

**Anforderungskatalog v 2.0 für die Begutachtung
von IT-Produkten im Rahmen des Gütesiegelverfahrens
beim ULD SH**



Anforderungskatalog v 2.0

Stand: 28.11.2014*

Nach § 4 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG) i. V. m. § 1 Abs. 1 Datenschutzgütesiegelverordnung (DSGSVO) wird ein informationstechnisches Produkt (IT-Produkt) auf Antrag des Herstellers oder der Vertriebsorganisation vom Unabhängigen Landeszentrum für Datenschutz zertifiziert, wenn das IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht. IT-Produkte im Sinne der Verordnung sind Hardware, Software, automatisierte Verfahren und IT-basierte Dienstleistungen, die zur Nutzung durch öffentliche Stellen (u. a. in Schleswig-Holstein) geeignet sind.

Der Anforderungskatalog stellt beispielhaft Datenschutz- und Datensicherheitsanforderungen sowie in ihrem Zusammenhang zu berücksichtigende Fragestellungen in Bezug auf wichtige Rechtsnormen dar. Er gibt eine Mustergliederung für das Abarbeiten von Anforderungen jeweils nach Datenart vor (siehe Prüfschema). Eine reine Prüfcheckliste kommt nicht in Betracht, da sich die Anforderungsprofile und Datenarten pro zu prüfendem IT-Produkt unterscheiden und außerdem die Sachverständigen ihre Bewertungen stets begründen müssen.

Insbesondere sind unterschiedliche Kriterien anzuwenden je nachdem, ob es sich um

1. IT-Produkte, die die einsetzenden Stellen eigenständig betreiben (in erster Linie Hard- und Software), oder
2. IT-Produkte, die Dritte im Auftrag der verantwortlichen Stellen betreiben (in erster Linie Verfahren und Dienstleistungen),

handelt.

So werden im ersten Fall in der Regel einige Aspekte der Nutzung, etwa die konkrete Formulierung von Einwilligungserklärungen oder die konkrete Konfiguration der Zugriffsrechte, erst beim Einsatz durch die einsetzende Stelle festgelegt. Diese Aspekte können daher im Vorfeld nur abstrakt geprüft werden, nämlich in Hinblick auf die Fragen, ob das IT-Produkt hinreichende Funktionalität beinhaltet, entsprechende Hinweise für einen datenschutzgerechten Einsatz in der Dokumentation gegeben und ggf. Mustertexte, beispielsweise für Einwilligungen oder Datenschutzerklärungen, bereitgehalten werden.

Im zweiten Fall hingegen besteht schon eine konkrete Implementierung durch den Anbieter bzw. den Auftragnehmer, die geprüft werden muss. Daneben sind vertragliche Aspekte zwischen öffentlicher Stelle und Auftragnehmer, etwa der Leistungskatalog bzw. die Ausgestaltung eines Auftragsdatenverarbeitungsvertrags, zu prüfen. Ggf. ist die Bereitstellung eines Mustervertrags erforderlich.

Schließlich sind Mischformen möglich, etwa die Bereitstellung von Datenverarbeitungskapazitäten oder einer Software (sog. Providing, z. B. Hosting, Infrastructure as a Service, Platform as a Service, Software as a Service). In diesem Fall sind sowohl Aspekte der angebotenen Funktionalität (z. B. Softwarefunktionalität) als auch Aspekte der konkreten Implementierung beim Dienstleister (z. B. Umfang und

***Historie:** V 1.0 (01.02.2002): Erstellung // V 1.0a (24.04.2002): Korrektur von Druckfehlern und eines Layoutfehlers in Abschnitt 3.1.1.4 // V 1.1 (04.03.2003): Korrekturen und geringfügige Ergänzungen in den Abschnitten 1.1 // V 1.2 (29.08.2005): Änderung der Gliederung des Komplex 2 und Ergänzung von Fragen, Ergänzungen für Abruf- und Gemeinsame Verfahren, Einfügung eines Anforderungsprofils für Protokolldaten (Anforderungsprofil B) // V2.0 (28.11.2014): Aktualisierung Gesetzesbezüge, Einbindung der Datenschutz-Schutzziele, Anpassungen der Struktur

Durchführung der Datensicherung) zu untersuchen. Sofern unterschiedliche Fragestellungen in Hinblick auf die Funktionalität eines IT-Produkts einerseits und Betriebsaspekten der Dienstleistung andererseits identifiziert werden können, sollen diese getrennt dargestellt werden.

Pro Fragestellung ist zu untersuchen,

- ob sie jeweils relevant für das IT-Produkt ist,
- ob das IT-Produkt zur Erfüllung der Datenschutzanforderung beiträgt, diese erschwert oder den Punkt unberührt lässt,
- ob eine Realisierung gemäß dem Stand der Technik erfolgt,
- die Erfüllung der Anforderungen keinen erheblichen Aufwand für die einsetzende Stelle erfordert,
- welche Standardeinstellung ausgeliefert wird bzw. voreingestellt ist,
- welche Konfigurationsmöglichkeiten oder anderen Freiheitsgrade bestehen,
- wie all dies dokumentiert ist und
- inwieweit die Anforderungen nutzeradäquat umgesetzt sind.

Die Relevanz der Fragestellungen wird sich insbesondere darin unterscheiden, ob es sich um spezielle Verwaltungsverfahren und darauf zugeschnittene IT-Produkte handelt oder ob es universeller einsetzbare IT-Produkte sind. Weitere Unterschiede in der Relevanz der Fragestellungen liegen darin, ob ein IT-Produkt in der Zukunft durch den Kunden betrieben werden wird (in erster Linie Hard- und Software) oder ob bereits zum Zeitpunkt der Untersuchung ein Betrieb erfolgt (etwa bei Verfahren und Dienstleistungen, die durch einen Anbieter erbracht werden).

Dieser Text stellt im **Komplex 1** zunächst Anforderungen an die Technikgestaltung dar. Dies betrifft insbesondere Anforderungen der Datenvermeidung und der Transparenz.

Komplex 2 zählt die einschlägigen Datenschutzbestimmungen auf, um die Zulässigkeit der angestrebten Datenverarbeitung überprüfen zu können.

In **Komplex 3** wird untersucht, welche technisch-organisatorischen Maßnahmen zum Schutz der Betroffenen das IT-Produkt unterstützt. Diese Maßnahmen leiten sich in erster Linie aus der Datenschutzverordnung (DSVO) ab.

Komplex 4 stellt Kriterien vor, um die Umsetzung der Rechte der Betroffenen (z. B. Benachrichtigung, Auskunft, Transparenzgebote) beurteilen zu können.

Alle Komplexe müssen gleichermaßen bei der Prüfung des IT-Produkts berücksichtigt werden.

A. Allgemeines Anforderungsprofil	9
Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten	9
1 Grundsätzliche technische Ausgestaltung von IT-Produkten	9
1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit	9
1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung)	9
1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung)	10
1.4 Datenschutz-Schutzziel: Intervenierbarkeit	11
1.5 Anpassung des IT-Produkts	12
1.6 Privacy by Default	12
1.7 Sonstige Anforderungen	13
2 Zulässigkeit der Datenverarbeitung	14
2.1 Ermächtigungsgrundlage für die Verarbeitung von Daten (für jede Phase der Datenverarbeitung gesondert zu betrachten)	14
2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten	14
2.1.2 Einwilligung des Betroffenen	14
2.1.3 Besonderheiten in den einzelnen Phasen der Datenverarbeitung	15
2.1.3.1 Vorschriften über die Datenerhebung	15
2.1.3.2 Vorschriften über die Übermittlung	15
2.1.3.3 Löschung nach Wegfall des Erfordernisses	16
2.2 Einhaltung allgemeiner datenschutzrechtlicher Grundsätze und Pflichten	16
2.2.1 Zweckbindung und Zweckänderung	16
2.2.2 Erleichterung der Umsetzung des Trennungsgebotes	17
2.2.3 Gewährleistung der Datensicherheit (§§ 5, 6 LDSG, Anlage zu § 9 BDSG)	17
2.3 Datenverarbeitung im Auftrag	17
2.4 Voraussetzungen besonderer technischer Verfahren	18
2.4.1 Gemeinsame Verfahren / Abrufverfahren	18
2.4.2 Trennung der Verantwortlichkeiten	19
2.4.3 Veröffentlichungen im Internet	19
2.4.4 Weitere besondere technische Verfahren	20
2.5 Sonstige Anforderungen	20
2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	20
3 Technisch-organisatorische Maßnahmen	21
3.1 Einzelne technisch-organisatorische Maßnahmen	21
3.1.1 Physikalische Sicherung	21
3.1.2 Authentisierung	22
3.1.3 Autorisierung	23
3.1.4 Protokollierung	24
3.1.5 Verschlüsselung und Signatur	25
3.1.6 Pseudonymisieren	26
3.1.7 Anonymisieren	26

3.2	Allgemeine Pflichten	27
3.2.1	Technisch-organisatorische Maßnahmen	27
3.2.1.1	Verfügbarkeit	27
3.2.1.2	Integrität	28
3.2.1.3	Vertraulichkeit	29
3.2.1.4	Nicht-Verkettbarkeit	30
3.2.1.5	Transparenz	31
3.2.1.6	Intervenierbarkeit	32
3.2.1.7	Protokollierung von Datenverarbeitungsvorgängen	33
3.2.1.8	Test und Freigabe	33
3.2.2	Erleichterung der Vorabkontrolle	33
3.2.3	Erleichterung bei der Erstellung des Verfahrenszeichnisses	34
3.2.4	Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten	34
3.2.5	Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten	35
3.3	Spezifische Pflichten	35
3.3.1	Verschlüsselung	35
3.3.2	Anonymisierung oder Pseudonymisierung	36
3.3.3	Technische Umsetzung von speziellen Anforderungen bei besonderem Technikeinsatz	36
3.3.3.1	Mobile Datenverarbeitungssysteme	36
3.3.3.2	Video-Überwachung und –Aufzeichnung	37
3.3.3.3	Automatisierte Einzelentscheidungen	37
3.3.3.4	Veröffentlichungen im Internet	37
3.4	Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren	38
3.5	Anforderungen an den Betrieb bei Auftragsdatenverarbeitung	38
3.6	Sonstige Anforderungen	39
4	Komplex 4: Rechte der Betroffenen	40
4.1	Aufklärung und Benachrichtigung	40
4.2	Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten	40
4.3	Auskunft	40
4.4	Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung)	41
4.4.1	Berichtigung	41
4.4.2	Vollständige Löschung	41
4.4.3	Sperrung	41
4.4.4	Einwand bzw. Widerspruch gegen die Verarbeitung	42
4.4.5	Gegendarstellung	42
4.5	Sonstige Anforderungen	42
B. Anforderungsprofil für Protokolldaten		43

A Allgemeines Anforderungsprofil

Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten 9

In diesem Komplex werden allgemeine und übergreifende Anforderungen an die Technikgestaltung bearbeitet. Dies betrifft insbesondere Anforderungen der Datenvermeidung und der Transparenz.

Komplex 2: Zulässigkeit der Datenverarbeitung 14

Die Frage der Zulässigkeit einer Datenverarbeitung beurteilt sich danach, welches Recht auf die Stellen anzuwenden ist, für die das IT-Produkt vorgesehen ist. Bei Stellen des Landes Schleswig-Holstein ist dies grds. das LDSG (in Verbindung mit der DSVO), bei Wettbewerbsunternehmen u. U. das BDSG (§ 3 Abs. 2 LDSG). Bei Sozialleistungsträgern gilt in der Regel das SGB. Daneben sind sämtliche speziellen bereichsspezifischen Regelungen zu beachten. Beispielhaft (aber nicht abschließend) seien hier genannt:

als Bundesrecht

- §§ 75 ff. Ausländergesetz,
- Bundesstatistikgesetz,
- Kunsturhebergesetz,
- Personenstandsgesetz,
- Pass- und Personalausweisgesetz,
- Strafgesetzbuch (insb. § 203),
- Strafprozessordnung,
- §§ 185 ff. Strafvollzugsgesetz,
- Straßenverkehrsgesetz,
- Telemediengesetz,
- Telekommunikationsgesetz

oder als Landesrecht

- § 45 Hochschulgesetz,
- Rundfunkstaatsvertrag,
- Landesmeldegesetz,
- Landesarchivgesetz,
- §§ 85 ff. Landesbeamtengesetz,
- Landesstatistikgesetz,
- Landesverwaltungsgesetz, insb. §§ 177 ff. (Polizei),
- § 4 Landespressegesetz,
- §§ 30 f. Schulgesetz,
- Datenschutzverordnung Schule.

Weiterhin sind die von den Datenschutzbeauftragten des Bundes und der Länder bzw. den Aufsichtsbehörden für den Datenschutz herausgegebenen gemeinsamen Materialien zu Einzelaspekten des Datenschutzes zu beachten. Dies können sog. Orientierungshilfen, Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie Beschlüsse des Düsseldorfer Kreises (des Zusammenschlusses der Aufsichtsbehörden) sein. Auch Dokumente von anerkannten EU-Datenschutzgremien (z. B. Artikel 29-Datenschutzgruppe) sollen zur Auslegung herangezogen werden.

Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen

21

In Komplex 3 werden für Datenschutzanforderungen, die sich bei zulässiger Datenverarbeitung im Wesentlichen aus den Katalogen nach BDSG und LDSG/DSVO über technische und organisatorische Maßnahmen ergeben, beispielhaft (technische) Maßnahmen diskutiert, die zur Umsetzung dieser Anforderungen führen können. Dabei wird auch der Grad der technischen Umsetzung dieser Maßnahmen mit Beachtung der jeweiligen Schutzziele (vgl. § 5 LDSG) durch das IT-Produkt problematisiert. Beachtet werden muss bei der Bewertung, welches Angreifermodell den getroffenen/zutreffenden Maßnahmen zugrunde liegt, gegen welche Angriffe Schutzmaßnahmen vom IT-Produkt selbst vorgesehen sind, welche zusätzlichen Maßnahmen unterstützt werden (bzw. ob es dabei Einschränkungen gibt) und schließlich, welche Restrisiken verbleiben.

Ebenso wie in Komplex 2 sind spezialgesetzliche Vorschriften sowie die Vorgaben in Orientierungshilfen, Beschlüssen und Entschließungen der Datenschutzbeauftragten bzw. Aufsichtsbehörden zu berücksichtigen.

Komplex 4: Rechte der Betroffenen

40

Die Gewährleistung der Betroffenenrechte wird heutzutage vielfach auf organisatorischer Ebene abgedeckt. Beim zu zertifizierenden IT-Produkt ist entscheidend, inwieweit dort technisch

- die Wahrnehmung der Rechte direkt durch die Betroffenen ermöglicht oder sogar gefördert sowie
- die organisatorische Ebene beim Betreiber zur Gewährleistung der Betroffenenrechte unterstützt wird.

Es sind jeweils zusätzlich sowohl die Aspekte der Datensparsamkeit (z. B. ob eine Abwicklung anonym oder unter Pseudonym möglich ist) als auch der Protokollierung der Wahrnehmung der Betroffenenrechte zu berücksichtigen.

B. Anforderungsprofil für Protokolldaten

43

Bewertung

Es ist zu beachten, dass innerhalb eines IT-Produkts verschiedene Datenarten verarbeitet und zwischen einzelnen Komponenten ausgetauscht werden. Beispielhaft seien hier *Betroffenendaten* (häufig auch als *Primärdaten* bezeichnet), z.B. Daten über Einwohner in einem Einwohnermeldeamt, und *Sekundärdaten*, z. B. Protokolldaten über Dateneingaben und Datenbankzugriffe, über Konfigurationsänderungen oder über das Betreten von Zutrittsgeschützten Räumen wie ein Rechenzentrum, genannt.

Für jede dieser Datenarten sind ggf. nur Teile des Anforderungskatalogs relevant. Durch mehrfaches Überprüfen des Katalogs (einmal für jede Datenart) müssen die entsprechenden Anforderungen gefunden und die Umsetzung durch das IT-Produkt bewertet werden.

A. Allgemeines Anforderungsprofil

Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten

1 Grundsätzliche technische Ausgestaltung von IT-Produkten

In diesem Komplex werden grundlegende Anforderungen an die Gestaltung eines IT-Produkts genannt. Bei der Begutachtung sind diese in Hinblick auf die technische Ausgestaltung des Produkts zu überprüfen und überblicksartig darzustellen. Eine Detailprüfung, beispielsweise die genaue Prüfung der Erforderlichkeit einzelner personenbezogener Daten, der technischen Ausgestaltung der Protokollierung oder der Funktionalität zur Umsetzung von Betroffenenrechten, erfolgt in den Komplexen 2 bis 4.

1.1 IT-Sicherheits-Schutzziele¹: Verfügbarkeit, Integrität, Vertraulichkeit

Untersuchungsgegenstand:

Ist sichergestellt, dass Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verwendet werden können (Verfügbarkeit)? Bleiben Daten unversehrt, vollständig, zurechenbar und aktuell (Integrität)? Kann nur befugt auf Verfahren und Daten zugegriffen werden (Vertraulichkeit)?

1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung)

Untersuchungsgegenstand:

Wurden die Anforderungen der Datenvermeidung und der Datensparsamkeit umgesetzt? Gibt es Methoden für frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren personenbezogener Daten, um eine Verkettbarkeit der Daten zu verhindern? Werden Zweckbindungen und Zwecktrennungen umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:

- Können personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden?
- Ist ein vollständiger Verzicht auf personenbezogene Daten möglich? Wenn nein, warum nicht?
- Welche (Kombinationen von) personenbezogenen Daten sind im Rahmen des Einsatzzwecks des IT-Produkts erforderlich? Wovon hängt dies ab?
- Ist für den Fall, dass Daten verarbeitet werden, die nicht personenbezogen sein sollen oder nicht personenbezogen ausgewertet werden sollen (z. B. technische Identifikatoren, Server-Logs), ein Personenbezug dieser Daten tatsächlich

¹ Anstelle des Begriffs „Schutzziel“ wird auch „Gewährleistungsziel“ verwendet.

auszuschließen?

- Können Betroffene das IT-Produkt anonym oder unter Pseudonym nutzen? Gilt dieses gegenüber dem Anbieter des IT-Produkts und / oder weiteren Nutzern?
- Kann auf die Verwendung von personenbezogenen Daten nicht verzichtet werden, ist häufig in späteren Verarbeitungsphasen oder bei späteren Nutzungen (z. B. statistischen Auswertungen) eine anonyme oder pseudonyme Nutzung möglich. Ist dies beim vorliegenden IT-Produkt der Fall, z. B. durch Aggregation der personenbezogenen Daten?
- Eine Anonymisierung ist der Pseudonymisierung vorzuziehen. Bei der Anonymisierung ist zu prüfen, ob eine Identifizierung auch mit Zusatzwissen im Rahmen des Möglichen ausgeschlossen werden kann. Ist dies der Fall?
- Liegt eine Pseudonymisierung vor, so ist zu prüfen, wer Zugriff auf die Zuordnungsfunktion hat. Insbesondere bei der Verwendung von pseudonymisierten Profilen ist außerdem zu prüfen, ob durch Anreicherungen des Profils über die Zeit oder durch zusätzliche Informationen der Betroffene auch ohne Kenntnis der Zuordnungsfunktion identifiziert werden könnte. Ist dies der Fall?
- Wird die Anonymisierung / Pseudonymisierung zum frühestmöglichen Zeitpunkt vorgenommen?
- Wovon hängt der Zeitpunkt der Anonymisierung oder Pseudonymisierung ab?
- Welche Mechanismen kommen zum Einsatz, um zweckfremde Datenerhebungen, -verarbeitungen und -nutzungen zu unterbinden? Sind Zweckänderungen vorgesehen?
- Wie werden Anonymisierung und Pseudonymisierung umgesetzt (automatisch / in welchen Abhängigkeiten)?
- Für den Fall, dass unter bestimmten Bedingungen eine Aufdeckung eines Pseudonyms ermöglicht wird (etwa auf gerichtliche Anordnung): Wie ist dies umgesetzt (unter welchen Bedingungen, wie wird dies überprüft, mit Hilfe welcher Parteien wird der Personenbezug hergestellt, sind zusätzliche Personen betroffen, wie erfolgt die Information der Betroffenen) und existiert hierzu eine schriftliche Prozessbeschreibung?
- Wie wird das Löschen umgesetzt (automatisch, in welchen Abhängigkeiten)? Zu technischen Fragen des Löschens siehe auch Abschnitt 4.3.2.
- Wird auf das Anlegen von temporären Datenbeständen (z. B. unnötige Protokollierung, Parallel- und Zwischenspeicherung) verzichtet? Falls temporäre Datenbestände entstehen: Sind diese Datenbestände wirksam gegen unbefugte Zugriffe gesichert? Wie und wann werden sie gelöscht?
- Verzichtet der Empfänger von Daten freiwillig bzw. auf Grundlage seiner veröffentlichten Informations- / Datenschutzpolicy auf die Speicherung und Auswertung der von ihm übermittelten (Teil-)Informationen, die für den Verarbeitungszweck nicht erforderlich sind? Erfolgt eine Filterung auf Empfängerseite für „zu viel“ übermittelte Daten?

1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung)

Untersuchungsgegenstand:

Liegt eine aussagekräftige und aktuelle Produktbeschreibung vor, aufgrund derer die einsetzende Stelle verantwortungsvoll über die Auswahl, Konfiguration und Nutzung

entscheiden kann? Ist die Darstellung der Funktionsweise des IT-Produkts während der Nutzung verständlich und nachvollziehbar? Sämtliche Transparenzaspekte sind sowohl gegenüber dem Betroffenen der Datenverarbeitung als auch der einsetzenden Stelle zu prüfen.

In diesem Zusammenhang wichtige Fragestellungen:

- Ist die Transparenz der Datenverarbeitung (Datenflüsse, Speicherungsorte, Übermittlungswege, Zugriffsmöglichkeiten) gegenüber
 - Anwendern (Systemadministration und Nutzern) sowie
 - Betroffenengewährleistet?
- Sind die gemachten Angaben für alle Zielgruppen verständlich?
- Sind die Vorkenntnisse, die zum Verstehen der Produktbeschreibung erforderlich sind (Sprache, Know-how), angemessen?
- Inwieweit sind ein leichter Zugriff auf die Produktbeschreibung und eine geeignete Auswertbarkeit gewährleistet (Inhaltsverzeichnis, Index, Volltextsuche)?
- Wird die Aktualität sichergestellt?
- Wird das zugrundeliegende Konzept der Datenverarbeitung ausreichend erläutert?
- Besteht eine Einsichtsmöglichkeit in den Quelltext / das Gerät? Für wen (auch für Außenstehende oder nur für die Sachverständigen im Gütesiegel-Verfahren oder für andere externe Auditoren)?

1.4 Datenschutz-Schutzziel: Intervenierbarkeit

Untersuchungsgegenstand:

Ist das IT-Produkt so gestaltet, dass in die Datenverarbeitung leicht eingegriffen werden kann, die einsetzende Stelle als „Herrin des Verfahrens und der Daten“ tatsächlich in die Datenverarbeitung eingreifen kann und dass die Wahrnehmung von Betroffenenrechten leicht möglich ist?

In diesem Zusammenhang wichtige Fragestellungen:

- Sind Eingriffsmöglichkeiten (etwa die Deaktivierung einzelner Nutzerkonten, die Löschung oder Sperrung von Daten Betroffener, die Deaktivierung einzelner Verarbeitungsschritte oder Programmmodule, das Unterbrechen der Datenverarbeitung) vorhanden und leicht umzusetzen? Ist klar definiert, unter welchen Umständen ein Eingriff möglich oder vorgesehen ist und welche Konsequenzen dies hat?
- Können Betroffene selbst in die Datenverarbeitung eingreifen, wenn die Datenverarbeitung im Umfeld von Betroffenen (etwa als App, RFID-Card etc.) betrieben wird oder eine Schnittstelle zum Betroffenen (etwa Webportal) existiert?
- Ist gewährleistet, dass die einsetzende Stelle „Herrin des Verfahrens und der Daten“ bleibt und die Möglichkeit hat, die Daten bei einem Anbieterwechsel mitzunehmen (Vermeidung eines sogenannten „Vendor Lock-In“, damit die Nutzung anderer IT-Produkte bzw. Dienste eine realistische Alternative bleibt)?
- Ist der Betreiber eines Diensts ausreichend gut für Nachfragen, Beschwerden oder die Wahrnehmung von Kontrollpflichten durch den Anwender bzw. von Betroffenenrechten erreichbar (Geeignetheit der Wege für die Erreichbarkeit aus

Sicht der Anwender und Betroffenen, Umfang, Sprache, Reaktionsgeschwindigkeit)? Wurden Rechtsstand bzw. Gerichtsstand im Sinne von Anwender und Betroffenen gewählt (z. B. um einen Zugriff auf den Betreiber eines Diensts zu ermöglichen)?

- Ist der Hersteller / Entwickler des IT-Produkts angemessen erreichbar, um ihm z. B. Informationen über Störungen bzw. Fehler zu melden? Wie wird diese Erreichbarkeit sichergestellt und Ansprechpartner den Betroffenen und / oder einsetzenden Stellen und / oder Auftragnehmern kommuniziert? Existieren hierzu schriftliche Prozessbeschreibungen?
- Ist im Rahmen eines Auftragsdatenverhältnisses der Auftragnehmer verpflichtet worden, den Auftraggeber über Datenschutzvorfälle zu unterrichten? Besteht beim Auftraggeber eine Kontaktstelle, die in angemessener Zeit entsprechende Meldungen des Auftragnehmers entgegennehmen kann? Wurde diese Kontaktstelle dem Auftragnehmer mitgeteilt?

1.5 Anpassung des IT-Produkts

Untersuchungsgegenstand:

Wird das IT-Produkt regelmäßig oder anlassbezogen an geänderte technische oder rechtliche Rahmenbedingungen angepasst?

