



# Datenschutzaudit Fragenkatalog

## 1 Überblick und Grundlagen

Dieses Kapitel behandelt grundlegende Angelegenheiten. Die hier aufgeworfenen Fragen unterstützen die Sachverständigen, um einen Überblick über die datenschutzrelevanten Angelegenheiten des Untersuchungsobjekts zu bekommen.

### 1.1 Verfahren und Zweck

- 1.1.1 Welche Datenverarbeitungsvorgänge werden in der Organisation durchgeführt?
- 1.1.2 Was sind die wichtigsten Vorgänge?
- 1.1.3 Welche weiteren Verfahren werden durchgeführt?
- 1.1.4 Sind immer die Zweckbestimmungen ausreichend definiert?
- 1.1.5 Wer hat Einsicht in personenbezogene Daten innerhalb und außerhalb des Unternehmens ?

### 1.2 Verarbeitete personenbezogene Daten

- 1.2.1 Werden personenbezogene Daten verarbeitet?
- 1.2.2 Sind die Angaben über die Verfahren mit personenbezogenen Daten und die Zweckbestimmungen offengelegt?
- 1.2.3 Sind die Angaben über die Verfahren mit personenbezogenen Daten und die Zweckbestimmungen plausibel?

### 1.3 Verarbeitete besondere personenbezogene Daten

- 1.3.1 Werden besondere Kategorien von Daten verarbeitet?
- 1.3.2 Welche Schutzstufen sind dafür vorgesehen?

## 1.4 Verantwortliche Person

- 1.4.1 Wer ist der Administrator für die Datenverarbeitung?
- 1.4.2 Werden die Datenverarbeitungsprozesse ganz oder teilweise von den Herstellern der Datenverarbeitungsverfahren gesteuert?
- 1.4.3 Ist vorgesehen, dass die datenverarbeitende Stelle die Datenverarbeitung alleine steuert?
- 1.4.4 Ist dies in den Verträgen mit den Herstellern und den Dienstleistern der Datenverarbeitungsprogramme festgelegt?
- 1.4.5 Werden die Daten im Auftrag der datenverarbeitenden Stelle verarbeitet?

## 1.5 Weitergabe von Daten an ein Drittland

- 1.5.1 Werden Daten an Länder übermittelt, die weder Mitglieder der EU noch des Europäischen Wirtschaftsgebietes sind, wenn die Prozesse betrieben werden?
- 1.5.2 In welcher Periodik geschieht die Übermittlung?

## 1.6 Datenvermeidung und Datensparsamkeit

- 1.6.1 Ist es möglich, die Datenverarbeitung auszuführen, ohne dass alle Daten identifizierbar sind?
- 1.6.2 Werden Daten automatisch anonymisiert oder pseudonymisiert? Wie sonst?
- 1.6.3 Wie werden pseudonymisierte Daten gegen eine zu leichte Re-Identifikation geschützt?
- 1.6.4 Werden Daten in einer identifizierbaren Form nur soweit erhoben, wie es der Zweckbestimmung, zu der sie erhoben werden, entspricht?

- 1.6.5 Welche Kombination von personenbezogenen Daten ist wirklich erforderlich? Wie weit ist es wirklich notwendig, bestimmte Daten zu kombinieren?
- 1.6.6 Sind Maßnahmen getroffen worden, um die unnötige Bildung von temporären Schattendaten zu vermeiden? Wenn solche temporäre Schattendateien gebraucht werden, wie gut sind sie gegen unbefugten Zugang geschützt?  
z. B. durch unnötiges Logging
- 1.6.7 Wenn Daten an andere Verantwortliche weitergegeben werden, sind Maßnahmen getroffen worden, um Daten auszufiltern, die vom Empfänger nicht gebraucht werden?
- 1.6.8 Wie lange werden Daten aufbewahrt? Ist die Aufbewahrungsdauer nicht länger als für die jeweilige Zweckbestimmung?

## **1.7    Transparenz und Beschreibung der Verfahrens**

- 1.7.1 Ist eine Transparenz in Hinblick auf die Datenverarbeitung und bezüglich der Nutzer der Verfahren oder auch der Betroffenen gesichert?  
(Datenfluss, Datenortung, Übertragungswege etc.)
- 1.7.2 Werden den Nutzern informative, auf dem neuesten Stand befindliche, verstehbare und mit einem richtigen Bezugs- und Suchsystem versehene Informationen übergeben? Ist es einfach, Zugang zu den Beschreibungen zu bekommen? Wie werden sie aktualisiert?
- 1.7.3 Sind die Grundkonzepte, auf die die Prozesse aufbauen, klar ausgewiesen?
- 1.7.4 Ist ein besonderes Wissen erforderlich, um die Beschreibung der Prozesse zu verstehen?
- 1.7.5 Sind Quellcodes zugänglich? Wem? Auch für externe Vertragspartner oder nur für einen ausgewiesenen Kreis von Experten?

## 1.8 Datenschutzerklärung

- 1.8.1 Sind informative, aktuelle und verstehbare Datenschutzerklärungen verfügbar?
- 1.8.2 Geben die Datenschutzerklärungen ausreichend Informationen über wichtige Datenschutzangelegenheiten?
- 1.8.3 Liefern die Datenschutzerklärungen spezifische und aussagefähige Informationen über die Verarbeitung personenbezogener Daten anstelle bloßer Versicherungen einer Erfüllung der gesetzlichen Pflichten?
- 1.8.4 Wird das Konzept der “highlight notices” genutzt, d. h. die wichtigsten Informationen werden so geliefert, dass sie auf einen Blick erkennbar sind?
- 1.8.5 Werden die Datenschutzerklärungen mehrsprachig verfügbar gemacht?
- 1.8.6 Sind die Datenschutzerklärungen deutlich erkennbar auf den Homepages der entsprechenden Webseiten gelinkt?
- 1.8.7 Gibt die Datenschutzerklärung Informationen über die Identität der datenverarbeitenden Stelle? Gibt sie Kontaktdetails, um im Falle von Fragen oder Beschwerden Kontakt aufzunehmen?

## 2 Legitimation der Datenverarbeitung

### 2.1 Zulässigkeit der Verarbeitung personenbezogener Daten durch Einverständnis

**Dieser Gegenstand betrifft die Legitimität der Datenverarbeitung. Insbesondere handelt es sich um die Frage der gesetzlichen Grundlage der Verarbeitung, besonderen Anforderungen bezogen auf die verschiedenen Phasen der Verarbeitung, der Erfüllung der allgemeinen Anforderungen an die Grundsätze und Pflichten des Datenschutzes und einer Reihe von besonderen Arten der Datenverarbeitungstätigkeiten.**

- 2.1.1 Entspricht das Einverständnis der Betroffenen in der vorliegenden Form den gesetzlichen Anforderungen über Einverständniserklärungen?
- 2.1.2 Ist die Zustimmung unzweideutig und ausreichend gezielt formuliert, indem der Zweck und die verschiedenen Phasen der Datenverarbeitung dargelegt sind?
- 2.1.3 Ist der Fall ausgeschlossen, dass die Betroffenen unter Druck gesetzt werden, Vorteile versprochen bekommen oder Nachteile angedroht werden?

