, die dazu bestimmt sind, die Persönlichkeit der betroffenen Person zu bewerten (betroffene Person) (Artikel 27 Absatz 2 Buchstabe b). Am relevantesten im Zusammenhang mit E-Kommunikationsdaten ist die Verarbeitung von Daten, die Verdächtigungen, Straftaten oder Sicherungsmaßregeln betreffen. Der Begriff „Sicherungsmaßregeln“ (engl. security measures) hat hier nichts mit Informationssicherheit zu tun, sondern mit Maßnahmen wie der Einweisung in die Psychiatrie - Zwangsmaßnahmen, die gegen eine Person zu ihrer eigenen Sicherheit (oder der anderer Personen) verhängt werden. Weitere Beispiele wären die Auswertung von Verkehrsdaten, die dazu bestimmt ist, Mitarbeiter zu bewerten, oder die verdeckte Überwachung zur Verwendung in Verwaltungsuntersuchungen. Die Meldung beim EDSB reicht zwar der behördliche Datenschutzbeauftragte ein, doch muss er zum Ausfüllen des an den EDSB gehenden Meldungsformulars Kontakt mit der für die Verarbeitung verantwortlichen Person aufnehmen. Für Ihre eigenen Planungen sollten Sie bedenken, wie lange es dauert, bis die Stellungnahme des EDSB vorliegt (bis zu zwei Monate, die um zwei weitere Monate verlängert werden können, nicht mitgerechnet die Zeit, während der der Fall zur Einholung weiterer Informationen ausgesetzt wird).

***Example 11:*** *Die Verwendung von Protokolldateien in Verwaltungsuntersuchungen*

*Wenn Ihre Einrichtung in ihre internen Vorschriften für Verwaltungsuntersuchungen die Verwendung von Protokolldateien im Verfahren aufnimmt, muss auch die Originalmeldung, die Sie Ihrem Datenschutzbeauftragten zu Verwaltungsuntersuchungen übermittelt haben, entsprechend aktualisiert werden. Da die Verwendung von Protokolldateien kein Selbstzweck, sondern Bestandteil von Verwaltungsverfahren ist, ist eine neue eigenständige Meldung nicht erforderlich.*

125 Nachstehend einige Beispiele von Verarbeitungen, die dem EDSB nicht gemeldet werden müssen:

a. Verarbeitung von Telefondaten allein für Zwecke der Gebührenabrechnung und der Verwaltung des Haushalts, unter der Voraussetzung, dass nicht beabsichtigt ist, die rechtmäßige Nutzung zu überprüfen oder Mitarbeiter zu bewerten;

b. Verarbeitung von Verkehrsdaten (z. B. E-Mail und Internet) für Zwecke der Sicherheit und des Verkehrsmanagements, die automatisiert und nicht nach Namen aufgeschlüsselt verarbeitet werden, unter der Voraussetzung, dass nicht beabsichtigt ist, die rechtmäßige Nutzung zu überprüfen oder Mitarbeiter zu bewerten.

R21: **Seien Sie mit Ihrer Dokumentation und Ihren Meldungen immer auf dem neuesten Stand**

126 Es liegt in Ihrer Verantwortung, Ihre Dokumentation und Ihre Meldungen immer auf dem neuesten Stand zu halten. Sobald Änderungen an Ihren Verfahren vorgenommen

werden, die den Inhalt der Meldung oder der Datenschutzerklärung berühren oder aus einem anderen Blickwinkel des Datenschutzes von Belang sind, teilen Sie dies Ihrem Datenschutzbeauftragten mit. Dies ist ein wichtiger Schritt im Rechenschaftsprozess.

## 3.8. Technische und organisatorische Sicherheitsmaßnahmen

### 3.8.1. Managen Sie Ihre Informationsrisiken

R22: **Schaffen Sie ein gut dokumentiertes Verfahren für das Risikomanagement, um Informationen zu schützen**

127 Ihre Organisation muss die angemessenen technischen und organisatorischen Maßnahmen ergreifen, um die sichere Nutzung (Sicherheit sowohl des Systems als auch der personenbezogenen Daten) des E-Kommunikationsnetzwerks und der Endgeräte zu gewährleisten, gegebenenfalls zusammen mit Dienst- oder Netzwerkanbietern. Gemäß Artikel 22 der Verordnung sollten diese Maßnahmen geeignet sein, ein Schutzniveau zu gewährleisten, das den für alle Daten bestehenden Risiken angemessen ist, und dies unter Berücksichtigung des Standes der Technik und der bei der Durchführung entstehenden Kosten.