In diesem Zusammenhang wichtige Fragestellungen:

- Wie überwacht der Hersteller / Betreiber regelmäßig Änderungen des Stands der Technik und veränderte rechtliche Rahmenbedingungen?
- Welche Maßnahmen sind durch den Hersteller vorgesehen, um das IT-Produkt bei geänderten technischen oder rechtlichen Rahmenbedingungen anzupassen?
- Welche Aktivitäten sind aufseiten der Betroffenen, der einsetzenden Stelle, ggf. des Auftraggebers oder Auftragnehmers erforderlich, um das IT-Produkt anzupassen?

1.6 Privacy by Default

Untersuchungsgegenstand:

Sind die Voreinstellungen maximal datenschutzfreundlich gewählt?

In diesem Zusammenhang wichtige Fragestellungen:

- Ist sinnvoll festgelegt, welche Funktionalität des IT-Produkts durch Nutzer bzw. einsetzende Stellen konfigurierbar ist und welche nicht?
- Gewährleistet die voreingestellte Konfiguration eine datenschutzgerechte Benutzung des IT-Produkts, oder sind dafür Änderungen notwendig?
- Für den Fall, dass die voreingestellte Konfiguration mit einer Einschränkung der Funktionalität verbunden ist: Ist eine sinnvolle Benutzung des IT-Produkts möglich? Steht dies im Einklang mit der Nutzererwartung? Ist bei Änderung der Konfiguration für eine Erweiterung der Funktionalität weiterhin eine datenschutzgerechte möglich?
- Auf welche Weise wird das IT-Produkt an die Bedürfnisse der Nutzer und der einsetzenden Stelle angepasst? Werden technische Standardkonfigurationen bzw. Standardabläufe und -verträge bei Dienstleistungen vorgegeben, die ggf. auf Initiative des Kunden geändert werden? Wenn ja: Sind die ausgelieferten technischen Konfigurationen bzw. angebotenen Abläufe maximal

datenschutzfreundlich?

- Wird das IT-Produkt in jedem Fall individualisiert eingerichtet bzw. angepasst (Customizing)? Wenn ja: Wie wird sichergestellt, dass datenschutzfreundliche und der speziellen (Datenschutz-)Situation des Kunden angepasste Konfigurationen bzw. Abläufe gewählt werden?

1.7 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit oder aus weiteren Datenschutzprinzipien ergeben?

Komplex 2: Zulässigkeit der Datenverarbeitung

2 Zulässigkeit der Datenverarbeitung

2.1 Ermächtigungsgrundlage für die Verarbeitung von Daten (für jede Phase der Datenverarbeitung gesondert zu betrachten)

2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten

Untersuchungsgegenstand:

Sind die Zulässigkeitsvoraussetzungen für die Datenverarbeitung erfüllt?

Rechtsgrundlagen:

§§ 11, 14-16 LDSG, §§ 28 ff. BDSG oder bereichsspezifisches Recht wie z. B. §§ 67a ff. SGB X

In diesem Zusammenhang wichtige Fragestellungen:

- Gibt es einen abgeschlossenen Katalog von Daten, die verarbeitet werden sollen?
 - Wenn ja: Wird die Erhebung und Speicherung auf diese Daten beschränkt (Vermeidung von Freitextfeldern)?
 - Wenn nein: Beschränken sich die Daten auf das Erforderliche?
- Erfolgt eine Verarbeitung besonders sensibler Daten (§ 67 Abs. 12 SGB X, § 3 Abs. 9 BDSG), die die Zulässigkeit einschränken könnte (§ 11 Abs. 3 LDSG, § 67a Abs. 1 S. 2, 67b Abs. 1 S. 2 SGB X, § 28 Abs. 6-9 BDSG)? Wie wird eine solche Einschränkung umgesetzt?
- Unterliegen die Daten zusätzlichen besonderen materiellen Anforderungen (z. B. berufliche Schweigepflicht, vgl. § 203 StGB), und wie werden diese bei der weiteren Verarbeitung berücksichtigt?
- Inwieweit sind Anonymisierungs- bzw. Pseudonymisierungsgebote (z. B. § 22 LDSG) zu beachten?

2.1.2 Einwilligung des Betroffenen

Untersuchungsgegenstand:

Wird die Wirksamkeit einer Einwilligung unterstützt?

Rechtsgrundlagen:

u. a. § 12 LDSG, § 67b Abs. 2, 3 SGB X, § 4a BDSG, § 13 Abs. 2 TMG, § 94 TKG

In diesem Zusammenhang wichtige Fragestellungen:

- Stellt das IT-Produkt eine Mustereinwilligungserklärung oder Hinweise zur Gestaltung der Einwilligungserklärung zur Verfügung? Ist die Formulierung einer vorgegebenen Einwilligungserklärung hinreichend bestimmt, d. h. enthält sie Angaben zu verarbeitenden Stellen, verarbeiteten Datenkategorien, den Phasen der Datenverarbeitung, insbesondere geplanten Übermittlungen und den Empfängern der Übermittlung, dem Zweck der Datenverarbeitung, einen Hinweis auf die Freiwilligkeit der Einwilligung sowie einen Hinweis auf die Widerrufbarkeit

der Einwilligung und sich daraus ergebende Konsequenzen?

- Ist die Einwilligungserklärung für die angesprochenen Zielgruppen (z. B. Jugendliche / IT-Laien) verständlich?
- Gibt es eine Beschränkung des Gültigkeitszeitraums von Einwilligungen?
- Sind die Formerfordernisse nach § 12 Abs. 3 LDSG (bzw. § 67b Abs. 2 SGB X, § 4a Abs. 1 S. 3, 4 BDSG) gewahrt?
- Kann die Einwilligung frei erklärt werden und ist nicht eine Leistung an die Erklärung der Einwilligung gekoppelt?
- Gibt es eine Unterstützung durch das IT-Produkt (dabei ist zu berücksichtigen, dass i. d. R. die Einwilligung vor der ersten Speicherung vorliegen muss)? Erfolgt das Einwilligungsmanagement IT-gestützt (Dokumentation der Einwilligung und ggf. des Widerrufs der Einwilligung)?

2.1.3 Besonderheiten in den einzelnen Phasen der Datenverarbeitung

2.1.3.1 Vorschriften über die Datenerhebung

Untersuchungsgegenstand:

Werden bestehende gesetzliche Regelungen bei der Erhebung von Daten umgesetzt?

Rechtsgrundlagen:

§ 13 Abs. 1 LDSG, § 67a Abs. 1 SGB X, § 28 Abs. 1 BDSG, vgl. § 13 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Welche Rechtsgrundlagen begründen die Zulässigkeit der Erhebung?
- Erfolgt eine Dokumentation über die Herkunft (§ 13 Abs. 1 S. 3 LDSG)?
- Erfolgt eine Unterrichtung bzw. Aufklärung des Betroffenen (§ 26 Abs. 1, 3 LDSG, § 67a Abs. 3, 5 SGB X) bzw. des Dritten (§ 67a Abs. 4 SGB X)? In welcher Form unterstützt das IT-Produkt dies?
- Erfolgt eine verdeckte Erhebung von Daten ohne Kenntnis des Betroffenen (z. B. bei biometrischen Verfahren)?

2.1.3.2 Vorschriften über die Übermittlung

Untersuchungsgegenstand:

Werden bestehende gesetzliche Regelungen bei der Übermittlung von Daten umgesetzt?

Rechtsgrundlagen:

§§ 8, 14-16 LDSG, §§ 67d-78 SGB X, §§ 28 ff. BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Welche Rechtsgrundlagen begründen die Zulässigkeit der Übermittlung?
- Erfolgt eine Protokollierung der Übermittlungen? Sind die datenschutzrechtlichen Vorschriften für die Protokolldaten erfüllt?
- Erfolgt ein Hinweis bzw. eine Verpflichtung auf die Zweckbindung der erhaltenen Daten (vgl. §§ 15 Abs. 2, 16 Abs. 4 LDSG, § 78 Abs. 2 SGB X, § 4b Abs. 6 BDSG)?

- Kann eine Zweckbindung technisch überwacht werden und können Daten, die nicht übermittelt werden dürfen, von der Übermittlung ausgeschlossen werden?
- Wird die Richtigkeit der Empfängeradresse verifiziert? Gibt es Filter für mögliche Adressaten bzw. Adressatenkreise, an die keinesfalls eine Übermittlung erfolgen darf (z. B. durch Sperrung von Empfängeradressen außerhalb des Hauses in einem E-Mail-System)?
- Filter für ausgehende Informationen: Gibt es Mechanismen, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten / Datenträgern zu verhindern oder zu erschweren, z. B. durch rückstandslose Beseitigung von personenbezogenen (Zusatz-)Daten bei möglicher Herausgabe (z. B. detaillierte Informationen über den Autor in Word-Dokumenten, automatisierte Weitergabe von Zusatzinformationen bei HTTP-Kommunikation durch Voreinstellungen im Webbrowser)?
- Gibt es Maßnahmen zur Steigerung der Sensibilität der Verarbeiter, um diese vor unbedachten / unerlaubten Übermittlungen zu schützen?
- Sind bei der Übermittlung an Dritte Maßnahmen vorgesehen, um Daten zu anonymisieren oder pseudonymisieren (§ 11 Abs. 6 LDSG) (siehe auch Abschnitte 1.2, 3.3.2)?

2.1.3.3 Löschung nach Wegfall des Erfordernisses

Untersuchungsgegenstand:

Wird sichergestellt, dass Daten nach Wegfall des Erfordernisses gelöscht werden oder ein Personenbezug abgetrennt wird?

Rechtsgrundlagen:

§ 28 Abs. 2 S. 2 LDSG, §§ 25, 35 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Sind Fristen (Löschungsfristen, Wiedervorlagefristen, Aufbewahrungsfristen, Archivierungspflichten) zu beachten? Wie wird deren Beachtung sichergestellt?
- Siehe auch Abschnitt 4.4.2 zur Löschung und Abschnitte 1.2 und 3.3.2 zur Anonymisierung/Pseudonymisierung.

2.2 Einhaltung allgemeiner datenschutzrechtlicher Grundsätze und Pflichten

2.2.1 Zweckbindung und Zweckänderung

Untersuchungsgegenstand:

Wie wird sichergestellt, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden bzw. dass eine Zweckänderung nur innerhalb des gesetzlichen Rahmens erfolgt?

Rechtsgrundlagen:

§ 13 Abs. 2 LDSG, § 67c Abs. 1 SGB X (Zweckbindung) und § 13 Abs. 3 LDSG, § 67c Abs. 2 SGB X, § 28 Abs. 2, 3 BDSG (Zweckänderung)

In diesem Zusammenhang wichtige Fragestellungen:

- Wie wird der Zweck dokumentiert, für den die personenbezogenen Daten erhoben werden?
- Gibt es eine reversionssichere Protokollierung der Verarbeitung, um Zweckänderungen nachweisen zu können?
- Wird die Zweckbindung dadurch garantiert, dass personenbezogene Daten vermieden werden oder ihre Verkettbarkeit und damit eine zweckändernde Nutzung verhindert oder eingeschränkt wird?
- Gibt es eine Kennzeichnung von Datensätzen mit entsprechenden Zwecken sowie das Durchsetzen von Zugriffsrechten, wodurch andere Auswertungsmethoden oder eine Übermittlung verhindert oder eingeschränkt werden?

2.2.2 Erleichterung der Umsetzung des Trennungsgebotes

Untersuchungsgegenstand:

Wird das Trennungsgebot unterstützt?

Rechtsgrundlage:

§ 11 Abs. 4 LDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Wie ist das Trennungsgebot technisch umgesetzt?
- Gibt es Verfahren zur automatisierten Anonymisierung/Pseudonymisierung (siehe auch Abschnitt 1.3)?
- Werden schutzwürdige Belange, die einer Weitergabe von untrennbar verbundenen Daten entgegenstehen, geprüft?

2.2.3 Gewährleistung der Datensicherheit (§§ 5, 6 LDSG, Anlage zu § 9 BDSG)

Untersuchungsgegenstand:

Werden die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit durch das IT-Produkt selbst ergriffen bzw. enthält das IT-Produkt Hinweise zur Umsetzung der erforderlichen Maßnahmen?

Prüfung im Komplex 3.

2.3 Datenverarbeitung im Auftrag

Untersuchungsgegenstand:

Erfolgt eine Datenverarbeitung im Auftrag bzw. ist eine solche vorgesehen? Sind die Voraussetzungen für eine Datenverarbeitung im Auftrag gegeben? Im Rahmen der Prüfung der Auftragsdatenverarbeitung (ADV) im Sinne des § 17 LDSG sind auch die im § 11 BDSG genannten Kriterien zur Konkretisierung hinzuzuziehen.

In diesem Zusammenhang sind zwei Arten der Auftragsdatenverarbeitung denkbar:

- eine Beauftragung eines Dienstleisters (in der Regel der Antragsteller) durch eine öffentliche Stelle,
- eine (Unter-)Beauftragung eines Dritten durch den Dienstleister (in der Regel der Antragsteller) im Rahmen der Erbringung der Dienstleistung (etwa Hosting der Server durch einen Unterauftragnehmer, die zur Dienstleistung durch den Antragsteller benötigt werden).

