ips Modul M4 - Datenschutzmanagement, Version 3.5

datenschutz cert GmbH
29. Juli 2020

datenschutz cert

Inhaltsverzeichnis

1. Allgemeines

Im Rahmen der datenschutzrechtlichen Prüfung eines Internet-, Waren- oder Dienstleistungsangebots kommt dem Datenschutzmanagement, also der datenschutzkonformen Organisation des geprüften Unternehmens mit Blick auf den Webservice/das Webportal, besondere Bedeutung zu. Datenschutzmanagement bezeichnet sämtliche Abläufe und Regelungen, die von einem Unternehmen zur Gewährleistung des Datenschutzes getroffen werden einschließlich der Festlegung einer internen Organisation zur Erreichung der Datenschutzziele und -maßnahmen, von Abläufen, Zuständigkeiten, betrieblichen Vorgaben (Richtlinien) sowie der Mittel (Hardware), mit denen diese umgesetzt werden. Das Datenschutzmanagement bewertet also diejenigen Vorkehrungen des Anbieters, die der Nutzer nicht „sieht" bzw. die er selbst nicht überprüfen kann. Aus diesem Grunde kommt den im Modul genannten Anforderungen eine besondere Bedeutung zu:

Während die übrigen, verfahrensbezogenen Module im Wesentlichen die gesetzlichen Anforderungen an die jeweilige Datenverarbeitung abbilden, enthält das Modul Datenschutzmanagement Kriterien hinsichtlich der internen technischen und organisatorischen Vorkehrungen zum Datenschutz und zur Datensicherheit im Unternehmen (bzw. in der Behörde, nachfolgend einheitlich „Unternehmen"). Hierzu zählen zum einen die vorherige Risikoanalyse und -bewertung zur Feststellung der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte der Betroffenen gemäß Art. 32 DSGVO. Zum anderen sind die zur Sicherstellung des Datenschutzes getroffenen technischen und organisatorischen Vorkehrungen gemäß Art 32 DSGVO, insbesondere die in Art. 32 Abs. 1 DSGVO genannten allgemeinen technischen und organisatorischen Sicherheitsmaßnahmen zur Pseudonymisierung, Verschlüsselung, Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit der Systeme, Wiederherstellbarkeit und Verfahren zur Evaluierung der Wirksamkeit der Maßnahmen. Darüber hinaus sind die in Art. 25 DSGVO normierten Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu achten.

Über die Einhaltung dieser Anforderungen hinaus zeichnet sich ein datenschutzrechtlich vorbildliches Unternehmen aber dadurch aus, dass es **mehr** für den Datenschutz unternimmt, als ausdrücklich gesetzlich gefordert ist.

Ein weiterer Anhaltspunkt für eine vorbildliche Datenschutzpraxis ist das Vorhandensein einer unternehmensinternen Datenschutzpolitik: Gibt es eine Datenschutzrichtlinie? Ist gewährleistet, dass die Datenschutzpolitik allen mit dem Umgang mit personenbezogenen Daten befassten Mitarbeitern bekannt ist und von diesen befolgt wird? Hat der Anbieter z.B. für IT-Prozesse oder Services anerkannte Datenschutz-Zertifikate oder –Gütesiegel erhalten?