128 Das bedeutet, dass Sie im Einklang mit den feststehenden Grundsätzen der guten Praxis (z. B. ISO/IEC 27000-Reihe) ein Verfahren für das Management von Informationsrisiken einzurichten haben. Der erste Schritt ist eine Bewertung der Risiken, die auch eine Analyse der Nutzung von E-Kommunikationsressourcen umfassen sollte. Diese Bewertung hilft Ihnen bei der Ermittlung der größten Sicherheitsrisiken und bildet die Grundlage für die Auswahl der geeigneten Kontrollen, die eingeführt werden müssen, um die Risiken auf ein für das Management annehmbares Niveau zu senken. Zum Verfahren des Risikomanagements gehört auch eine regelmäßige Überprüfung der Risikobewertung sowie der Angemessenheit von Garantien und Kontrollen.

129 Sie müssen das Verfahren für das Management von Informationsrisiken nach festgelegten Standards für solche Verfahren ordnungsgemäß dokumentieren und es als eine Strategie der Einrichtung **kommunizieren**. Es muss **regelmäßig überarbeitet** werden, um sicherzustellen, dass es seine Wirksamkeit behält und sich an neue und sich wandelnde Ziele der Organisation anpasst.

130 In das Verfahren (vor allem in die Analyse von Sicherheitsrisiken) **sollten nicht nur die mit Sicherheit befassten Mitarbeiter** der EU-Einrichtung **eingebunden werden**. Zu **berücksichtigen sind bei der Analyse die Auswirkungen auf alle Bereiche der Organisation**, weshalb an den Diskussionen eine möglichst große Vielfalt von Vertretern (HR, Datenschutzbeauftragter, Datenschutzkoordinator, Kerngeschäftsbereiche) teilnehmen sollte.

131 Sie sollten das Ergebnis des Verfahrens für das Management von Informationsrisiken und der Prüfung bestehender Sicherheitsrisiken allen Betroffenen und potenziell

Betroffenen klar kommunizieren; für das Management und andere sind möglicherweise detailliertere Ausführungen angebracht.

### 3.8.2. Outsourcing von Dienstleistungen

**R23: Nehmen Sie in Verträge mit externen Dienstleistern Datenschutzklauseln auf**

132 Es kann vorkommen, dass EU-Einrichtungen Aufgaben im Bereich der Verarbeitung von E-Kommunikationsdaten an externe Dienstleister übertragen möchten. So greift vielleicht Ihre Organisation auf externe Unternehmen zurück, die die Sicherheit überwachen, die Virenbekämpfung durchführen, das E-Mail-Management übernehmen oder Statistiken erstellen. In diesen Fällen sind besondere Vorkehrungen zu treffen. Vor allem gilt:

a. Ihre Einrichtung sollte bei der Auswahl eines Anbieters große Sorgfalt walten lassen, damit er hinreichende Garantien für die gemäß der Verordnung erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen bietet: **Es ist Sache der Einrichtung, dafür zu sorgen, dass der Anbieter** diese Maßnahmen **einhält**;

b. die Beziehung zwischen der EU-Einrichtung und dem Anbieter ist in einem Vertrag oder einem Rechtsakt zu formalisieren, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist. In dem Dokument ist zu bestimmen,

   i. dass der Anbieter **nur auf Weisung** Ihrer Organisation handelt;

   ii. dass die in der Verordnung geregelten Verpflichtungen in den Bereichen **Vertraulichkeit und Sicherheit** auch für den Anbieter gelten (es sei denn, er unterliegt bereits ähnlichen Verpflichtungen nach einzelstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG). Bei Auftragnehmern außerhalb der EU müssen angemessene Garantien gewährt sein. Zur Frage von Datenübermittlungen siehe das Positionspapier des EDSB zur Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU, insbesondere S. 18-21.