### 2.2 Zulässigkeit der Verarbeitung personenbezogener Daten durch Vertragsverhältnis

- 2.2.1 Werden alle Verarbeitungen von personenbezogenen Daten wirklich für die Erfüllung der Verträge gebraucht? Wenn nicht, bitte beschreiben.
- 2.2.2 Sind die Verträge, die von den Betroffenen gezeichnet werden, frei von Vorbehalten, die die Sammlung von weiteren personenbezogenen Daten, als für die Vertragserfüllung erforderlich, erlaubt?
- 2.2.3 Sind diese Vorbehalte akzeptierbar?
- 2.2.4 Sind die Bearbeiter darüber unterrichtet, was der Zweck der zusätzlich gefragten Information ist, und dass die Angabe dieser zusätzlichen Information freiwillig ist?

## **2.3 Zulässigkeit der Verarbeitung personenbezogener Daten durch gesetzliche Verpflichtung**

- 2.3.1 Durch welche gesetzliche Grundlage ist diese Verpflichtung gestützt?
- 2.3.2 Gibt es gesetzliche Regelungen, die ausdrücklich auflisten, welche Daten erhoben werden dürfen?
- 2.3.3 Wenn ja: Sichern die entsprechenden Verfahren dies? Ist sichergestellt, dass die verwendeten Programme dem entsprechen und nicht frei editierbare Felder haben?

## **2.4 Zulässigkeit der Verarbeitung personenbezogener Daten durch lebenswichtige Interessen**

- 2.4.1 Gibt es erhebliche lebenswichtige Interessen der datenverarbeitenden Stelle?
- 2.4.2 Wie wird "lebenswichtig" ausgelegt?
- 2.4.3 Ist es notwendig, sich darauf zu berufen oder kann ein Einverständnis mit dem Betroffenen eingeholt werden?

## **2.5 Zulässigkeit der Verarbeitung personenbezogener Daten durch öffentliche Aufgaben**

- 2.5.1 Welches ist der entsprechende gesetzliche Vorbehalt?
- 2.5.2 Wird die Verarbeitung / werden die Daten für die Aufgaben wirklich gebraucht?

## **2.6 Zulässigkeit der Verarbeitung personenbezogener Daten durch Interessenausgleich**

- 2.6.1 Welche legitimen Interessen der datenverarbeitenden Stelle werden durch die Verfahren bedient?
- 2.6.2 Welche fundamentalen Rechte und Interessen der Betroffenen werden durch die Verarbeitung berührt?

- 2.6.3 Ist eine Verhältnismäßigkeit zwischen den legitimen Interessen der datenverarbeitenden Stelle und den Rechten und Interessen der Betroffenen gesichert?

## 3 Legitimation der Verarbeitung besonderer personenbezogener Daten

### 3.1 Zulässigkeit der Verarbeitung sensibler personenbezogener Daten durch ausdrückliches Einverständnis

3.1.1 Genügt das Einverständnis der Betroffenen in der von ihm ausgedrückten Form den Anforderungen an ein Einverständnis?

3.1.2 Wie ausdrücklich ist das Einverständnis?

### 3.2 Zulässigkeit der Verarbeitung sensibler personenbezogener Daten durch Arbeitsrecht

3.2.1 Erfüllen die Verfahren die Pflichten und die entsprechenden Rechte der datenverarbeitenden Stelle auf dem Gebiet des Arbeitsrechtes?

3.2.2 Wie genau ist die Berechtigung durch Gesetze? Deckt es die Verarbeitung ab?

3.2.3 Welche Sicherheitsvorkehrungen liefern die Gesetze? Sind sie erfüllt?

### 3.3 Zulässigkeit der Verarbeitung sensibler personenbezogener Daten auf Grund von lebenswichtigen Interessen

3.3.1 Was sind die erheblichen lebenswichtigen Interessen?

3.3.2 Wie wird "lebenswichtig" ausgelegt?

3.3.3 Sind Betroffene physisch oder gesetzlich nicht in der Lage, ihr Einverständnis zu geben?

### 3.4 Zulässigkeit der Verarbeitung sensibler personenbezogener Daten durch gemeinnützige Einrichtungen

3.4.1 Werden personenbezogene Daten von einer Stelle verarbeitet, die politische, religiöse, philosophische oder gewerkschaftliche Ziele verfolgt? Handelt es sich um eine gemeinnützige Einrichtung?

siehe: Tendenzschutz

3.4.2 Wird eine Datenverarbeitung im Zusammenhang mit den legitimen Aktivitäten der Einrichtung durchgeführt? Wer bestimmt dies?

3.4.3 Betrifft die Verarbeitung wirklich nur die Mitglieder dieser Einrichtung und nicht Personen, die nur regelmäßig Kontakt in Verbindung mit den Zwecken der Einrichtung haben?

3.4.4 Sind personenbezogene Daten nur mit dem Einverständnis des Betroffenen zur Weitergabe an Dritte freigegeben?

### **3.5 Zulässigkeit der Verarbeitung sensibler personenbezogener Daten aus Veröffentlichungen**

3.5.1 Bezieht die Datenverarbeitung Daten ein, die vom Betroffenen ausdrücklich veröffentlicht worden sind?

3.5.3 Gibt es Aussagen über die Hautfarbe einer Person oder über offensichtliche körperliche Behinderungen?

### **3.6 Zulässigkeit der Verarbeitung sensibler personenbezogener Daten zur Wahrnehmung berechtigter Interessen**

3.6.1 Bezieht sich diese Verarbeitung auf Daten, die für die datenverarbeitende Stelle bei der Ausübung Ihrer rechtlichen Forderungen oder Verteidigungen notwendig sind?

3.6.2 Wie gut ist begründet, ob die Daten für die datenverarbeitende Stelle bei der Ausübung Ihrer rechtlichen Forderungen oder Verteidigungen notwendig sind?

3.6.3 Wer liefert die Begründung?

### **3.7 Verarbeitung besonderer personenbezogener Daten auf besonderer gesetzlicher Grundlage**

3.7.1 Welches ist die gesetzliche Grundlage?

3.7.2 Welchem wichtigen öffentlichen Interesse ist damit gedient?

- 3.7.3 Ist die Verarbeitung auf bestimmte empfindliche personenbezogene Daten ausgerichtet?
- 3.7.4 Welche Sicherheitsvorkehrungen liegen in der Verarbeitung? Sind sie angemessen?
- 3.7.5 Ist die gesetzliche Grundlage in der EU-Datenschutzrichtlinie hinterlegt?

## 4 Anforderungen an die Datenverarbeitung für besondere Zwecke

### 4.1 Verarbeitung von sensiblen personenbezogenen Daten für medizinische und verwandte Zwecke

- 4.1.1 Sind empfindliche Daten für eine der folgenden Zwecke erfasst: Vorbeugende Medizin, medizinische Diagnose, Gesundheitsversorgung, Management im Gesundheitsdienst?
- 4.1.2 Wenn ja: Dienen die Daten alle dem Zweck und geht nichts darüber hinaus?
- 4.1.3 Sind die Daten anonymisiert oder pseudonymisiert wann immer es möglich ist, besonders wenn es sich um sekundäre Zwecke handelt?
- 4.1.4 Werden die Daten von Fachleuten im Gesundheitswesen verarbeitet? Unterliegen sie der Schweigepflicht?
- 4.1.5 Wenn es sich um Fachleute handelt, die nicht aus dem Gesundheitsbereich sind, unterliegen sie entsprechenden Schweigepflichten?