2. Unternehmensorganisation

2.1. Bestellung eines betrieblichen / behördlichen Datenschutzbeauftragten

2.1.1. Rechtliche Grundlagen

Gemäß Art. 37 Abs. 1 DSGVO haben Behörden und öffentliche Stellen grundsätzlich einen Datenschutzbeauftragten (DSB) zu bestellen, wenn sie personenbezogene Daten verarbeiten, mit Ausnahme von Gerichten im Rahmen ihrer justiziellen Tätigkeit. Dies schließt gemäß § 1 Abs. 1 BDSG-Neu auch öffentliche Stellen ein, die am Wettbewerb teilnehmen. Auch wenn die Kerntätigkeiten des Verantwortlichen die umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen oder die Verarbeitung besonderer Kategorien von Daten (Art. 9 DSGVO) oder Daten über strafrechtliche Verurteilungen von Straftaten umfassen ist ein Datenschutzbeauftragter zu bestellen. Zusätzlich verpflichtet § 38 BDSG-Neu Verantwortliche und Auftragsverarbeiter einen DSB zu bestellen, wenn in der Regel mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Werden Verarbeitungen vorgenommen, die einer Datenschutzfolgenabschätzung (DSFA) unterliegen oder personenbezogene Daten geschäftsmäßig zur anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung bedarf es einer Bestellung eines BSD unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen. Der DSB kann gemäß Art. 37 Abs. 6 DSGVO auch ein Externer sein.

Für die Unternehmen, die Telemedien anbieten, dürften die Voraussetzungen für die Benennungspflicht eines DSB überwiegend gegeben sein. Dies gilt jedenfalls dann, wenn im Rahmen der Internetnutzung Logprotokolle und ähnliche Aufzeichnungen über das persönliche Nutzungsverhalten geführt werden oder wenn entgeltpflichtige Dienste mit personenbezogener Abrechnung angeboten werden.

Der DSB hat gemäß Art. 39 DSGVO die Aufgabe, auf die Einhaltung DSVGO sowie anderer Vorschriften, sowie Strategien des Verantwortlichen über den Datenschutz zu überwachen. Konkret hat er die Aufgaben den Verantwortlichen und die Beschäftigten hinsichtlich ihrer Pflichten zu unterrichten und beraten, Zuständigkeiten zuzuweisen, die Sensibilisierung und Schulung der an der Verarbeitung beteiligten Personen zu überwachen, auf Anfrage im Zusammenhang mit der Datenschutz-Folgeabschätzung zu beraten und die Durchführung zu überwachen, mit der Aufsichtsbehörde zusammenzuarbeiten und ihr als Anlaufstelle zu dienen. Sofern der DSB Angestellter des Verantwortlichen, kann er gemäß Art. 38 abs. 6 DSGVO und § 7 Abs. 2 BDSG-Neu andere Aufgaben wahrnehmen, solange diese nicht zu einem Interessenkonflikt führen. Bei Ausführung dieser Tätigkeiten muss der DSB das mit der Verarbeitung verbundene Risiko mit Blick auf Art, Umfang, Umständen und Zwecken der Verarbeitung berücksichtigen. Er ist von dem Unternehmen über alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Ferner sind ihm alle erforderlichen Ressourcen und Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen.

Der DSB muss die für diese Aufgabe die berufliche Qualifikation und das Fachwissen, dies setzt u.a. voraus, dass er die notwendigen Kenntnisse über das Unternehmen und

seine Organisation, Kenntnisse über die Datenverarbeitung, insbesondere über die eingesetzte Hard- und Software, sowie Kenntnisse hinsichtlich der einschlägigen rechtlichen Vorschriften haben.

Für den Bereich der Telemedien setzt das „Fachwissen" neben den o.g. Qualifikationen insbesondere vertieftes technisches Verständnis und administratoren-ähnliche Kenntnisse von Betriebs- und Dateisystemen voraus. Eine gute Umsetzung der gesetzlichen Anforderungen an die Person und die Aufgabe des betrieblichen Datenschutzbeauftragten zeigt sich insbesondere im ständigen Wissenszuwachs des Betreffenden: soweit interne Mitarbeiter für diese Position eingesetzt werden, haben diese anfangs oft nicht alle der erforderlichen Qualifikationen, sondern müssen sich diese im Laufe der Zeit erst aneignen. In der Aufgabenwahrnehmung ist der DSB weisungsfrei (Art. 38 Abs, 3 DSGVO und § 6 Abs. 3 Satz 1 BDSG-Neu). Er kann also nicht von der Unternehmensleitung angewiesen werden, bestimmte Aufgaben nicht oder zu einem späteren Zeitpunkt anzugehen oder andere Aufgaben bevorzugt oder in bestimmter Weise zu erledigen. Der DSB ist in seiner Funktion dem Behördenleiter bzw. Geschäftsführer / Vorstand direkt zu unterstellen (Art. 38 Abs. 3 S. 2 DSGVO).