Im ersten Fall wird der zugrundeliegende ADV-Vertrag zukünftig durch die einsetzende Stelle geschlossen. In der Regel sind hierfür entsprechende Musterverträge durch den Antragsteller bereitzuhalten und durch die Sachverständigen zu überprüfen und zu bewerten.

Im zweiten Fall gibt es bereits ein konkretes Vertragsverhältnis zwischen Dienstleister und (Unter-)Auftragnehmer. Dieses ist durch die Sachverständigen bzgl. Auswahl und Ausgestaltung zu prüfen und zu bewerten. Außerdem ist zu belegen, dass der Auftraggeber seinen Prüfpflichten gegenüber dem Auftragnehmer nachgekommen ist. Sofern die Dienstleistung des Auftragnehmers zum Gütesiegelgegenstand gehört, ist auch diese durch die Sachverständigen zu untersuchen. Hierfür können zwar auch Unterlagen bzw. Testate von externen Prüfern herangezogen werden. In der Regel ist jedoch auch eine Vorortprüfung beim Auftragnehmer erforderlich.

Rechtsgrundlagen:

§ 17 LDSG, § 80 SGB X, § 11 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Ist eine Verarbeitung der Daten durch einen externen Dritten zulässig (vgl. dazu § 203 StGB, § 80 Abs. 5 SGB X)?
- Gibt es einen Vertrag oder einen Mustervertrag zur Datenverarbeitung im Auftrag?
- Entspricht der Vertrag den Anforderungen der einschlägigen Vorschriften (§ 17 Abs. 2 LDSG, § 80 SGB X, § 11 Abs. 2 BDSG)?
- Wie wird die Kontrolle des Auftragnehmers durch den Auftraggeber unterstützt?
- Wird die regelmäßige Kontrolle des (Unter-)Auftragnehmers durch den Auftraggeber dokumentiert?
- Wie wird das Recht des Auftraggebers, dem Auftragnehmer Weisungen zu erteilen, unterstützt?
- Wie sind die technischen und organisatorischen Maßnahmen umgesetzt, die die Bindung des Auftragnehmers an die Weisungen der einsetzenden Stelle sicherstellen?
- Wie werden die durch den Auftragnehmer getroffenen technisch-organisatorischen Maßnahmen beim Auftraggeber dokumentiert (§ 4 Abs. 7 DSGVO)?

2.4 Voraussetzungen besonderer technischer Verfahren

2.4.1 Gemeinsame Verfahren / Abrufverfahren

Untersuchungsgegenstand:

Werden Daten in einem gemeinsamen Verfahren oder einem automatisierten Abrufverfahren an Dritte übermittelt und sind die Voraussetzungen für die Einrichtung eines solchen Verfahrens erfüllt?

Rechtsgrundlagen:

§ 8 LDSG, § 79 SGB X, vgl. § 10 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Ist ein automatisiertes Abrufverfahren unter den Beteiligten zulässig (vgl.

insbesondere § 79 SGB X)?

- Inwieweit ist die Einrichtung des Verfahrens in Hinblick auf die schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen?
- Wie wird die Zuständigkeit der Verfahrensbeteiligten für einzelne Verfahrensteile festgelegt und die Kontrollierbarkeit der Zulässigkeit gewährleistet?
- Inwiefern sind Festlegungen von Fachaufsichtsbehörden zu Zwecken, Art der übermittelten Daten, Empfängern sowie technischen und organisatorischen Maßnahmen zu beachten (§ 10 Abs. 2 BDSG, § 79 Abs. 2 SGB X)?
- Inwiefern bestehen Unterrichtungspflichten von Aufsichtsbehörden (§ 10 Abs. 3 BDSG, § 79 Abs. 3 SGB X)?
- Wie sind die Protokollierungserfordernisse für Datenübermittlungen und Abrufe (z. B. § 8 Abs. 4, 5 LDSG, § 10 Abs. 4 BDSG, § 79 Abs. 4 SGB X) umgesetzt?

2.4.2 Trennung der Verantwortlichkeiten

Untersuchungsgegenstand:

Gibt es eine Trennung der Verantwortung für die Gewährleistung der Ordnungsmäßigkeit und der Verantwortung für die gespeicherten Daten bzw. ist eine solche Trennung vorgesehen?

Rechtsgrundlagen:

§ 8 Abs. 2 LDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Gibt es eine Rechtsgrundlage gemäß § 8 Abs. 2 LDSG für die Trennung der Verantwortlichkeiten?

2.4.3 Veröffentlichungen im Internet

Untersuchungsgegenstand:

Werden personenbezogene Daten im Internet veröffentlicht und liegt hierfür eine Rechtsgrundlage vor?

Rechtsgrundlage:

§ 21 LDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Erlaubt eine Rechtsvorschrift die Veröffentlichung oder hat der Betroffene hierin eingewilligt?
- Wurde der Betroffene im Fall der Einwilligung umfänglich über die Veröffentlichung der Daten aufgeklärt?
- Sollen Daten nach § 11 Abs. 2 LDSG oder Daten von Mandatsträger und öffentlich tätigen Personen im Rahmen eines Dienst- oder Arbeitsverhältnisses veröffentlicht werden?
- Wurde die Veröffentlichung befristet bzw. ein Datum für die Löschung bestimmt?
- Existieren Prozeduren / Verfahren, die eine Löschung der Daten bzw. Prüfung der Wiederholungsveröffentlichung sicherstellen?

2.4.4 Weitere besondere technische Verfahren

Untersuchungsgegenstand:

Wie wird die Beachtung zusätzlicher speziellen materiell-rechtlichen Anforderungen beim Einsatz besonderer technischer Verfahren sichergestellt?

In diesem Zusammenhang wichtige Fragestellungen:

Sind besondere Anforderungen einschlägig, z. B.

- Zulässigkeit von mobilen personenbezogenen Datenverarbeitungssystemen (§ 18 Abs. 1 LDSG, § 6c BDSG) – siehe auch Abschnitt 3.3.3.1 (mobile Datenverarbeitungssysteme),
- automatisierte Einzelentscheidungen (§ 19 LDSG, § 6a BDSG, § 67b Abs. 4 SGB X) – siehe auch Abschnitt 3.3.3.3 (automatisierte Einzelentscheidungen),
- Video-Überwachung und –Aufzeichnung (z. B. § 20 LDSG, § 6b BDSG) – siehe auch Abschnitt 3.3.3.2 (Videoüberwachung)?

2.5 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit oder aus weiteren Datenschutzprinzipien ergeben?

2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens

Untersuchungsgegenstand:

Wird eine gebotene oder geforderte Pseudonymisierung erleichtert oder unterstützt?

Rechtsgrundlagen:

§ 2 Abs. 2 Nr. 7 LDSG, § 67 Abs. 8a SGB X, § 3 Abs. 6a BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Ist eine Pseudonymisierung von Daten für Zwecke der Forschung (§ 22 Abs. 1 LDSG) geboten?
- Ist eine Pseudonymisierung von Daten im Rahmen der Datenverarbeitung und Übermittlung (§ 11 Abs. 6 LDSG) gefordert oder geboten?
- Siehe auch Abschnitt 3.1.6.

Komplex 3: Technisch-organisatorische Maßnahmen

Die rechtlichen Vorschriften für die zu ergreifenden technisch-organisatorischen Maßnahmen im LDSG wurden 2012 novelliert; neu ist dabei die Formulierung der Anforderungen in Form von Schutzziele, die bei der Verarbeitung personenbezogener Daten umzusetzen sind. Die in § 5 LDSG angesprochenen Schutzziele erfordern es u. a., befugte von unbefugten Datenverarbeitungen zu unterscheiden. Die in der Praxis dabei verwendeten Maßnahmen (z. B. Berechtigungskonzepte, Authentisierungsverfahren, Signaturen) können mittelbar der Umsetzung mehrerer Schutzziele dienen. Ebenso können einzelne Maßnahmen neben den abstrakten Anforderungen aus § 5 LDSG auch spezifische Anforderungen, beispielsweise aus §§ 6 und 8 LDSG, umsetzen.

Eine gutachterliche Prüfung, die sich in ihrer Struktur ausschließlich anhand der Schutzziele orientiert, kann zu unnötigen Doppelbeschreibungen auf Ebene der Maßnahmen führen. Im systematischen Aufbau eines Gutachtens können daher die Maßnahmen, die der Umsetzung mehrerer Schutzziele dienen, in einem vorangestellten Abschnitt beschrieben werden. Bei der detaillierten Prüfung von Schutzziele und spezifischen Anforderungen kann dann auf den vorangestellten Abschnitt verwiesen werden.

Prüfaspekte für Maßnahmen, die in einem vorangestellten Abschnitt des Gutachtens beschrieben werden können, sind in Abschnitt 3.1 enthalten. Dieser Abschnitt erhebt keinen Anspruch auf Vollständigkeit; ebenso dürften nicht alle in diesem Abschnitt angesprochenen Maßnahmen in allen Konstellationen relevant sein. Bei der Abfassung des Gutachtens sind die Sachverständigen frei, weitere Maßnahmen in den vorangestellten Abschnitt zu integrieren. Ebenso kann es erforderlich sein, bei komplexen Zertifizierungsgegenständen in dem vorangestellten Abschnitt Maßnahmen aus Abschnitt 3.1 mehrfach zu beschreiben: Besteht ein Zertifizierungsgegenstand beispielsweise aus der Bereitstellung und Betrieb einer Software durch einen Auftragnehmer (z. B. Software as a Service), so kommen typischerweise mehrere Rechte- und Rollenkonzepte zum Einsatz kommen, etwa für die Nutzer einer Anwendung (Auftraggeberseite) einerseits und die Administratoren der technischen Plattform (z. B. Datenbanken, Betriebssysteme) auf der Auftragnehmerseite andererseits.

Es empfiehlt sich, die Gliederung des Gutachtens an der Gliederung des Anforderungskatalogs auszurichten. Dabei kann der vorangestellte Abschnitt des Gutachtens, der übergreifende Datensicherheitsmaßnahmen beschreibt, in Gliederungspunkt 3.1 dargestellt werden.

3 Technisch-organisatorische Maßnahmen

3.1 Einzelne technisch-organisatorische Maßnahmen

3.1.1 Physikalische Sicherung

Untersuchungsgegenstand:

Wird durch geeignete Maßnahmen Unbefugten der Zutritt zu Datenverarbeitungsanlagen und Zugang zu Datenträgern verwehrt?

Rechtsgrundlagen:

Vgl. auch Anlage zu § 9 BDSG S. 1, Nr. 1 Zutrittskontrolle und Nr. 2 Zugangskontrolle

In diesem Zusammenhang wichtige Fragestellungen:

- Werden Zutritte protokolliert? Welchen datenschutzrechtlichen Regelungen unterliegen die entstehenden Protokolldaten?
- Unterliegen die Zutrittskontrollmechanismen ihrerseits datenschutzrechtlichen Regelungen (insb. bei Chipkarten, Token, biometrische Verfahren durch die Verarbeitung von Sekundärdaten)? Siehe dazu auch die Fragestellungen zu 3.1.2 und 3.1.3.
- Ist die Vergabe von Zutrittsrechten nachvollziehbar und revisions sicher dokumentiert?

3.1.2 Authentisierung

Um über die Befugnis eines Zugriffs auf Daten entscheiden zu können (Autorisierung, siehe Abschnitt 3.1.3), ist es u. a. entscheidend, die Identität oder die Rolle der zugreifenden Person oder des zugreifenden Systems festzustellen. Besonders datenschutzfreundlich sind Techniken, mit denen nur bestimmte Eigenschaften (wie Gruppenzugehörigkeiten) nachgewiesen werden (z. B. attributbasierte Credentials).

Untersuchungsgegenstand:

Werden Nutzer durch geeignete Maßnahmen authentisiert?

In diesem Zusammenhang wichtige Fragestellungen:

- Ist eine Identifizierung erforderlich oder ist eine Verifikation einer Gruppenzugehörigkeit (z. B. „Nutzer gehört zur Gruppe der über 18-Jährigen“), an die weitere Rechte (siehe 3.1.3) geknüpft sind, ausreichend?
- Gibt es eine Beschränkung des Gültigkeitszeitraums von Authentisierungsmechanismen?
- Wenn ein Passwortschutz zur Anwendung kommt: Ist er sicher umgesetzt, z. B. durch Einmalpasswörter (z. B. Challenge-Response), Schutz gegen Ausspähung oder Erraten, dauerhafte oder zeitlich befristete Sperrung bei Fehlversuchen, Vergabe/Wechsel durch Nutzer selbst, Prüfung der Länge, Prüfung von Komplexitätsanforderungen, Einschränkung der Wiederverwendbarkeit?
- Unterliegen die Authentisierungsmechanismen ihrerseits datenschutzrechtlichen Regelungen (insb. bei Chipkarten, Token, biometrische Verfahren durch die Verarbeitung von Sekundärdaten)?
- Werden die Authentisierungsdaten sicher gespeichert (z. B. salted Hashes bei Passwörtern, Zugriffsschutz bei Token und Chipkarten)?
- Gibt es Rücksetzungs- oder Fallback-Mechanismen für verloren gegangene oder vergessene Authentisierungsdaten? Sind diese sicher implementiert (z. B. zuverlässige Identifizierung desjenigen, dessen Authentisierungsdaten / -mechanismen verloren gegangen sind)? Wird auf ein Erheben von zusätzlichen personenbezogenen Daten, ggf. auch von Dritten, für solche Rücksetzungs- oder Fallback-Mechanismen verzichtet (z. B. „Geburtsname der Mutter“)?