### 4.2 Verarbeitung von Daten über strafrechtliche Verurteilungen

- 4.2.1 Werden Daten erfasst, die sich auf Straftaten, Verurteilungen oder Sicherheitsmaßnahmen beziehen?
- 4.2.2 Wenn ja: Werden die Daten nur unter der Aufsicht einer Behörde verarbeitet? Durch welches Gesetz?
- 4.2.3 Werden die Daten durch eine nicht-öffentliche Einrichtung verarbeitet?
- 4.2.4 Wenn ja: Durch welches Gesetz?
- 4.2.5 Welche Sicherheitsvorkehrungen sind durch diese Gesetze gefordert? Sind sie genau passend und angemessen?

4.2.6 Sind sie so detailliert ausgeführt, dass die Daten nicht zu einer vollständigen Auflistung der Verurteilungen führen?

4.2.7 Ist die Genehmigung, solche Daten zu verarbeiten, in der EU-Datenschutzrichtlinie genannt?

## **4.3 Verarbeitung von Daten von Ordnungswidrigkeitsverfahren und zivilrechtliche Urteile**

4.3.1 Werden Daten erhoben, die sich auf Bußgelder oder Urteile in Zivilverfahren beziehen?

## **4.5 Verarbeitung von Daten für den ausschließlichen Zweck des Journalismus oder des künstlerischen oder literarischen Ausdrucks**

4.5.1 Wird eine Verarbeitung zum Zwecke des journalistischen, künstlerischen oder literarischen Ausdrucks betrieben?

4.5.2 Wenn ja: Ist das der einzige Zweck? Wer bestimmt das und wie?

4.5.3 Gibt es nach nationalem Recht eine Regelung für die Verarbeitung von Daten für diesen Zweck?

## 5 Besondere Einschränkungen für bestimmte Datenverarbeitungsprozesse

### 5.1 Besondere Einschränkungen in der Verarbeitung von Suchdaten

5.1.1 Ist sichergestellt, dass nicht durch eine Kombination von Suchdaten ein persönliches Profiling angelegt wird?

### 5.2 Besondere Einschränkungen bei unverlangten Direkt-Marketing-Kontakten mit Vertragspartnern

5.2.1 Ist sichergestellt, dass nicht durch Auswertung von Kaufdaten ein Profiling zur Vermarktung von Produkten und Leistungen außerhalb des erklärten Interesses des Kunden angelegt wird?

## 6 Besondere Anforderungen an die Phasen der Datenverarbeitung

Diese Kapitel behandelt die besonderen Anforderungen bezogen auf die verschiedenen Phasen der Datenverarbeitung.

### 6.1 Informationspflichten bei der Datenerhebung

- 6.1.1 Werden Daten von Betroffenen oder von anderen Quellen erhoben?
- 6.1.2 Wenn ja: Ist sichergestellt, dass Daten nicht heimlich erhoben werden, d. h. ohne Kenntnisnahme des Betroffenen?
- 6.1.3 Werden Aufzeichnungen über die Datenquellen gemacht?
- 6.1.4 Werden die Betroffenen und entsprechende Dritte über verschiedene Umstände so informiert, wie die Gesetze es fordern?

### 6.2 Interner Datenverschluss

- 6.2.1 Werden die Daten intern nur denen zugänglich gemacht, die den Zugang benötigen? Wie ist dies gesichert?
- 6.2.2 Werden die Daten intern auch für einen anderen als den ursprünglichen Zweck zugänglich gemacht?
- 6.2.3 Wenn ja: Was ist die gesetzliche Grundlage für eine weitere Verarbeitung?
- 6.2.4 Sind die sekundären Zwecke mit den primären Zwecken, für die die Daten erhoben wurden, vereinbar?
- 6.2.5 Werden nur die Daten, die gebraucht werden, demjenigen, der sie für den sekundären Zweck benötigt, zugänglich gemacht?
- 6.2.6 Sind die Betroffenen darüber informiert, entweder bei der Erhebung oder bei der ersten Zugänglichmachung für einen neuen Zweck?

6.2.7 Wenn ja: Wie haben sie diese Information erhalten?

## **6.3 Verschluss von Daten gegenüber Dritten**

6.3.1 Werden die Daten an Dritte weitergegeben für den Zweck, zu dem sie ursprünglich erhoben wurden?

6.3.2 Wenn ja: Wer sind die Dritten?

6.3.3 Sind die Betroffenen informiert über den Zugang, über die einzelnen Daten oder wenigstens über die Art der Daten, die zugänglich gemacht wurden und über den/die Empfänger oder wenigstens die Art der Empfänger?

6.3.4 Werden Zugänglichmachungen für Dritte aufgezeichnet?

6.3.5 Werden die Empfänger darüber informiert, dass sie die Daten nur für den Zweck nutzen dürfen, für den sie diese erhalten haben?

6.3.6 Wird gefordert, dass sie dafür garantieren sollen?

6.3.7 Sind solche Garantien bindend?

6.3.8 Können sich die Betroffenen darauf berufen?

6.3.9 Werden nur Daten weitergegeben, die für den Zweck gebraucht werden, für den sie bei dem/den Dritten verarbeitet werden?

## **6.4 Löschung von Daten nach Ablauf der Erforderlichkeit**

6.4.1 Ist gesichert, dass personenbezogene Daten, ob aktuelle Daten oder Back-ups, gelöscht oder anonymisiert werden, wenn sie nicht mehr gebraucht werden für den Zweck, für den sie gespeichert wurden?

- 6.4.2 Sind genaue Aufbewahrungsfristen gesetzt oder Termine benannt, wann Daten überprüft werden?
- 6.4.3 Wie ist gesichert, dass diese Anforderungen eingehalten werden?
- 6.4.4 Können Daten, die nicht länger für den ursprünglichen Zweck gebraucht werden, aber nicht wegen Aufbewahrungspflichten gelöscht werden dürfen, gesperrt oder sonstwie von der gewöhnlichen Verarbeitung ausgeschlossen werden?

## 7 Konformität mit den allgemeinen Grundsätzen des Datenschutzes

### 7.1 Benennung des Zweckes und Begrenzung des Zweckes

- 7.1.1 Werden die Daten für ausgewiesene, ausdrückliche und legitime Zwecke erhoben?
- 7.1.2 Wie sind die Zwecke, für die Daten erhoben werden, dokumentiert?
- 7.1.3 Werden die Daten weiter für andere Zwecke, als diejenigen, für die sie ursprünglich erhoben wurden, verarbeitet?
- 7.1.4 Sind diese anderen Zwecke mit denjenigen Zwecken vereinbar, für den die Daten ursprünglich erhoben worden sind?
- 7.1.5 Werden Aufzeichnungen über die Verarbeitungsschritte gemacht, so dass es möglich ist, einen Datenmissbrauch zu ermitteln?
- 7.1.6 Ist die Aufzeichnung manipulationssicher?
- 7.1.7 Wird Datensparsamkeit betrieben und gibt es Vorkehrungen, um zu verhindern, dass auf Datensätze durch andere Prozesse zugegriffen werden kann?

### 7.2 Angemessenheit

- 7.2.1 Unter der Annahme, dass die rechtliche Grundlage für die Verarbeitung personenbezogener Daten gegeben ist, ist eine vernünftige Relation zwischen dem Zweck und dem Datenumfang gegeben?
- 7.2.2 Wenn ja: Sind die Inhalte der Datenfelder angemessen?

### 7.3 Datenqualität

- 7.3.1 Sind vernünftige technische Vorkehrungen getroffen worden, um sicherzustellen, dass die Genauigkeit, Vollständigkeit und Aktualität der Daten gegeben ist?