**R24: Überwachen Sie Auftragnehmer daraufhin, ob sie die Datenschutzklauseln in ihren Verträgen korrekt anwenden**

133 Die Verordnung gilt auch für alle ausgelagerten Dienstleistungen, und es ist Sache der Einrichtung, dafür zu sorgen, dass sich externe Unternehmen an die Grundsätze halten und die entsprechenden Garantien anwenden. So können beispielsweise die Mitarbeiter des Auftragnehmers aufgefordert werden, Vertraulichkeitserklärungen ähnlich denen zu unterzeichnen, die auch die eigenen Mitarbeiter Ihrer Organisation unterzeichnen.

## ANHANG 1: ZUSAMMENFASSUNG DER DATENSCHUTZGRUNDSÄTZE

Die nachstehende Liste vermittelt einen raschen Überblick über allgemein anerkannte Datenschutzgrundsätze. Sie finden sie alle oder mehrheitlich in den Datenschutzvorschriften der EU. Es ist Ihre Aufgabe als für die Verarbeitung Verantwortlicher, sie einzuhalten, und Sie müssen in der Lage sein, die Einhaltung nachzuweisen. Sie ersetzen nicht die in diesen Leitlinien formulierten Ratschläge, beschreiben aber die dahinter stehende Gedankenwelt.

1. **Personenbezogene Daten müssen nach Treu und Glauben verarbeitet werden, und ihre Verarbeitung muss rechtmäßig sein.**
   Sie müssen für eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten sorgen. So könnte die Verarbeitung für die Wahrnehmung von Aufgaben erforderlich sein, die Ihrer Einrichtung vom Gesetz übertragen wurden (darunter notwendige interne Verwaltungsaktivitäten). Bei einer Verarbeitung nach Treu und Glauben geht es darum, dass den Menschen gesagt wird, was mit ihren Daten geschieht, und dass Sie sich daran halten.

2. **Personenbezogene Daten sind für festgelegte, eindeutige und rechtmäßige Zwecke zu verarbeiten und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.**
   Legen Sie ausdrücklich fest, warum und wie Sie personenbezogene Daten verarbeiten. Verwenden Sie sie nicht auf eine Weise, die mit diesem ursprünglichen Zweck nicht zu vereinbaren ist.

3. **Personenbezogene Daten müssen dem Zweck entsprechen, für den sie verarbeitet werden, dafür erheblich sein und dürfen nicht darüber hinausgehen.**
   Machen Sie sich Gedanken darüber, welche Daten Sie benötigen, um Ihre festgelegten Zwecke zu erreichen, und verarbeiten Sie dann nur diese Datenkategorien, nicht mehr.

4. **Personenbezogenen Daten müssen sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sein.**
   Tragen Sie Sorge dafür, dass die von Ihnen verarbeiteten Daten sachlich richtig sind; sachlich unrichtige Daten können die falschen Entscheidungen nach sich ziehen. Sorgen Sie gegebenenfalls dafür, dass die Daten auf dem neuesten Stand sind.

5. **Bestehen des Rechts auf Auskunft und Berichtigung**
   Personen haben das Recht auf Auskunft über ihre von Ihrer Einrichtung verarbeitete personenbezogene Daten und auf die Berichtigung unrichtiger Daten. Machen Sie ihnen die Ausübung dieser Rechte leicht. Das kann auch Ihnen dabei helfen, für sachlich richtige und auf dem neuesten Stand befindliche Daten zu sorgen.

6. **Verarbeitete personenbezogene Daten dürfen nicht länger als notwendig gespeichert werden.**
   Denken Sie darüber nach, wie lange Sie die Daten wirklich aufbewahren müssen, und bewahren Sie sie dann wirklich nur für diesen Zeitraum auf, nicht länger.

7. **Achten Sie auf die Sicherheit personenbezogener Daten**
   Führen Sie eine Risikobewertung durch und ergreifen Sie die angemessenen Sicherheitsvorkehrungen, berücksichtigen Sie dabei den Stand der Technik, die Risiken der Verarbeitung und die Kosten für die Umsetzung.

**8. Vorschriften für Übermittlungen**

Sorgen Sie dafür, dass Sie die spezifischen Vorschriften für Übermittlungen personenbezogener Daten an Dritte, insbesondere in Länder außerhalb der EU, einhalten.