- Werden Authentisierungsdaten eingesetzt, die eine Verkettung ermöglichen (z. B. gültige E-Mail-Adresse als Benutzername bei einer Benutzernamen / Passwort-Authentisierung)? Ist dies gewollt?

3.1.3 Autorisierung

Um über die Befugnis eines Zugriffs auf Daten, Systeme oder Verfahren (nachfolgend Objekte) entscheiden zu können (Autorisierung), ist es u. a. entscheidend, die Identität, Gruppenzugehörigkeit oder Rolle der zugreifenden Person oder des zugreifenden Systems festzustellen (siehe Abschnitt 3.1.2). Ein Berechtigungsmanagement ordnet Berechtigungen einzelnen Identitäten (z. B. Nutzerkonten), Gruppen oder Rollen zu.

In diesem Zusammenhang wichtige Fragestellungen:

- Ist der Detaillierungsgrad der zu vergebenden Berechtigungen ausreichend? Sind ggf. Rollenkonzepte (etwa besondere Berechtigungen von System- und Verfahrensadministration und Kontrollrollen wie Leitung, Datenschutzbeauftragter oder Revision) berücksichtigt?
- Produkt- und systemabhängig kann es mehrere Administrationsebenen geben, beispielsweise Administrationen auf Ebene des Betriebssystems, einer Datenbank, eines Dateisystems und der Anwendung selbst, die unmittelbaren Zugriff auf die verarbeiteten Daten erlauben. Werden Administrationsebene(n) und Anwendungsebene(n) ausreichend getrennt?
- Wie wird die Vergabe dieser Rechte dokumentiert (z. B. durch eine Protokolldatei, ein externes Tool)? Wer hat Zugriff auf die Dokumentation? Wie wird die Einhaltung der Aufbewahrungsfrist der Dokumentation sichergestellt (vgl. auch Abschnitt 3.3)?
- Wie kann die Dokumentation ausgewertet werden?
 - Nach Berechtigungen, die einzelne Personen, Rollen, Gruppen oder Systeme innehaben (Sicht der Zugreifenden: „Welche Zugriffe sind durch den Zugreifenden X auf welche Objekte möglich?“)
 - Nach Berechtigungen, die Zugriffe auf einzelne Objekte erlauben? (Sicht der Objekte: „Welche Personen, Rollen, Gruppen oder Systeme können auf das Objekt Y zugreifen?“)
 - Ist ggf. der Export der Berechtigungen oder der Einsatz eines zusätzlichen Tools erforderlich, um die Auswertungen in beide Richtungen vorzunehmen?

Für Hardware/Software:

- Wird die Vergabe von Berechtigungen innerhalb des IT-Produkts dokumentiert (z. B. durch eine Protokollierung oder eine chronologische Protokolldatei?) Ist ein externes Tool zur Protokollierung oder Auswertung der Protokolldatei erforderlich?
- Wie wird die Einhaltung der Aufbewahrungsfrist der Dokumentation sichergestellt? Gemäß § 3 Abs. 3 i. V. m. Abs. 2 Nr. 5 sind dies 5 Jahre nach der letzten Verarbeitung automatisierten Daten; die Dokumentation kann auch außerhalb des IT-Produkts erfolgen.

Für Dienstleistungen im Rahmen des IT-Produkts (Sicht des Auftraggebers):

- Insbesondere bei Mischformen wie der Bereitstellungen von Anwendungen (Application Providing) ist darzustellen, welche Administrationsaufgaben durch

den Auftraggeber bzw. durch den Auftragnehmer wahrgenommen werden sollen. Gleiches gilt bei getrennten Verantwortlichkeiten nach § 8 Abs. 2 LDSG.

- Wie kann die Berechtigungsdokumentation ausgewertet werden? Ist dazu die Mithilfe des Auftragnehmers erforderlich?
- Wie wird die Einhaltung der Aufbewahrungsfrist der Dokumentation der Berechtigung sichergestellt? Ist die Aufbewahrungsfrist abhängig von der Lebensdauer der Objekte?

Für Dienstleistungen im Rahmen des IT-Produkts (Sicht des Auftragnehmers):

- Werden Administrationsebene(n) und Anwendungsebene(n) ausreichend getrennt?
- Ist der Detaillierungsgrad der zu vergebenden Berechtigungen ausreichend? Sind ggf. Rollenkonzepte (etwa besondere Berechtigungen von System- und Verfahrnsadministration und Kontrollrollen wie Leitung, Datenschutzbeauftragter oder Revision) berücksichtigt?
- Wie wird die Vergabe dieser Rechte dokumentiert (z. B. durch eine Protokolldatei, ein externes Tool)? Wer hat Zugriff auf die Dokumentation? Wie wird die Einhaltung der Aufbewahrungsfrist der Dokumentation sichergestellt (vgl. auch Abschnitt 3.3)?

3.1.4 Protokollierung

Protokollierungen und Dokumentationen sind in verschiedenen Zusammenhängen relevant, beispielsweise bei Speicherung, Verarbeitung, Veränderung, Abrufen und Übermittlungen von Daten, der Einrichtung, Änderung und Löschung von Berechtigungen, Vergabe und Entzug von Authentisierungsdaten, Änderung von Parameter und Konfigurationsdaten, Ausführung und Rückeinspielung von Backups etc. Protokollierungen erfolgen häufig sowohl produktbasiert, als auch außerhalb von IT-Produkten, etwa auf speziellen Protokollierungsservern.

Untersuchungsgegenstand: Gegenstand dieses Prüfpunktes ist nicht Art, Umfang und Notwendigkeit der Protokollierung einzelner Ereignisse, sondern Behandlung und Umgang mit den Protokolldaten. Daher sind die Aspekte dieses Abschnitts ggf. mehrfach für verschiedene Arten von Protokollen anzuwenden.

In diesem Zusammenhang wichtige Fragestellungen:

- Wie lassen sich die Protokolldaten auswerten? Gibt es automatisierte Auswertungsroutinen? Nach welchen Kriterien? Welche Zugriffsrechte gibt es?
- Sofern eine stichprobenartig Protokollierung erfolgt: Sind Stichproben ausreichend? Ist der Umfang der Stichprobe konfigurierbar?
- Wurden die datenschutzrechtlichen Anforderungen für die Verarbeitung der Protokolldaten geprüft? Sind ggf. spezielle Regelungen zu beachten (z. B. bei Aufzeichnung von Telefonaten, Videoüberwachung)?
- Wann werden die Protokolldaten gelöscht (zeitgesteuert statt speicherplatzgesteuert)?
- Sind gesetzliche Speicherfristen für die Protokolldatenbestände zu beachten (z. B. § 6 Abs. 4 LDSG), oder sind die Speicherfristen durch die Anwender festzulegen? Wie können sie in diesem Fall konfiguriert werden?

- Welche Maßnahmen wurden zum Schutz „überlaufender“ Protokolldateien unternommen?
- Wie werden die technischen und organisatorischen Maßnahmen, die hinsichtlich des Zugriffs, der Auswertung und der Löschung der Protokolldaten getroffen wurden, dokumentiert (§ 4 Abs. 5 DSGVO)?

Für Hardware/Software:

- Können Protokoll- und Dokumentationsdaten exportiert werden?
- Wie erfolgt die Löschung?

Für Dienstleistungen im Rahmen des IT-Produkts (Sicht des Auftraggebers):

- Kann der Auftraggeber jederzeit die ihn betreffenden Dokumentationen und Protokolle einsehen? Ist dies mit Kosten verbunden?
- Ist der Auftragnehmer zur Herausgabe der Dokumentationen und Protokolle bei Beendigung des Auftrags an den Auftraggeber verpflichtet?
- Ist die Mithilfe des Auftragnehmers bei der Auswertung der Protokolle erforderlich?

Für Dienstleistungen im Rahmen des IT-Produkts (Sicht des Auftragnehmers):

- Kann der Auftragnehmer Dokumentationen und Protokolle bei Beendigung des Auftrags an den Auftraggeber herausgeben?
- Ist für die Auswertung von Protokolldateien eine Hilfestellung für den Auftraggeber erforderlich?
- Erfolgt im Rahmen der Protokollierung eine Mandantentrennung beim Auftragnehmer?

3.1.5 Verschlüsselung und Signatur

Untersuchungsgegenstand:

Werden Verschlüsselungs- und Signaturverfahren adäquat umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:

- Ist die Übertragung von Daten durch öffentliche Netze mit Hilfe von Verschlüsselungsverfahren geschützt (z. B. SSL)? Falls ja, sind geeignete Mechanismen implementiert, die das nachträgliche Brechen der Verschlüsselung – und damit die Offenbarung der Kommunikationsinhalte – bei bereits abgeschlossenen Kommunikationsvorgängen wirksam unterbinden (Stichwort: Forward Secrecy)?
- Werden anerkannte und offengelegte Verschlüsselungs- bzw. Signaturverfahren eingesetzt?
- Ist im Zusammenhang mit den eingesetzten Signaturverfahren die Verwendung von Pseudonymen möglich?
- Sind Schlüsselgenerierung, Schlüsselmanagement und Zertifikat Handling adäquat realisiert?
- Gibt es Maßnahmen zur Schlüsselhinterlegung für Schlüssel zur Entschlüsselung von Datenbeständen bzw. Überprüfung von Signaturen?

- Wurden ausreichende Schlüssellängen eingesetzt?
- Wurden Maßnahmen vorgesehen, falls sich die verwendeten Verfahren oder Schlüssellängen als unzulänglich herausstellen sollten (z. B. Wechsel des Verfahrens oder seiner Komponenten, Umschlüsseln etc.)?
- Existieren geeignete Mechanismen, um die Inhalte einer Kommunikation hinreichend zu sichern (z. B. durch eine Ende-zu-Ende-Verschlüsselung)?
- Sind die zum Einsatz kommenden Verschlüsselungsmechanismen so gestaltet, dass sie vom Nutzer auf einfache Weise verwendet werden können? Gibt es für einen solchen Einsatz geeignete Hinweise?
- Liegen alle notwendigen Informationen für die Dokumentation gemäß § 4 Abs. 4 DSGVO vor?

3.1.6 Pseudonymisieren

Untersuchungsgegenstand:

Wird eine gebotene oder geforderte Pseudonymisierung erleichtert oder unterstützt?

In diesem Zusammenhang wichtige Fragestellungen:

- Welche Organisationen oder Betroffenen haben Zugriff auf die Zuordnungsfunktion bei einer Pseudonymisierung?
- Sind geeignete Maßnahmen ergriffen worden, um die Zuordnungsfunktion bei einer Pseudonymisierung zu sichern?
- Ist die Zuordnungsfunktion geeignet, dass ohne Kenntnis und Nutzung dieser Zuordnungsfunktion der Personenbezug nicht hergestellt werden kann? Besteht das Risiko, auch ohne Kenntnis und Nutzung der Zuordnungsfunktion mit nur wenig Zusatzwissen den Personenbezug von einzelnen Daten(sätzen) herstellen zu können (etwa bei einer Pseudonymisierung durch Vertauschen von Namensbuchstaben, Anreicherung von Profilen etc.)?
- Für den Fall, dass unter bestimmten Bedingungen eine Aufdeckung eines Pseudonyms ermöglicht wird (etwa auf gerichtliche Anordnung): Wie ist dies umgesetzt (unter welchen Bedingungen, wie wird dies überprüft, mit Hilfe welcher Parteien wird der Personenbezug hergestellt, sind zusätzliche Personen betroffen, wie erfolgt die Information der Betroffenen) und existiert hierzu eine schriftliche Prozessbeschreibung?

3.1.7 Anonymisieren

Untersuchungsgegenstand:

Wird eine gebotene oder geforderte Anonymisierung erleichtert oder unterstützt?

In diesem Zusammenhang wichtige Fragestellungen:

- Werden durch die Anonymisierung alle unmittelbar identifizierenden Angaben (z. B. Namen, Kennnummern, Telefonnummern, IP-Adressen etc.) entfernt oder so verändert, dass eine Identifizierung nicht mehr möglich ist?
- Ist die Anonymisierung geeignet und effektiv, oder besteht das Risiko, mit nur wenig Zusatzwissen den Personenbezug von einzelnen Daten(-sätzen) herstellen zu können (etwa durch Abruf von Informationen aus öffentlich zugänglichen Quellen)?

- Können Aussagen zur Qualität der Anonymisierung getroffen werden (Stichwort: „k-anonymity“)?

3.2 Allgemeine Pflichten

3.2.1 Technisch-organisatorische Maßnahmen

Untersuchungsgegenstand:

Werden die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit durch das IT-Produkt selbst ergriffen bzw. enthält das IT-Produkt Hinweise zur Umsetzung der erforderlichen Maßnahmen?

Rechtsgrundlagen:

§ 5 LDSG, § 78a SGB X oder § 9 BDSG jeweils mit Anlage

3.2.1.1 Verfügbarkeit

Untersuchungsgegenstand: Verfügbarkeit

Gewährleisten die ergriffenen Maßnahmen, dass Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (Verfügbarkeit)?