## 8 Besondere Arten der Datenverarbeitung

### 8.1 Datenverarbeitung durch die zuständige Stelle

- 8.1.1 Empfängt die Datenverarbeitende Stelle Daten zur Verarbeitung?
- 8.1.2 Wenn ja: Was für Daten?
- 8.1.3 Gibt es eine getrennte gewerbliche Stelle für Auftragsdatenverarbeitung?
- 8.1.4 Ist die Verarbeitung durch die datenverarbeitende Stelle gesetzlich erlaubt?
- 8.1.5 Ist die Verarbeitung durch die datenverarbeitende Stelle anhand eines schriftlichen Vertrages oder durch ein anderes gesetzliches Mittel geregelt?
- 8.1.6 Führt dieser Vertrag oder anderes gesetzliches Mittel aus, dass der Auftragsdatenverarbeiter nur auf Anweisung der datenverarbeitenden Stelle handeln kann?
- 8.1.7 Fordert dieser Vertrag oder dieses gesetzliche Mittel, dass der Auftragsdatenverarbeiter alle notwendigen Sicherheitsmaßnahmen anwendet?
- 8.1.8 Wie prüft der Auftragsdatenverarbeiter die Übereinstimmung mit den Anforderungen im Vertrag mit der datenverarbeitenden Stelle oder den gesetzlichen Mitteln?

### 8.2 Übergabe an Drittländer

- 8.2.1 Werden Daten übermittelt an Länder, die weder Mitglieder der EU noch der Europäischen Wirtschaftszone sind?  
siehe Drittländer
- 8.2.2 Sichert das in Frage kommende Drittland einen angemessenen Schutz?

- 8.2.3 Wenn das Drittland keinen entsprechenden Schutz garantiert, ist einer der gesetzlichen Ausnahmetatbestände anwendbar?
- 8.2.4 Im Einzelnen: Ist die Übermittlung erforderlich für die Erfüllung eines Vertrages zwischen dem Betroffenen und der datenverarbeitenden Stelle?
- 8.2.5 Gibt es bindende Verbandsregeln an dessen Stelle, um die Erfüllung der Anforderungen der Datenschutzrichtlinie durch alle Beteiligten sicherzustellen?
- 8.2.6 Wenn die personenbezogenen Daten in die USA übermittelt werden: Hat sich der Empfänger dem Safe Harbor-System angeschlossen?

## 9 Formalitäten

### 9.1 Benachrichtigung

- 9.1.1 Gibt es bei der Verarbeitung Anforderungen für eine Benachrichtigung?
- 9.1.2 Sind die Informationen zum Benachrichtigten bereits verfügbar?
- 9.1.3 Gibt es Verfahren, die sichern, dass die Einzelheiten der Benachrichtigungen nötigenfalls auf den neuesten Stand gebracht werden?

### 9.2 Vorabprüfung

- 9.2.1 Gibt es Verfahren, die eine Vorprüfung verlangen?
- 9.2.2 Wenn ja: Sind die Informationen für solche Vorabprüfungen fertig verfügbar und wurden diese der Person, die die Prüfung ausführt, übergeben?
- 9.2.3 Wer führt die Vorabprüfung durch?
- 9.2.4 Sind die entsprechenden Verfahren tatsächlich wie erforderlich vorab geprüft und mit den gesetzlichen Anforderungen übereinstimmend gesehen worden?

## 10 Sicherung der Rechte der Betroffenen

Dieses Kapitel listet die Kriterien auf, die bei der praktischen Einrichtung der Rechte der Betroffenen anzuwenden sind. Im Einzelnen handelt es von den Rechten informiert zu werden, dem Recht aus Zugang, Korrektur, Löschung und Sperrung entsprechend der Richtlinie 95/46/EC. . Weiterhin betrifft dieses Kapitel die Rechte, die durch die Richtlinie 2002/58/EC gesichert sind. Beispiel: Das Recht auf Vertraulichkeit der Kommunikation und das Recht über Sicherheitsrisiken informiert zu sein.

### 10.1 Das Recht, informiert zu werden, allgemein

- 10.1.1 Sind die Betroffenen durch die datenverarbeitende Stelle informiert worden?
- 10.1.2 Wenn ja: Weist die Information die Identität der datenverarbeitenden Stelle oder ggf. seines Vertreters aus?
- 10.1.3 Wenn ja: Schließt diese Information den Zweck der Verarbeitung ein?  
Nicht nur den primären Zweck, für den die Daten erhoben wurden, sondern auch andere, nicht-offensichtliche sekundäre Zwecke.
- 10.1.4 Wenn ja: Schließt die Information die Empfänger oder Kategorien von Empfängern ein, die Zugang zu den Daten erhalten?
- 10.1.5 Wenn ja: Enthält diese Information Kategorien von Daten, die betroffen sind?
- 10.1.6 Wenn ja: Schließt die Information Angaben darüber ein, ob Antworten auf Fragen verpflichtend oder freiwillig sind, als auch die möglichen Konsequenzen bei einer Nichtbeantwortung.
- 10.1.7 Wenn ja: Schließt die Information die Rechtsbelehrung über den Zugang zu den Daten und das Recht auf Korrektur der Daten des Betroffenen ein?
- 10.1.8 Welche anderen Informationen stehen zur Abgabe bereit?

- 10.1.9 Wenn nicht: Hat der Betroffene bereits diese Informationen?
- 10.1.10 Gibt es besondere Maßnahmen, um die Transparenz zu verbessern?
- 10.1.11 Wenn ja: Können ausgewiesene Verarbeitungsschritte den Betroffenen erklärt werden?

## **10.2 Das Recht, informiert zu werden, Informationen an die Betroffenen bei einer direkten Datenerhebung**

- 10.2.1 Welche Informationen erhält der Betroffene zum Zeitpunkt der Datenerhebung?
- 10.2.2 Wie wird dies übergeben?  
Beispiel: Im Datenerhebungsbogen, im Pop-up Fenster auf der Webseite
- 10.2.3 Ist die Aufmerksamkeit des Betroffenen besonders hierauf gelenkt?  
oder ist es halb versteckt, kleiner geschrieben

## **10.3 Das Recht Informiert zu werden, Informationen, die an die Betroffenen übergeben werden, wenn Daten von anderen Quellen erhoben werden.**

- 10.3.1 Welche Information gibt die datenverarbeitende Stelle dem Betroffenen und wann gibt sie diese?
- 10.3.2 Wie wird sie übergeben?  
Beispiel: Brief, , Link auf einer Webseite
- 10.3.3 Wie klar ist die Information? Wird der Betroffene sich sofort bewusst darüber, dass eine Nachricht eine Information über ihn oder einen Dritten enthielt?

## **10.4 Zugangsrechte**

- 10.4.1 Gibt es Zugang zu allen wichtigen Informationen über die Daten und die Betroffenen?
- 10.4.2 Wird für alle wichtigen Informationen über die Zwecke der Verarbeitung Zugang gewährt?

- 10.4.3 Wird für alle wichtigen Informationen über die Herkunft und Kategorien der Empfänger Zugang gewährt?
- 10.4.4 Wird für alle wichtigen Informationen über Einzelheiten der Verarbeitung Zugang gewährt?
- 10.4.5 Wird für alle wichtigen Informationen über Einzelheiten der logischen Struktur der Datenbanken Zugang gewährt?
- 10.4.6 Können alle Daten über den Betroffenen leicht abgerufen werden, um eine Anfrage schnell und wirksam bearbeiten zu können?
- 10.4.7 Wie wird die Identität der Betroffenen geprüft?
- 10.4.8 Werden Datenzugänge aufgezeichnet?

## **10.5 Recht auf Korrektur**

- 10.5.1 Sind Funktionen vorhanden, um bei Bedarf Datenkorrekturen vorzunehmen?
- 10.5.2 Werden Irrtümer automatisch korrigiert?
- 10.5.3 Wie werden sonst angemessene und sofortige Berichtigungen gesichert?
- 10.5.4 Wie wird die Qualität solcher Korrekturen gesichert?
- 10.5.5 Wie wird die Identität eines Betroffenen, der eine Korrektur verlangt, geprüft?
- 10.5.6 Werden vorherige Empfänger der Daten über die Korrekturen informiert?
- 10.5.7 Ist dies von bestimmten Umständen abhängig?
- 10.5.8 Wenn ja: Von welchen?

10.5.9 Wird der Betroffene darin einbezogen?

## 10.6 Recht auf Löschung

10.6.1 Wenn Daten gelöscht werden, wie geschieht das? Ist die Löschung vollständig und irreversibel? Wie werden unbeabsichtigte Kopien vermieden?

10.6.2 Können Daten selektiv gelöscht werden?

10.6.3 Werden Daten durch Überschreiben gelöscht?

10.6.4 Wenn ja: Ist das Überschreiben ausreichend?

10.6.4 Wie wirkt sich das Löschen auf die Datensicherung aus?

10.6.5 Werden frühere Empfänger von Daten über die Löschung informiert?

10.6.6 Hängt dies von bestimmten Umständen ab?

10.6.7 Wenn ja: Von welchen? Wird der Betroffene darin einbezogen?

10.6.8 Wie werden Löschfristen oder Wiedervorlagen zur Prüfung der Löschbarkeit behandelt?

## 10.7 Recht auf Sperrung

10.7.1 Können die Daten markiert werden, so dass sie nicht mehr für die gewöhnliche Verarbeitung gebraucht werden, während sie in der Datenbank verbleiben? Wie geschieht dieses?

Technik des "Flags setzen"

10.7.2 Werden von solchen Sperrungen Aufzeichnungen gemacht?

## 10.8 Recht auf Widerspruch zur Verarbeitung

- 10.8.1 Gibt es technische Mittel, das Recht des Betroffenen, Einspruch gegen die Datenverarbeitung zu erheben, zu realisieren?
- 10.8.2 Wenn ja : Wie geht das?
- 10.8.3 Werden Einsprüche an die früheren Empfänger der Daten weitergegeben? Wie geschieht dies?
- 10.8.4 Wie werden in dem Land, in dem sich der Standort der datenverarbeitenden Stelle befindet, die Rechte auf Widerspruch zur Datenverarbeitung zum Zwecke des Direkt Marketings geregelt?
- 10.8.5 Sind Mechanismen vorhanden, um diese Regelungen zu erfüllen?

## **10.9 Das Recht über Sicherheitsrisiken informiert zu werden**

- 10.9.1 Ist die Datenverarbeitende Stelle (auch) ein Provider für elektronische Kommunikations-Dienste?
- 10.9.2 Wenn ja: Hat die datenverarbeitende Stelle angemessene Systeme zur Verfügung, um den Dienst sicher zu machen?
- 10.9.3 Kann das Unternehmen Sicherheitsrisiken angemessen und ausreichend identifizieren?
- 10.9.4 Welche Maßnahmen werden getroffen, um dem Unternehmen zu ermöglichen, die User oder Kommunikationsteilnehmer über solche Risiken zu informieren?
- 10.9.5 Werden die Kommunikationsteilnehmer tatsächlich über solche Risiken informiert? Gibt es aus der letzten Zeit Fälle?

## **10.10 Das Post und Fernmeldegeheimnis**

- 10.10.1 Sind angemessene Maßnahmen eingesetzt worden, um zu verhindern, dass Abhören, Speichern oder andere Formen, Abfangen oder Überwachung der Kommunikation oder entsprechende Verbindungsdaten durch andere Personen geschieht als durch die jeweiligen Nutzer?
- 10.10.2 Geschieht dies ohne das Einverständnis der Betroffenen, außer wenn es gesetzlich autorisiert ist?
- 10.10.3 Wenn die Daten vorübergehend aus technischen Gründen gespeichert werden, geschieht dies ohne Verletzung des Post- und Fernmeldegeheimnisses?
- 10.10.4 Wie wird in diesem Zusammenhang das Post- und Fernmeldegeheimnis sichergestellt?
- 10.10.5 Welche Maßnahmen werden getroffen, um sicherzustellen, dass Mitschnitte etc., die vorgeblich legal sind (wie das Verhindern von Betrug) tatsächlich mit der Gesetzeslage übereinstimmen?
- 10.10.6 Welche Maßnahmen werden getroffen, um eine sichere, z. B. manipulationsfreie Aufzeichnung zur Übergabe der Mitschnitte oder anderer Kommunikationsdetails, wie Verbindungsdaten oder Ortungsdaten an die Strafverfolgungsbehörden, zu schaffen?

## **10.11 Das Recht informiert zu werden über Cookies und andere Informationen, die auf Endgeräten gespeichert sind.**

- 10.11.1 Wird der betroffene Nutzer mit klaren und vollständigen Informationen über den Zweck der Verarbeitung versorgt?

## **10.12 Das Recht Rechnungen ohne Details zu erhalten.**

- 10.12.1 Bietet die datenverarbeitende Stelle elektronische Kommunikationsdienste gegen Rechnung an?
- 10.12.2 Wenn ja: Welche Alternativen werden angeboten gegenüber Rechnungen mit allen Verbindungsdetails?

- 10.12.3 Wie werden die Kunden über diese Optionen informiert und können zwischen solchen Alternativen wählen? Sind sie frei von Gebühren?

## **10.13 Das Recht, bei ausgehenden Leitungen die Rufnummer zu unterdrücken**

- 10.13.1 Bietet das Unternehmen elektronische Kommunikation einschließlich mobiler und fester telefonischer Kommunikation an?
- 10.13.2 Wenn ja: Bietet das Unternehmen einfache und leichte Mittel, damit der Kunde die oben genannten Optionen nutzen kann? Ist diese kostenlos?
- 10.13.3 Wird die Öffentlichkeit über diese Optionen informiert?

## **10.14 Besondere Rechte bezüglich der Verzeichnisse von Teilnehmern elektronischer Kommunikationsdienste**

- 10.14.1 Veröffentlicht das Unternehmen eine öffentliches Verzeichnis seiner Kommunikationsteilnehmer?
- 10.14.2 Wenn ja: Was ist der Zweck des Verzeichnisses?
- 10.14.3 In welcher Form geschieht dies?  
(Buch, CD ROM, online)
- 10.14.4 Gibt es in diesem Verzeichnis besondere Funktionen?  
z. B. Rückwärtssuche
- 10.14.5 Wenn ja: Sind die Betroffenen darüber informiert und haben sie ihr Einverständnis gegeben?
- 10.14.6 Im umgekehrten Fall: Sind Maßnahmen getroffen worden, um sicherzustellen, dass bestimmte Dienste nicht unterstützt werden?
- 10.14.7 Wie wirksam ist dies? Kann es einfach umgangen werden?
- 10.14.8 Können Teilnehmer entscheiden, dass eine Weitergabe ihrer Daten zu Marketingzwecken verwendet wird?