In diesem Zusammenhang wichtige Fragestellungen:

Für IT-Produkte:

- Bietet das IT-Produkt Funktionalitäten für Datensicherungen (z. B. Exportschnittstellen zu Datensicherung)?
- Hat die einsetzende Stelle eigene Datensicherungsmaßnahmen zu ergreifen (z. B. Backup auf Dateiebene)? Sind dazu ggf. weitere, nicht vom IT-Produkt umfasste Komponenten (z. B. spezifische Backup-Agents für DBMS, Mail-Server etc.) erforderlich?
- Wird zwischen Archivierung und Datensicherung funktional unterschieden?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftraggebers):

- Gibt es vertragliche Festlegungen für Verfügbarkeiten (Service Level Agreements)?
- Berücksichtigen diese auch Fälle eines vollständigen Datenverlustes (etwa bei Fällen, in den auch Backup-Verfahren versagen)?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftragnehmers):

- Gibt es vertragliche Festlegungen für Verfügbarkeiten (Service Level Agreements)?
- Welche Maßnahmen wurden getroffen, um die Verfügbarkeit von Daten und Verfahren zu gewährleisten (z. B. Redundanzkonzepte, Datensicherungskonzepte, Notstrom etc.)? Sind sie ausreichend?

- Wurden diese Maßnahmen getestet (z. B. Backup- & Recovery-Tests)?
- Wird der Auftraggeber auf eventuelle Pflichten (z. B. eigene Datenkopien) oder Einschränkungen („nicht bei höherer Gewalt“) hingewiesen?
- Wenn zur Dienstleistung zusätzliche IT-Produkte verwendet wurden:
 - Beinhalten diese Mechanismen, um die Verfügbarkeit der Daten zu gewährleisten (siehe oben)?
 - Werden diese Mechanismen durch den Auftragnehmer sachgerecht eingesetzt (Einbindung in die Redundanz- und Datensicherungskonzepte des Auftragnehmers)?

3.2.1.2 Integrität

Untersuchungsgegenstand: Integrität

Gewährleisten die ergriffenen Maßnahmen, dass Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (Integrität)?

In diesem Zusammenhang wichtige Fragestellungen:

Generell:

- Gibt es Integritätsprüfungen eingegebener Daten?
- Gibt es im Rahmen der Interventionsfähigkeit Mechanismen zum Umgang mit vermeintlichen Integritätsverletzungen (z. B. wenn eine unzulänglich spezifizierte Integritätsprüfung fälschlich eine Integritätsverletzung meldet)?

Für IT-Produkte:

- Wie schützt das IT-Produkt gespeicherte Daten gegen unbefugte oder unbeabsichtigte Modifikationen?
- Wie schützt das IT-Produkt übertragene Daten gegen unbefugte oder unbeabsichtigte Modifikationen?
- Auf welche Weise können Modifikationen, die nicht unterbunden werden können, zumindest erkannt werden (z. B. durch Signaturen oder Fehlercodes)?
- Auf welche Weise stellt das IT-Produkt die Aktualität von Daten sicher oder unterstützt die einsetzende Stelle dabei, Daten aktuell zu halten (z. B. Möglichkeiten und Schnittstellen zum Update von Daten, Aktualitätsinformationen, Hinweise auf Alter der Daten)?
- Wie schützt das IT-Produkt die Mechanismen, durch die automatisiert eine Änderung der Daten erfolgt (z. B. Verarbeitungslogik, Berechnungsverfahren, Entscheidungssysteme)?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftraggebers):

- Erfordert die Dienstleistung die Übertragung von Daten zwischen Auftragnehmer und Auftraggeber (ggf. außerhalb der benutzten IT-Produkte)? Ist diese gegen unbefugte oder unbeabsichtigte Modifikation geschützt?
- Auf welche Weise können Modifikationen im Einflussbereich des Auftragnehmers, die nicht unterbunden werden können, zumindest erkannt werden?

- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftragnehmers):

- Wenn zur Dienstleistung zusätzliche IT-Produkte verwendet wurden:
 - Beinhalten diese Mechanismen, um die Integrität der Daten zu gewährleisten (siehe oben)?
 - Werden diese Mechanismen durch den Auftragnehmer sachgerecht eingesetzt?
- Wie schützt der Auftragnehmer gespeicherte Daten (außerhalb ggf. benutzter IT-Produkte) gegen unbefugte oder unbeabsichtigte Modifikationen?
- Wie schützt der Auftragnehmer übertragene Daten (außerhalb ggf. benutzter IT-Produkte) gegen unbefugte oder unbeabsichtigte Modifikationen?
- Ist die IT-Infrastruktur des Auftragnehmers gegen Schadsoftware ausreichend geschützt?

3.2.1.3 Vertraulichkeit

Untersuchungsgegenstand: Vertraulichkeit

Gewährleisten die ergriffenen Maßnahmen, dass nur befugt auf Verfahren und Daten zugegriffen werden kann (Vertraulichkeit)?

In diesem Zusammenhang wichtige Fragestellungen:

Generell:

- Werden Firewalls oder Intrusion Detection & Response Systems wirkungsvoll gegen unbefugte Zugriffe eingesetzt?
- Sind verwendete Verschlüsselungsverfahren adäquat umgesetzt?
- Sind Maßnahmen zum Löschen/Sperren/Zerstören der Daten oder Geräte bei unbefugtem Öffnen/Eingriffen (z. B. bei Chipkarten) vorgesehen?
- Werden geeignete Mechanismen eingesetzt, um eine absichtliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. Kennzeichnung der Daten für Sensibilisierung (z. B. „VS“) oder Nachverfolgbarkeit (z. B. steganographische Markierung)?
- Filter für ausgehende Informationen: Gibt es Mechanismen, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. durch rückstandslose Beseitigung von personenbezogenen (Zusatz-)Daten bei möglicher Herausgabe (z. B. detaillierte Informationen über den Autor in Word-Dokumenten, automatisierte Weitergabe von Zusatzinformationen bei HTTP-Kommunikation durch Voreinstellungen im Webbrowser)?
- Werden Mechanismen eingesetzt, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. durch die Reduktion des Einsichtswinkels bei Monitoren oder das Vermeiden von Abstrahlung bei Monitoren, (Funk-)Tastatur, Maus usw. (Tempest)?
- Wird die rückstandslose Beseitigung von personenbezogenen Daten von Datenträgern/Geräte(teile)n (z. B. Festplatten, Faxbauteile, Speicherkarten, USB-Speichermedien), die an Dritte weitergegeben werden können, gewährleistet oder

unterstützt?

- Wurden Maßnahmen ergriffen, um die Sensibilität der Verarbeiter zu steigern (z. B. automatisierte Warnhinweise etc.)?

Für IT-Produkte:

- Wie schützt das IT-Produkt gespeicherte Daten gegen unbefugte oder unbeabsichtigte Kenntnisnahme?
- Wie schützt das IT-Produkt übertragene Daten gegen unbefugte oder unbeabsichtigte Kenntnisnahme?
- Wie schützt das IT-Produkt Funktionalitäten (z. B. Exportfunktionen) gegen unbefugte oder unbeabsichtigte Verwendung?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftraggebers):

- Erfordert die Dienstleistung die Übertragung von Daten zwischen Auftragnehmer und Auftraggeber (ggf. außerhalb des benutzten IT-Produkts)? Ist diese gegen unbefugte oder unbeabsichtigte Kenntnisnahme geschützt?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftragnehmers):

- Wenn zur Dienstleistung IT-Produkte verwendet wurden:
 - Beinhalten diese Mechanismen, um die Vertraulichkeit der Daten zu gewährleisten (siehe oben)?
 - Werden diese Mechanismen durch den Auftragnehmer sachgerecht eingesetzt?
- Wie schützt der Auftragnehmer gespeicherte Daten (auch außerhalb ggf. benutzter IT-Produkte) gegen unbefugte oder unbeabsichtigte Kenntnisnahme?
- Wie schützt der Auftragnehmer übertragene Daten (auch außerhalb ggf. benutzter IT-Produkte) gegen unbefugte oder unbeabsichtigte Kenntnisnahme?

3.2.1.4 Nicht-Verkettbarkeit

Untersuchungsgegenstand: Nicht-Verkettbarkeit

Gewährleisten die ergriffenen Maßnahmen, dass personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (Nicht-Verkettbarkeit)?

In diesem Zusammenhang wichtige Fragestellungen:

Für IT-Produkte:

- Kommen Anonymisierungs- oder Pseudonymisierungsmechanismen zum Einsatz?
- Werden nicht mehr benötigte (Identifizierungs-)Daten frühzeitig gelöscht?
- Können personenbezogene Daten in Hinblick auf den ausgewiesenen Zweck gekennzeichnet werden?
- Gibt es Mechanismen, die eine Datenverarbeitung bzw. -nutzung abhängig von

einer Zweckkennzeichnung der Daten oder Systeme steuern können? (Funktionalitätsbeschränkung bei zweckwidriger Verarbeitung)?

- Können rechtlich zulässige zweckübergreifende oder zweckändernde Verarbeitungen besonders geschützt werden (z. B. Vier-Augen-Prinzip, besondere Rollen und Rechte)?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftraggebers):

- Werden die Daten ausreichend von den Daten anderer Auftraggeber getrennt?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftragnehmers):

- Werden die Daten der Auftraggeber ausreichend voneinander getrennt?
- Werden Daten (oder Teile davon) auftraggeberübergreifend² für eigene Zwecke des Auftragnehmers verarbeitet? Ist dies rechtlich legitimiert? Werden dabei personenbezogenen Daten verarbeitet, oder wird der Personenbezug durch Anonymisierung entfernt?
- Werden Daten (oder Teile davon) auftraggeberübergreifend verarbeitet, um auftraggeberindividuelle Dienste³ zu erbringen? Ist dies rechtlich legitimiert? Werden dabei personenbezogenen Daten verarbeitet, oder wird der Personenbezug durch Anonymisierung entfernt?

3.2.1.5 Transparenz

Untersuchungsgegenstand: Transparenz

Gewährleisten die ergriffenen Maßnahmen, dass die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (Transparenz)?

In diesem Zusammenhang wichtige Fragestellungen / Dokumente (siehe auch Hinweise im Dokument „Produktdokumentation“):

- Sind die Kategorien der verarbeiteten Daten nachvollziehbar dokumentiert?
- Sind die Prozessbeschreibungen nachvollziehbar dokumentiert?
- Können Konfigurationen und Datenverarbeitungsschritte im konkreten Fall nachvollzogen werden?
- Können die für die Nachvollziehbarkeit der Datenverarbeitung erforderlichen Protokolle (Protokollereignis, Detaillierungsgrad, Speicherdauer) konfiguriert werden?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

² Z. B. Berechnung von Durchschnittswerten über alle Auftraggeber.

³ Z. B. Berechnung der auftraggeberindividuellen Abweichung von Durchschnittswerten.

Für Dienstleistungen (Sicht des Auftraggebers):

- Sind die für die Nachvollziehbarkeit der Datenverarbeitung erforderlichen Protokolle (Protokollereignis, Detaillierungsgrad, Speicherdauer) festgelegt?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftragnehmers):

- Können die für die Nachvollziehbarkeit der Datenverarbeitung erforderlichen Protokolle (Protokollereignis, Detaillierungsgrad, Speicherdauer) festgelegt werden?

3.2.1.6 Intervenierbarkeit

Untersuchungsgegenstand: Intervenierbarkeit

Sind die Verfahren so gestaltet, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den §§ 26 bis 30 LDSG wirksam ermöglichen (Intervenierbarkeit)?

In diesem Zusammenhang wichtige Fragestellungen:

Für IT-Produkte:

- Gibt es Produktfunktionalitäten, so dass die in Komplex 4 aufgeführten Rechte der Betroffenen umgesetzt werden können?
- Kann in einzelne Prozessschritte des Verfahrens, die sich als unsicher oder unrechtmäßig herausstellen, eingegriffen werden? Können solche Prozessschritte deaktiviert werden?
- Kann in einzelne Prozessschritte zugunsten einzelner Betroffener eingegriffen werden (z. B. falls Prozessschritte in Bezug auf einzelne Betroffene unrechtmäßig oder unsicher sind)?⁴
- Falls Betroffene selbst an der Datenverarbeitung direkt beteiligt sind⁵: Sind Mechanismen vorgesehen, um die Datenverarbeitung aktiv zu beeinflussen, etwa zu deaktivieren oder zu stoppen?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftraggebers):

- Können Auftraggeber die Datenverarbeitung ihres Auftragnehmers effektiv beeinflussen?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen nachvollziehbar für die einsetzende Stelle beschrieben?

Für Dienstleistungen (Sicht des Auftragnehmers):

- Können Auftraggeber die Datenverarbeitung des Auftragnehmers effektiv beeinflussen, wenn sie ihrer Verantwortung als datenverarbeitende Stelle gerecht

⁴ Z. B. Gegendarstellungen, Ausschluss von Übermittlungen bei gesperrten Daten, Eingriffe in automatisierte Einzelentscheidungen.