10.14.9 Wenn ja: Können sie das kostenfrei? Wie wirkt sich solch eine Entscheidung aus?

## 11 Personalangelegenheiten

### 11.1 Personalwirtschaft

- 11.1.1 Ist ein rechtmäßiger Umgang mit Arbeitnehmerdaten nach § 28 BDSG gesichert?
- 11.1.2 Ist ein rechtmäßiger Umgang mit Bewerberdaten nach § 28 BDSG gesichert?
- 11.1.3 Ist die Zulässigkeit von Eingriffen in das Fernmeldegeheimnis bei der Überwachung der Telekommunikation und des Internetverhaltens der Mitarbeiter gesichert?

### 11.2 Betriebsrat

- 11.2.1 Sind die Informations- und Mitspracherechte des Betriebsrats bei der Durchführung von Sicherheitskontrollen gewährleistet?
- 11.2.2 Sind die Informations- und Mitspracherechte des Betriebsrats hinsichtlich der Überwachung von Leistung und Verhalten der Mitarbeiter nach § 87 Abs. 1 Nr. 6 BetrVG gewährleistet?

## 12 Verhinderung von unberechtigtem Zugang zu Daten, Programmen, Grundstücken, Gebäuden und Geräten

Die Verhinderung von unbefugtem Zugang zu Daten ist eine der Schlüsselmaßnahmen, um den Verlust der Integrität, Vertraulichkeit und Verfügbarkeit von personenbezogenen Daten zu verhindern. Der Zugang muss auf einem physischen und einem logischen Niveau geregelt werden: Der physische Zugang bezieht sich auf den Zugang zu Einrichtungen, Räumen, Hardware, Verbindungsleitungen, Datenspeicher usw., während der logische Zugang sich auf nicht-physischen Zugang zu Daten, Software, Funktionalitäten, usw. bezieht. Aus technischer Sicht ist der Zugang nicht nur auf natürliche Personen beschränkt, sondern schließt auch den Zugang über Hard- und Software ein. Dies betrifft insbesondere Treiber, Links und Verfahren, die Systeme verbinden.

### 12.1 Physikalische Zugriffskontrolle

Die physische Zugangskontrolle ist bedeutend für die "real life" - Datenverarbeitung, für den tatsächlichen Gebrauch der IT-Prozesse und der IT-Dienste.

- 12.1.1 Welche Maßnahmen verhindern unerlaubten Zugang zu Einrichtungen, Räumen, Hardware, Archiven, beweglichen Medien, Ausdrucken?
- 12.1.2 Sind diese Maßnahmen angemessen?
- 12.1.3 Werden Zugänge aufgezeichnet?

### 12.2 Zugang zu Speichermedien und mobilen Geräten

Eine Zugangskontrolle zu Medien, die Daten speichern (Bänder, CDs/DVDs usw.) ist entscheidend weil die logische Zugangskontrolle (wie Lese-/Schreibrechte auf Dateien oder Datenbanktabellen) oft umgangen werden kann, wenn man einmal Zugang zu diesen Medien hat.

- 12.2.1 Speichert das Unternehmen die Sicherung auf beweglichen Datenträgern?
- 12.2.2 Wenn ja: Werden die beweglichen Datenträger sicher aufbewahrt?
- 12.2.3 Speichert das Unternehmen Daten auf Papierdokumenten?

- 12.2.4 Wenn ja: Werden die Ausdrücke sicher aufbewahrt?
- 12.2.5 Sind Hardwaregegenstände, die Daten tragen, beweglich und müssen auf die gleiche Art wie bewegliche Medien behandelt werden?
- 12.2.6 Wenn ja: Werden bewegliche Medien sicher gelagert?
- 12.2.7 Wenn ja: Gibt es Aufzeichnungen über die Medien, deren Inhalt und den Verbleib?

## **12.3 Zugang zu Daten, Programmen und Geräten**

- 12.3.1 Sichert die datenverarbeitende Stelle die Hardware mit mechanischen Schlössern, PIN und Passwörtern?
- 12.3.2 Software: Hat die datenverarbeitende Stelle Zugangskontrollen entsprechend dem "Rollen-Modell" eingerichtet?
- 12.3.3 Feinkörnigkeit: Können die Zugangsrechte so gesichert werden, dass sie sich auf Lesen, Schreiben, Übertragen, Drucken etc. beziehen und bei den Daten auf Datei, Datensatz, Feld, Tabelle etc.?
- 12.3.4 Gibt es entsprechende Rollen für die Verwaltung der Zugangsrechte?  
Gewährung und Widerruf von Rechten, Gruppen und Zuordnungen zu den User-Accounts
- 12.3.5 Ist die Administration der Zugangsrechte getrennt von der technischen Administration?
- 12.3.6 Werden die Einrichtungen der Zugangskontrolle ordentlich genutzt?
- 12.3.7 Wer verwaltet die Zugangsrechte?

## **12.4 Identifikation und Authentifizierung**

- 12.4.1 Liefert die Administration angemessene Identifikation als Authentifizierungsmittel?

12.4.2 Verhindert das System wiederholte Versuche der Identifikation und Authentifizierung nach einer bestimmten Anzahl von gescheiterten Versuchen?

12.4.3 Ist die Methode der Verhinderung angemessen?

## 12.5 Gebrauch von Passwörtern

12.5.1 Durch welchen Mechanismus ist gesichert, dass die Passwörter vertraulich und sicher zugewiesen, verteilt und aufbewahrt werden?

12.5.2 Sind sie so aufbewahrt, dass sie nicht aus den gespeicherten Daten wiederhergestellt werden können?

12.5.3 Können User leicht ihre Passwörter ändern?

12.5.4 Erzwingt das Unternehmen einen periodischen Passwortwechsel?

12.5.5 Liefern die Systeme Mechanismen, um eine ausreichende Passwortqualität zu sichern?

12.5.6 Werden sowohl Laufzeiten als auch die Qualität der Passwörter von der Administration gesteuert?

12.5.7 Was geschieht im Falle eines vergessenen Passwortes? Werden Passwörter per e-mail versendet?

12.5.8 Welche Prozesse sichern, dass die Passwörter auf vertrauliche Weise vergeben, verteilt und gespeichert werden und ihre Integrität behalten?

12.5.9 Werden Passwortwechsel in regelmäßigen Abständen gefordert?

12.5.10 Können Passwörter, die für eine maschinenbetriebene Authentifizierung gebraucht werden, ausgewechselt werden?

12.5.11 Wird eine Minimalqualität für Passwörter verlangt?

## 12.6 Organisation und Dokumentation der Zugangskontrolle

- 12.6.1 Bietet das System einen leichten Zugang zum Verzeichnis für die User-Rechte?
- 12.6.2 Sind Einzelheiten verfügbar über Zeiträume, Personen, Gruppen und der Gewährung/des Widerrufs von Zugangsrechten?
- 12.6.3 Ist eine Log-Datei dazu verfügbar? Wird sie automatisch erstellt?
- 12.6.4 Sind Zugangsrechte ordentlich organisiert, klar dokumentiert und eindeutig für jeden User?
- 12.6.5 Sind die Regeln für die Verwaltung der Zugangsrechte ordentlich und klar dokumentiert?
- 12.6.6 Werden Rechte zurückgenommen, wenn sie nicht länger gebraucht werden?
- 12.6.7 Sind Tokens, die für die Authentifikation gebraucht werden auch Teil der Inventare?  
Schlüssel, Smart Cards, Hardware Sicherheitstoken

## 13 Zugang zu der Verarbeitung personenbezogener Daten

### 13.1 Logging Mechanismus

**Die Evaluation muss die Frage einschließen, ob genügend Aufzeichnungsmechanismen eingerichtet sind.**

- 13.1.3 Kann die Zugangsaufzeichnung soweit konfiguriert werden, dass Details wie "Zugang zum Schreiben", Zugang zum Einfügen" aufgenommen werden können?
- 13.1.4 Können die Aufbewahrungsfristen für LogDaten konfiguriert werden?
- 13.1.5 Werden verschiedene Protokolldaten gespeichert, so dass es für die Log-Dateien unterschiedliche Aufbewahrungsfristen geben muss?  
Beispiel: 2 Jahre für Zugangsdaten zu Personalsachen, 5 Jahre für Zugangsrechte im Allgemeinen
- 13.1.7 Können die Log-Dateien in Hinsicht auf definierte Ziele leicht ausgewertet werden?

### 13.2 Betrieb der Log-Dateien

**Weil Log-Dateien wie personenbezogenen Daten zu behandeln sind, muss die Evaluierung auch die Frage einschließen, ob die Verarbeitung von Log-Daten durch technische und organisatorische Maßnahmen gesichert ist.**

- 13.2.1 Sind die Sicherheitsmaßnahmen für die Speicherung von Log-Daten die Gleichen wie für personenbezogene Daten?
- 13.2.2 Können Rechte zum Lesen von Log-Daten an Nicht-Administratoren vergeben werden?
- 13.2.3 Kann die Aufbewahrungsfrist für Log-Daten konfiguriert werden?
- 13.2.4 Kann das Logging gesperrt oder abgeschaltet werden? Durch wen? Wir dies geloggt?
- 13.2.6 Werden die Log-Dateien regelmäßig vom Datenschutzbeauftragten und dem Sicherheitsbeauftragten gesichtet?

- 13.2.7 Werden die Log-Daten nach Ablauf der Aufbewahrungsfrist sicher gelöscht?
- 13.2.8 Kann das Logging gesperrt oder abgeschaltet werden? Durch wen? Wird es aufgezeichnet?

## 14 Sicherheit im Netzwerk und bei Übertragungen

Sicherheit im Netzwerk und bei Übertragungen betrifft die Sicherheit der IT-Infrastruktur und die Sicherheit der übermittelten und transportierten Daten, während der erste Aspekt gewöhnlich die gesamte Infrastruktur in den Vordergrund rückt, ist der zweite Aspekt eher Gegenstand für besondere Regelungen nach der Art der übermittelten Daten, des Empfängers usw.

### 14.1 Allgemein

- 14.1.1 Wird die Identität der Empfänger verifiziert?
- 14.1.2 Ist die Übertragung von Authorisierungsdaten gesichert?
- 14.1.3 Ist die Sicherheit beim Remote-Access auf Daten oder dem Unternehmensnetz vergleichbar mit dem internen Zugang?
- 14.1.4 Werden Übertragungen über öffentliche Netze verschlüsselt?
- 14.1.5 Wenn es eine Verbindung zwischen dem internen und dem externen Netzwerk gibt, gibt es eine Sicherheitseinrichtung?
- 14.1.6 Wenn ja: Trennen die Firewall-Regeln die Netze hinreichend?
- 14.1.7 Ist das interne Netzwerk gegen Malware, das durch externe Verbindungen übertragen werden könnte, gesichert?

## 15 Methoden zur Vermeidung von unbeabsichtigtem Verlust von Daten; Methoden zur Datensicherung und Datenwiederherstellung

### 15.1 Allgemeine Maßnahmen

- 15.1.1 Werden angemessene Zugangskontrollmechanismen gebraucht, um zu verhindern, dass unbefugtes Löschen, Manipulieren von Daten oder Programmen vorkommt?
- 15.1.2 Werden angemessene Zugangskontrollmechanismen gebraucht, um zu verhindern, dass unbefugte Unterbrechungen von Strom oder Netzwerkverbindungen oder unbefugtes Deaktivieren von IT-Systemen vorkommt?
- 15.1.3 Welche Maßnahmen wurden ergriffen gegen Feuer, Wasser und starke elektromagnetische Felder?
- 15.1.4 Welche Maßnahmen wurden ergriffen zum Schutz gegen Stromausfall?

### 15.2 Back-up-Mechanismus

- 15.2.1 Bietet das System automatische Back-up-Mechanismen?
- 15.2.2 Können die Back-up-Häufigkeiten konfiguriert werden?
- 15.2.3 Schließt das Back-up die Konfigurationsdaten ein?
- 15.2.4 Können Back-ups nur von autorisiertem Personal angelegt werden?
- 15.2.5 Sind die Back-up-Daten verschlüsselt?
- 15.2.6 Liefert das System Mittel zum Testen einer einwandfreien Back-up-Prozedur?
- 15.2.7 Wie behandelt das System die Löschungen von Daten in den Back-up-Dateien?

## 15.3 Back-up-Speicherung

- 15.3.1 Bietet das System verschiedene Speichereinrichtungen für Back-up-Daten?
- 15.3.2 Sind die Back-up-Daten gegen unautorisierten Zugang gesichert?
- 15.3.3 Werden die Back-up Dateien sicher gelagert?
- 15.3.4 Werden die Back-up Dateien gegen unautorisierten Zugriff gesichert?

## 15.4 Datenrettung

- 15.4.1 Hat das System eine Funktionalität, um Daten von back-ups ohne Re-Installation eines Programmes wiederherzustellen?
- 15.4.2 Hat das System eine Funktionalität, um Konfigurationen von back-ups ohne Reinstallation eines Programmes wiederherzustellen?
- 15.4.3 Ist der Weiderherstellungsprozess getestet worden?

## 16 Datenschutz und Sicherheitsmanagement

### 16.1 Sicherheitsregeln

16.1.1 Ist eine schriftliche Sicherheitspolicy erstellt worden und ist sie verfügbar?

16.1.2 Werden Sicherheitsziele vom Management wirksam weiterentwickelt?

### 16.2 Risiko-Analyse

16.2.1 Sind schriftliche Risikoanalysen verfügbar?

16.2.2 Wenn ja: Sind diese aussagekräftig?

### 16.3 Dokumentation von technischen und organisatorischen Schutzmaßnahmen

16.3.1 Enthält Software-Dokumentation des Unternehmens Informationen über implementierte Sicherheits- und Datenschutzmaßnahmen?

16.3.2 Ist eine detaillierte schriftliche Dokumentation der technischen und organisatorischen Maßnahmen verfügbar?

16.3.3 Sind Versionsgeschichten, Autoren und Angaben über Personen, die Programme und Systeme eingerichtet haben, verfügbar?

### 16.4 Dokumentation persönlicher Pflichten

16.4.1 Sind die Pflichten von am System beteiligten Mitarbeitern dokumentiert?

16.4.2 Ist diese Dokumentation leicht zugänglich?

### 16.5 Inventar von Hardware, Software, Daten und Speichermedien

16.5.1 Gibt es ein stets aktualisiertes Inventarverzeichnis, das alle Hardware, Software, Verfahren und Medien enthält?

Diese Dokumentation soll auch Informationen über Netzwerkverbindungen liefern.

16.5.2 Wenn ja: Ist dies hinreichend aussagekräftig und korrekt geführt?

## 16.6 Media Management

16.6.1 Erlauben die Speichermedien die Feststellung der Art von Informationen, die sie enthalten?

16.6.2 Werden sie verzeichnet und gelagert an einem Platz mit Zugangsrestriktionen auf autorisiertes Personal entsprechend dem Dokument für die Sicherheits-Policy?