⁵ Z. B. durch Endgeräte im Bereich der Betroffenen (etwa Chipkarten, Meysysteme, Sensoren etc.) oder bei der Datenerhebung oder -verarbeitung durch Betroffene (etwa per Webseiten, E-Mail-Clients etc.).

werden?

3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen

Untersuchungsgegenstand:

Werden Daten und Datenverarbeitungsvorgänge (u. a. Eingabe, Veränderung, Weitergabe, Abruf, Löschung etc.) protokolliert, wenn dies rechtlich erforderlich ist?

Rechtsgrundlagen:

§§ 5 Abs. 1 Nr. 4, 6 Abs. 4, 8 Abs. 4, 14 Abs. 3, 15 Abs. 2 LDSG, §§ 9 S. 1, 10 Abs. 4 BDSG, § 79 Abs. 4 SGB X

In diesem Zusammenhang wichtige Fragestellungen:

- Welche der Daten werden ausschließlich automatisiert gespeichert, so dass erhöhte Protokollierungsanforderungen (z. B. § 6 Abs. 4 LSDG) bestehen?
- Ist eine Vollprotokollierung erforderlich? Sind Stichproben ausreichend? Ist der Umfang der Stichprobe konfigurierbar?

Für Dienstleistungen (Sicht des Auftraggebers und des Auftragnehmers):

- Wie werden die technischen und organisatorischen Maßnahmen, die hinsichtlich des Zugriffs, der Auswertung und der Löschung der Protokolldaten getroffen wurden, dokumentiert (§ 4 Abs. 5 DSVO)?

3.2.1.8 Test und Freigabe

Untersuchungsgegenstand:

Werden automatisierte Verfahren vor ihrem Einsatz und nach wesentlichen Änderungen überprüft und freigegeben?

Rechtsgrundlage:

§ 5 Abs. 2 LDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Werden Test und Freigabe unterstützt (z. B. durch die Mitlieferung von relevanten und umfassenden Testdaten/fällen, Hinweise zu Prüfungen, Bereitstellung von Formularen etc.)?

Für Dienstleistungen (Sicht des Auftraggebers):

- Für welche Teile der Datenverarbeitung trägt der Auftraggeber die Verantwortung für die Durchführung von Test und Freigabe?
- Wie werden die Ergebnisse von Tests und die Freigabe dem Auftragnehmer kommuniziert?

Für Dienstleistungen (Sicht des Auftragnehmers):

- Für welche Teile der Datenverarbeitung trägt der Auftragnehmer die Verantwortung für die Durchführung von Test und Freigabe?

3.2.2 Erleichterung der Vorabkontrolle

Untersuchungsgegenstand:

Wird eine eventuell notwendige Vorabkontrolle durch das IT-Produkt (inkl.

Beschreibung) unterstützt?

Rechtsgrundlagen:

§ 9 LDSG, vgl. § 4d Abs. 5, 6 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Werden Test und Freigabe unterstützt (z. B. durch die Mitlieferung von relevanten und umfassenden Testdaten/fällen, Hinweise zu Prüfungen, Bereitstellung von Formularen etc.)
- Werden Werkzeuge (Formulare, interaktive Tools) zur Erstellung von individuell zugeschnittenen Dokumentationen und Konzepten bereitgestellt?

3.2.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses

Untersuchungsgegenstand:

Wird durch das IT-Produkt (inkl. Beschreibung) die Erstellung von Verfahrensverzeichnissen oder die Meldung von Verfahren unterstützt?

Rechtsgrundlagen:

§ 7 LDSG, Meldepflichten in §§ 4d, 4e BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Werden Werkzeuge (Formulare, interaktive Tools) zur Erstellung von individuell zugeschnittenen Dokumentationen und Konzepten bereitgestellt?
- Werden prototypische Dokumentationen und Konzepte bereitgestellt?

3.2.4 Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Untersuchungsgegenstand:

Inwieweit wird die Benachrichtigung der Aufsichtsbehörde und des Betroffenen im Falle von unrechtmäßiger Kenntniserlangung von Daten vom IT-Produkt geleistet oder unterstützt?

Rechtsgrundlagen:

§ 27a LDSG, § 42a BDSG, § 109a TKG, § 15a TMG

In diesem Zusammenhang wichtigen Fragestellungen:

- Werden mit dem IT-Produkt einschlägige und von den §§ 27a LDSG und 42a BDSG erfasste Daten verarbeitet?
- Gibt es aufseiten der einsetzenden Stelle oder ihrer Dienstleister Mechanismen, die die Aufdeckung einer unrechtmäßigen Kenntniserlangung durch Dritte ermöglichen?
- Gibt es aufseiten der einsetzenden Stelle oder ihrer Dienstleister geeignete dokumentierte Prozesse, die sicherstellen, dass die Informationspflichten der §§ 27a LDSG bzw. 42a BDSG eingehalten werden können bzw. wird sie hierzu in die Lage versetzt.
 - Werden im Rahmen der Sicherheitsanalyse entsprechende Vorfälle betrachtet, bewertet und deren Eintrittswahrscheinlichkeit analysiert?

- Gibt es innerhalb der verantwortlichen Stelle oder ihrer Dienstleister hierfür einen Verantwortlichen?
- Besteht innerhalb der verantwortlichen Stellen (oder / und ggf. bei ihren Dienstleistern) Kenntnis über die für sie zuständige Aufsichtsbehörde?
- Gibt es bei der verantwortlichen Stelle oder ihren Dienstleistern festgelegte Informationen (bspw. Informationsrundschriften, Presstexte etc.), die bei solchen Vorfällen Verwendung finden?
- Werden den jeweils Betroffenen Quellen genannt, bei denen sie ggf. weitere Informationen und Verhaltensvorschläge (bspw. hinsichtlich der regelmäßigen und genauen Kontrolle von Bankinformationen) einholen können?
- Werden entsprechende Vorfälle bei der verantwortlichen Stelle oder bei ihren Dienstleistern angemessen dokumentiert?

3.2.5 Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten

Untersuchungsgegenstand:

Wird die / der behördliche Datenschutzbeauftragte bei der Wahrnehmung ihrer / seiner Pflichten unterstützt?

Rechtsgrundlagen:

§ 10 LDSG, vgl. § 81 Abs. 4 SGB X, §§ 4e, 4f BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Werden Test und Freigabe unterstützt (z. B. durch die Mitlieferung von relevanten Testdaten, Hinweise zu Prüfungen, Bereitstellung von Formularen etc.)?
- Wird die datenschutzrechtliche Kontrolle des IT-Produkts und seines Betriebes durch geeignete Maßnahmen (z. B. Bereitstellung adäquater Dokumentation, Hilfsmittel bei der Auswertung von Protokolldaten etc.) unterstützt?

3.3 Spezifische Pflichten

3.3.1 Verschlüsselung

Untersuchungsgegenstand:

Wird eine bestehende Pflicht zur Verschlüsselung von Datenbeständen adäquat umgesetzt?

Rechtsgrundlagen:

§ 6 LDSG, Anlage zu § 9 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Werden personenbezogene Daten, die mit Hilfe informationstechnischer Geräte außerhalb der Räumlichkeiten der datenverarbeitenden Stelle verarbeitet werden, verschlüsselt?

- Kann die datenverarbeitende Stelle die Daten wieder entschlüsseln?
- Wenn die Verschlüsselung aus technischen Gründen nicht möglich ist, liegen dann dem Schutzbedarf der personenbezogenen Daten angemessene Verfahrensregelungen vor?
- Werden anerkannte und offengelegte Verschlüsselungsverfahren eingesetzt?
- Sind Schlüsselgenerierung und Schlüsselmanagement adäquat realisiert?
- Wurden ausreichende Schlüssellängen eingesetzt?
- Wurden Maßnahmen vorgesehen, falls sich die verwendeten Verfahren oder Schlüssellängen als unzulänglich herausstellen sollten (z. B. Wechsel des Verfahrens oder seiner Komponenten, Umschlüsseln etc.)
- Sind die zum Einsatz kommenden Verschlüsselungsmechanismen so gestaltet, dass sie vom Nutzer auf einfache Weise verwendet werden können? Gibt es für einen solchen Einsatz geeignete Hinweise?

3.3.2 Anonymisierung oder Pseudonymisierung

Untersuchungsgegenstand:

Wird eine gebotene oder geforderte Anonymisierung oder Pseudonymisierung erleichtert oder unterstützt?

Rechtsgrundlagen:

§ 2 Abs. 2 Nr. 6, 7, § 11 Abs. 6, § 22 Abs. 1 LDSG, § 67 Abs. 8a SGB X, § 3 Abs. 6a BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Ist eine Anonymisierung oder Pseudonymisierung von Daten für Zwecke der Forschung (§ 22 Abs. 1 LDSG) geboten?
- Ist eine Pseudonymisierung von Daten im Rahmen der Datenverarbeitung und Übermittlung (§ 11 Abs. 6 LDSG) gefordert oder geboten?
- Sind die Anonymisierungs- bzw. Pseudonymisierungsverfahren effizient?
- Siehe auch Abschnitte 1.2, 3.1.6 und 3.1.7 .

3.3.3 Technische Umsetzung von speziellen Anforderungen bei besonderem Technikeinsatz

3.3.3.1 Mobile Datenverarbeitungssysteme

Untersuchungsgegenstand:

Werden die besonderen Vorschriften zur Information der Betroffenen bei der Verwendung personenbezogener Speicher- und Verarbeitungsmedien (z. B. Chipkarten) umgesetzt?

Rechtsgrundlagen:

§ 18 Abs. 2 LDSG, § 6c BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Sind die Verarbeitungsgeräte und die hierauf betriebene Software so gestaltet, dass Verarbeitungsvorgänge sowie Art und Umfang personenbezogener Daten jederzeit erkennbar sind?

- Kann der Betroffene die Datenverarbeitung jederzeit verhindern?
- Werden besondere Vorkehrungen gegen unzulässiges Auslesen (etwa bei RFID-Karten) getroffen?

3.3.3.2 Video-Überwachung und –Aufzeichnung

Untersuchungsgegenstand:

Werden die gesetzlichen Vorgaben umgesetzt?

Rechtsgrundlagen:

§ 20 Abs. 2 S. 1 LDSG, § 6b Abs. 2, 4 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Wird die Tatsache einer Beobachtung den Betroffenen erkennbar gemacht?
- Wird die Einhaltung der festgelegten Löschungsfristen für Aufzeichnungen sichergestellt?
- Werden geeignete Sicherungsmaßnahmen zum Schutz der Aufzeichnungen ergriffen?

3.3.3.3 Automatisierte Einzelentscheidungen

Untersuchungsgegenstand:

Werden die gesetzlichen Vorgaben umgesetzt?

Rechtsgrundlagen:

§ 19 S. 2 Nr. 2 LDSG, § 6a Abs. 2 Nr. 2, Abs. 3 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Auf welche Weise können Betroffenen ihre besonderen persönlichen Interessen vor der Entscheidung geltend machen?
- Auf welche Weise kann dem Betroffenen Auskunft über den logischen Aufbau der Datenverarbeitung, hier speziell den Entscheidungsmechanismen, gegeben werden? Liegen der verantwortlichen Stelle dazu alle notwendigen Informationen vor?
- Sofern Scoring zur Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses eingesetzt wird: Werden die Voraussetzungen des § 28b BDSG eingehalten?

Siehe auch Abschnitt 2.4.4 zu Rechtsgrundlagen für automatisierte Einzelentscheidungen.

3.3.3.4 Veröffentlichungen im Internet

Untersuchungsgegenstand:

Werden die gesetzlichen Vorgaben zur Veröffentlichung von Daten im Internet umgesetzt?

Rechtsgrundlage:

§ 21 LDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Wie kann die Veröffentlichung von Daten im Internet befristet werden?
- Wie können Fristen festgelegt werden?
- Werden danach die Daten automatisch gelöscht oder gesperrt, so dass ein Zugriff aus dem Internet heraus nicht mehr möglich ist?
- Kommen Mechanismen zum Einsatz, die die dauerhafte Archivierung von Internetveröffentlichungen durch Dritte erschweren oder zumindest anzeigen, dass dies nicht gewünscht ist (z. B. Ausschluss von Archivierungsdiensten in robots.txt)?

3.4 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren

Untersuchungsgegenstand:

In welcher Weise werden Anwender bei der Erfüllung ihrer Pflichten aus der DSVO unterstützt?