16.6.3 Gibt es ein Verzeichnis der Speichermedien mit den entsprechenden technischen Daten und Aufgaben?

## 16.7 Bestellung und Pflichten von Datenschutzbeauftragten

16.7.1 Ist ein Datenschutzbeauftragter bestellt worden?

16.7.2 Liegen Bestelldokumente vor?

## 16.8 Ausbildung des Personals und Vertraulichkeit

16.8.1 Werden die Mitarbeiter regelmäßig über Datenschutz unterrichtet?

16.8.2 Wie wird die Unterrichtung ausgeführt?

16.8.3 Wird die Zeit und die Teilnahme solcher Unterrichtungen aufgezeichnet?

16.8.4 Wird die Erfüllung der Teilnahmepflicht schriftlich festgehalten? Hat eine Verletzung der Pflicht disziplinarische Maßnahmen zur Folge?

## 16.9 Datenschutz und Sicherheitsaudit

- 16.9.1 Werden Maßnahmen zur Datensicherheit bzw. zum Datenschutz regelmäßig auf ihre Wirksamkeit und Angemessenheit kontrolliert?
- 16.9.2 Gibt es darüber schriftliche Berichte?

## 16.10 Incident Management

- 16.10.1 Wie werden Zwischenfälle behandelt?
- 16.10.2 Sind schriftliche Pläne verfügbar, die wichtige Handlungen und Prozeduren darlegen, die im Falle eines Zwischenfalls verfolgt werden müssen? Ist darin klargelegt, welches Personal in seinen entsprechenden Rollen verantwortlich ist?
- 16.10.3 Werden Aufzeichnungen vorgenommen über Zwischenfälle und die Wiederherstellungsverfahren, die dem Zwischenfall folgen?
- 16.10.4 Wenn ja: Sind diese Aufzeichnungen verfügbar?
- 16.10.5 Wie geht man mit Sicherheitslücken um?

## 16.11 Test und Release

- 16.11.1 Werden Prozeduren und Software in einer formalen Prozedur freigegeben?
- 16.11.2 Werden Tests zuvor durchgeführt?
- 16.11.3 Werden Testdaten verwendet?
- 16.11.4 Sind diese Tests dokumentiert?

## 17 Besondere Techniken

### 17.1 Daten Löschen und Entfernen

**Personenbezogene Daten müssen gelöscht werden, wenn sie nicht mehr benötigt werden. Dies ist sowohl für einzelne Fälle wichtig als auch hinsichtlich der Disposition von Hardware, Software und Speichermedien.**

- 17.1.1 Kann ein Löschen dokumentiert werden in einer Weise, dass die gelöschten Daten nicht mehr erkannt werden?
- 17.1.2 Bietet das System automatische Funktionalitäten zum Löschen nach Ablauf der Aufbewahrungsfrist?
- 17.1.3 Löscht das System Daten in einer Weise, dass sie nie mehr wiederhergestellt werden können?
- 17.1.4 Wenn ja: Ist die Löschmethode zuverlässig und wirksam?
- 17.1.5 Ist es erforderlich, Teile der Hardware zu entfernen und unbrauchbar zu machen, bevor sie entsorgt werden?
- 17.1.6 Werden Geräte und Datenträger physikalisch zerstört?
- 17.1.7 Wenn Geräte Dritter für die Verarbeitung personenbezogener Daten gebraucht werden, welche Maßnahmen mussten ergriffen werden, um sicherzustellen, dass keine personenbezogenen Daten auf den Geräten bei der Rückgabe verbleiben?
- 17.1.8 Werden Speichermedien vor der Entsorgung unbrauchbar gemacht oder zerstört?
- 17.1.9 Sind diese Dritten zuverlässig?
- 17.1.10 Wenn ja: Wenn Dienste Dritter dafür gebraucht werden, ist dies gesetzeskonform?
- 17.1.11 Wie wird dies festgestellt?

- 17.1.12 Sind die Methoden für eine physische Zerstörung zuverlässig und wirksam?

## 17.2 Temporary Files

**Wenn zeitlich befristete Dateien oder Daten angelegt werden, muss der Zugang zu diesen Daten in der gleichen Weise gesteuert werden wie der Zugang zu regulären Daten. Temporäre Daten müssen gelöscht werden, wenn sie nicht mehr benötigt werden.**

- 17.2.1 Produziert das System Temporary files?
- 17.2.2 Gibt es einen Zugang zu diesen Daten, die vom System gesteuert werden?
- 17.2.3 Werden Temporary files automatisch gelöscht?
- 17.2.4 Geschieht das auf eine sichere Art?
- 17.2.5 Gibt es eine automatische Prozedur, die warnt, wenn einige Temporary files nicht ordentlich gelöscht werden, die dann eine Möglichkeit zu einer verlässlichen Löschung bietet?

## 17.3 Dokumentation von Software

- 17.3.1 Liefert die Dokumentation leicht verstehbare Angaben über die zu verarbeiteten Daten, Funktionalitäten, Schnittstellen mit Dritten etc.?
- 17.3.2 Liefert die Dokumentation leicht verstehbare Angaben über die Abläufe, so dass die entsprechenden Konfigurationen für die Realisierung des Datenschutzes möglich sind?
- 17.3.3 Ist die Dokumentation von Administratoren und Usern handhabbar?  
  
Diese Frage bezieht sich auf den Inhalt des Datenschutzes und die Sicherheitsfunktionen, nicht aber zum allgemeinen Inhalt.
- 17.3.4 Reicht die Dokumentation aus, damit der Betreiber alle seine Pflichten erfüllen kann?

## 17.4 Verschlüsselung

- 17.4.1 Sind die Verschlüsselungen wirksam?
- 17.4.2 Wie werden die Verschlüsselungs-Keys gehandhabt?
- 17.4.3 Was geschieht, wenn ein Schlüssel verloren geht?
- 17.4.4 Werden Schlüssel auf sichere Weise übergeben?

## 17.5 Pseudonymisierung und Anonymisierung

- 17.5.1 Wird eine Pseudonymisierung oder Anonymisierung durchgeführt?
- 17.5.2 Wenn ja: Bietet diese hinreichend Schutz gegen eine Re-Identifizierung?

## 17.6 Sicherung von Transparenz und automatische Entscheidungen

- 17.6.1 Bezieht das System automatisierte Einzelentscheidungen ein, die erkennbar die Betroffenen berührt?
- 17.6.2 Werden die Betroffenen darüber informiert? Wenn ja, durch die datenverarbeitende Stelle, automatisch oder auf Anfrage?
- 17.6.3 Wird der Betroffene über die Angelegenheit, um die es geht, informiert?
- 17.6.4 Kann der Betroffene diese Entscheidung anfechten?
- 17.6.5 Wenn ja: Durch die datenverarbeitende Stelle, automatisch oder nur auf Anfrage?
- 17.6.6 Wenn ja: Wird die Angelegenheit dann von einer natürlichen Person bearbeitet und zur Entscheidung gebracht?

- 17.6.7 Welche datentechnische Verfahren werden bei solchen Einzelentscheidungen genutzt?
- 17.6.8 Ist eine Vorprüfung durch den Datenschutzbeauftragten erforderlich?
- 17.6.9 Wenn ja: Ist sie angefordert und durchgeführt worden?