In diesem Zusammenhang wichtige Fragestellungen:

- Gibt es Anleitungen, um die nach DSVO geforderten Unterlagen bzgl. des Einsatzes von Informationstechnik (§ 3 Abs. 2 DSVO), der Sicherheitsmaßnahmen (§ 4 DSVO) und des Vorgehens bei Test und Freigabe (§ 5 DSVO) zu erstellen?
- Wie wird die Erstellung des Sicherheitskonzeptes und der Risikoanalyse (nach § 4 Abs. 2 DSVO) unterstützt (siehe auch Abschnitte 3.2.3, 3.2.4)?
- Wie werden Test und Freigabe (nach § 5 DSVO) sowie deren Protokollierung und Dokumentation unterstützt (siehe auch Abschnitte 3.2.3, 3.2.4)?
- Wie wird die Erstellung der Verfahrensdokumentation (nach § 3 DSVO) unterstützt, insbesondere die Darstellung des Verfahrenszwecks (nach § 3 Abs. 2 Nr. 1 DSVO, siehe auch Rechtsgrundlagen nach Abschnitt 2) sowie die Verfahrensbeschreibung (nach § 3 Abs. 1 DSVO, siehe auch Abschnitte 3.2.3, 3.2.4)? Wie wird dokumentiert, welchen Personen welche Nutzungsrechte an welchen informationstechnischen Geräten, Programmen und automatisierten Dateien für welche Zeiträume gewährt wurden (z. B. durch die Bereitstellung von Werkzeugen zur Dokumentation der Nutzungsrechtevergabe und Administration)? Wie werden dabei die Aufbewahrungsfrist von mindestens 5 Jahren (§ 3 Abs. 3 DSVO) und die Revisionsicherheit sichergestellt?
- Wie wird dokumentiert, welche Personen für welche Zeiträume befugt sind, Änderungen an der Funktionsweise von informationstechnischen Geräten, an den Programmen, an der Speicherorganisation der automatisierten Dateien und den Nutzungsrechten vorzunehmen (vgl. § 3 Abs. 2 Nr. 5 DSVO)? Wie werden dabei die Aufbewahrungsfrist von mindestens 5 Jahren und die Revisionsicherheit sichergestellt?

3.5 Anforderungen an den Betrieb bei Auftragsdatenverarbeitung

Untersuchungsgegenstand:

Werden die technisch-organisatorischen Vorgaben aus dem Auftragsdatenverarbeitungsvertrag durch den Auftragnehmer eingehalten, wenn das IT-Produkt Teil einer Auftragsdatenverarbeitung ist? Sind die Maßnahmen angemessen und vollständig?

Maßnahmen, die typischerweise durch Auftragnehmer einer Datenverarbeitung umzusetzen sind:

- Physikalischer Zugriffsschutz (Zutrittskontrolle)
- Zugangs- und Zugriffskontrolle für Mitarbeiter des Auftragnehmers
- Sicherung der Netzzugänge (z. B. Firewall, Intrusion Detection Systems)
- Sicherung der Integrität der Daten und Datenverarbeitungssystem (z. B. Schutz vor Manipulation inkl. Schadsoftware, regelmäßiges Patchen)
- Sicherung der Verfügbarkeit (z. B. Erstellung und sichere Lagerung von Backups., Umsetzung von Redundanzkonzepten, Brandschutz, Notstromversorgung)
- Regelmäßige interne Kontrolle der Sicherheitsmaßnahmen

In diesem Zusammenhang wichtige Fragestellungen:

- Wie werden diejenigen Aspekte der Datenverarbeitung, die durch den Auftragnehmer durchgeführt werden, im Sinne der DSVO (siehe Abschnitt 3.4) dokumentiert?
- Werden alle technisch-organisatorischen Maßnahmen, die standardmäßig mit Auftraggebern vereinbart werden (etwa durch Musterverträge oder AGB), durch den Auftragnehmer umgesetzt?
- Auf welche Weise kann ein Auftraggeber dies kontrollieren?
- Auf welche Weise weist der Auftragnehmer die Umsetzung der vereinbarten technisch-organisatorischen Maßnahmen nach?

3.6 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit oder aus weiteren Datenschutzprinzipien ergeben?

4 Komplex 4: Rechte der Betroffenen

4.1 Aufklärung und Benachrichtigung

Untersuchungsgegenstand:

Inwieweit werden Aufklärung und Benachrichtigung von Betroffenen vom IT-Produkt geleistet oder unterstützt?

Rechtsgrundlagen:

§ 26 LDSG, § 33 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Gibt es besondere Maßnahmen, um die Transparenz der Datenverarbeitung für den Betroffenen sicherzustellen?
- Können einzelne Datenverarbeitungsschritte (z. B. Übermittlungen in Form eines „Einzelnutzungsnachweises“) dem Betroffenen verdeutlicht werden?

4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten

Untersuchungsgegenstand:

Inwieweit wird die Benachrichtigung des Betroffenen im Falle von unrechtmäßiger Kenntniserlangung von Daten vom IT-Produkt geleistet oder unterstützt?

Rechtsgrundlagen:

§ 27a LDSG, § 42a BDSG, § 109a TKG, § 15a TMG

Zu in diesem Zusammenhang wichtige Fragestellungen siehe Kapitel 3.2.4.

4.3 Auskunft

Untersuchungsgegenstand:

Wird eine Auskunft vom IT-Produkt angemessen unterstützt?

Rechtsgrundlagen:

§ 27 LDSG, §§ 25, 83 SGB X, § 34 BDSG, § 13 Abs. 7 TMG, § 93 TKG, Art. 12 EU-DSRL

In diesem Zusammenhang wichtige Fragestellungen:

- Gibt es eine automatisierte Auskunftsbearbeitung durch das IT-Produkt, so dass Hemmschwellen beim Betroffenen und zeitliche Verzögerungen gering sind?
- Sind alle Daten zur Auskunftserteilung leicht auffindbar; gibt es Hilfsmittel dazu?
- Werden untrennbare Verknüpfungen mit personenbezogenen Daten anderer Betroffener vermieden?
- Gibt es eine Protokollierung bei der Übermittlung personenbezogener Daten?
- In welcher Weise erfolgt eine Authentisierung des Auskunftsberechtigten? Ist sie sowohl verlässlich als auch datensparsam umgesetzt?
- Erfasst die Auskunftsmöglichkeit den gesamten Auskunftsanspruch (gespeicherte

Daten, Zweck und Rechtsgrundlage, Herkunft und Empfängerkreis (Auftragnehmer, Datenveränderung), Funktionsweise (logischer Aufbau), Protokolldaten) von automatisierten Verfahren?

- Für den Fall von einer Verarbeitung von Daten unter Pseudonym: Ist eine Auskunftserteilung unter Pseudonym vorgesehen? Wie ist sie realisiert?

4.4 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegen-darstellung)

Rechtsgrundlagen:

§§ 28, 29 LDSG, § 84 SGB X, § 35 BDSG

4.4.1 Berichtigung

Untersuchungsgegenstand:

In welcher Form leistet oder unterstützt das IT-Produkt die Berichtigung von Daten?

In diesem Zusammenhang wichtige Fragestellungen:

- Gibt es automatisierte Berichtigungsbearbeitung vom IT-Produkt?
- Wie wird eine korrekte und unverzügliche Umsetzung der Berichtigung?
- Wie wird eine automatisierte Berichtigung qualitätsgesichert?
- Wie werden Berichtigungen an Empfänger vorangegangener Datenübermittlungen weitergeleitet?

4.4.2 Vollständige Löschung

Untersuchungsgegenstand:

Wie ist die Löschung realisiert?

In diesem Zusammenhang wichtige Fragestellungen:

- Wird vollständig und irreversibel gelöscht?
- Geschieht dies durch physikalisches Löschen auf allen Medien (ohne zusätzliche Kopien, etwa innerhalb einer Funktion zum Rückgängigmachen von Löschungen)?
- Ist eine Selektivität des Löschens möglich (z. B. problematisch bei optischen Speichermedien wie CD-ROM)?
- Wird durch Überschreiben gelöscht? Ist die Umsetzung (z. B. Anzahl der Überschreibvorgänge) adäquat?
- Wie ist die Umsetzung der Löschung auf Backup-Medien realisiert?
- Wie werden Löschungen an Empfänger vorangegangener Datenübermittlungen weitergeleitet?
- Wie werden Lösch- und Prüffristen (Wiedervorlage) realisiert oder unterstützt?

4.4.3 Sperrung

Untersuchungsgegenstand:

Wie wird eine Sperrung von Daten umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:

- Gibt es eine Möglichkeit, die Datensätze so zu kennzeichnen bzw. auszusondern, dass sie für die normale Verarbeitung nicht zur Verfügung stehen, aber gleichwohl gespeichert bleiben?
- Wie wird dies gewährleistet?
Wie wird die Sperrung und ggf. Aufhebung der Sperre protokolliert (Zeitpunkt, Auftraggeber etc.) (siehe auch Abschnitt 3.2.1.7)?

4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung

Untersuchungsgegenstand:

Gibt es eine technische Unterstützung des Widerspruchsrechts?

Rechtsgrundlagen:

§ 29 LDSG, § 84a Abs. 1a SGB X, § 35 Abs. 5 BDSG

In diesem Zusammenhang wichtige Fragestellungen:

- Wie werden Widersprüche an Empfänger vorangegangener Datenübermittlungen weitergeleitet?

4.4.5 Gendarstellung

Untersuchungsgegenstand:

Wie wird realisiert, dass auf Verlangen des Betroffenen dessen Gendarstellung beigefügt wird?

Rechtsgrundlagen:

§ 35 Abs. 6 S. 2 BDSG

4.5 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit oder aus weiteren Datenschutzprinzipien ergeben?

B. Anforderungsprofil für Protokolldaten

Für die Bewertung der Verarbeitung von Protokolldaten sind nicht immer sämtliche Anforderungen aus dem Allgemeinen Anforderungsprofil einschlägig. Im Folgenden sind die wichtigsten Anforderungen dargestellt, die bei der Bewertung der Protokolldaten zu beachten sind. Dieser Katalog ist nicht abschließend, im Einzelfall können auch weitere Anforderungen zu prüfen sein.

Komplex 1:

Es sind die 6 Schutzziele aus Kapitel 1 zu beachten. Hierbei gilt insbesondere:

- **Datenvermeidung und Datensparsamkeit**

Wird der Grundsatz der Datenvermeidung und Datensparsamkeit berücksichtigt, d. h. werden Protokolldaten nur in dem erforderlichen Maß erhoben und wird – falls dieser nicht erforderlich – auf den Personenbezug verzichtet bzw. nachträglich entfernt?

- **Zweckbindung**

Wird sichergestellt, dass die Protokolldaten nur für den vorher bestimmten Zweck verarbeitet werden und bei Zweckerreichung zeitnah die Löschung erfolgt?

- **Nicht-Verkettbarkeit**

Wird sichergestellt, dass die Protokolldaten nur mit den im Zusammenhang stehenden Primärdaten verarbeitet werden? Sie dürfen nicht mit anderen Daten verbunden werden und nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden.

- **Transparenz**

Ist der Umfang der Protokollierung für die Betroffenen hinreichend transparent?

Komplex 2:

- Auf welcher Rechtsgrundlage ist die Erhebung und Speicherung der Protokolldaten zulässig? Sind die Voraussetzungen der Rechtsgrundlage erfüllt?
- Wird die Einhaltung der Zweckbindung für Protokolldaten (§ 13 Abs. 6 LDSG, § 14 Abs. 4 BDSG) durch das IT-Produkt unterstützt?
- Gibt es gesetzliche Aufbewahrungsfristen für die Protokolldaten? Werden die Protokolldaten nach Ablauf der Frist bzw. nach Wegfall des Erfordernisses gelöscht?

Komplex 3:

- Fragestellungen aus 3.1.1
- Sind die Protokolldaten ausreichend gegen unbefugte Zugriffe, gegen Manipulationen und gegen Verlust geschützt? Wer kann die Zugriffsbefugnisse

verwalten (wichtig für die Manipulationsresistenz sowie bei gemeinsamen Verfahren und Abrufverfahren).

- Können anhand der protokollierten Daten die in § 6 Abs. 4 LDSG genannten Informationen über Bearbeiter, Änderungsvorgänge, den Zeitpunkt sowie die Art und Weise der Speicherung, Verarbeitung und Übermittlung ermittelt werden? Insbesondere: Kann bei ändernden Zugriffen ermittelt werden, welche Datenbestände vor der Änderung verfügbar waren? Kann bei lesenden Zugriffen ermittelt werden, welche Daten der zugreifenden Person angezeigt bzw. übermittelt werden? (Dies ist nicht evident, wenn lediglich Datenbankbefehle protokolliert werden.)
Können die Protokolldaten zusammen mit den gespeicherten Daten sichtbar gemacht werden?
- Sind ggf. unterschiedliche Speicherfristen mit folgender Löschung für verschiedenartige Protokolldaten, die aber durch ein System verarbeitet werden, technisch darstellbar (vgl. z. B. § 6 Abs. 4 LDSG und § 8 Abs. 6 DSVO)?
- Wie wird eine unzulässige Verkettung von Protokolldaten verhindert?
- Sind die bereits ergriffenen und die noch zu ergreifenden Maßnahmen im Rahmen der Sicherstellung von Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit nachvollziehbar für die einsetzende Stelle beschrieben?

Komplex 4

Sind die Protokolldaten im Sinne des Komplexes 4 verarbeitbar (selektive Löschung von Einzeldaten, Beauskunftung, Berichtigung, Sperrung, Einwand)? Dies betrifft zum einen die Protokolldaten der zugreifenden Person selbst (in erster Linie Mitarbeiterinnen und Mitarbeiter) als Betroffene, zum anderen die Daten der Betroffenen (Bürgerinnen und Bürger), deren (Primär-)Daten verarbeitet und als Teile der Protokolldaten erhoben, gespeichert und verarbeitet werden.