2.1.2. Fragen

- Sind die gesetzlichen Voraussetzungen für die Bestellungspflicht eines DSB gegeben, denn es handelt sich um eine Verarbeitung
  - durch eine öffentliche Stelle oder Behörde?
  - die hauptsächlich die umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen umfassen?
  - welche hauptsächlich besondere Kategorien von Daten oder Daten über strafrechtliche Verurteilungen von Straftaten umfasst?
  - die einer Datenschutzfolgenabschätzung unterliegt?
  - die die geschäftsmäßige anonymisierte Übermittlung personenbezogener Daten umfasst?
  - Zwecken der Markt- und Meinungsforschung dient?
  - 10 Mitarbeiter, die mit der automatisierten personenbezogenen DV befasst sind?
- Ist ein DSB bestellt?
- Ist die Bestellung schriftlich erfolgt?
- Werden ggf. Meldepflichten gegenüber der Datenschutzaufsichtsbehörde bzw. dem/der LfDI erfüllt?
- Ist die Unabhängigkeit des DSB in seiner Aufgabenwahrnehmung gewährleistet?
- Wie ist der DSB in die Unternehmensorganisation eingebunden? Welche anderen Aufgaben hat er wahrzunehmen?
- Existieren für den DSB eine Stellbeschreibung bzw. bei externen DSB vertragliche Festlegungen der wahrzunehmenden Aufgaben?
- Besitzt der DSB die erforderliche Fachkunde (technische und rechtliche Kenntnisse) und Zuverlässigkeit/ berufliche Qualifikation und das Fachwissen?

- Wird dem (internen) DSB ausreichend Arbeitszeit für die Wahrnehmung seiner Aufgaben zur Verfügung gestellt?
- Werden dem DSB die nötigen Arbeitsmittel (Räume, Einrichtungen etc.) bzw. Hilfspersonal zur Verfügung gestellt?
- Wird der DSB in geplante Änderungen bei der Datenverarbeitung mit einbezogen/ alle Fragen mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden?
- Wird der DSB entsprechend geschult (Fortbildungen, Seminare, Arbeitsgruppen)?
- Wie kontrolliert der DSB die ordnungsgemäße Anwendung von DV-Programmen? Prüft der DSB den Umgang mit personenbezogenen Daten?
- Wird der DSB von der Unternehmensleitung rechtzeitig über Vorhaben zur Verarbeitung personenbezogener Daten unterrichtet?
- Ist gewährleistet, dass der DSB gemäß Art. 35 DSGVO erforderliche Datenschutz-Folgenabschätzung durchführt?
- Wird dem DSB die Übersicht (Art. 39 Abs. 1 lit. c DSGVO und § 7 Abs. 1 Nr. 3 BDSG-Neu) zur Verfügung gestellt?
- Gewährleistet der DSB die datenschutzrechtliche Unterrichtung, Schulung und Sensibilisierung der Mitarbeiter?
- Nimmt der DSB eine Risikokoordinierung vor?

2.1.3. Bewertung

0 Punkte: die gesetzlichen Anforderungen sind nicht oder nur unzureichend umgesetzt

- es ist kein DSB bestellt
- es ist zwar ein DSB bestellt, eine Wahrnehmung seiner Aufgaben findet aber nicht statt (DSB ist nur pro Forma bestellt)
- der DSB ist zwar bestellt, ihm wird aber keine Arbeitszeit zur Wahrnehmung seiner Aufgaben eingeräumt
- der DSB besitzt nicht die erforderlichen rechtlichen oder technischen Kenntnisse
- die Unabhängigkeit des DSB ist nicht gewährleistet
- erforderliche Datenschutz-Folgeabschätzungen finden nicht statt
- der DSB erhält keine Kenntnis von dem Verzeichnis von Verarbeitungstätigkeiten

1 Punkt: die gesetzlichen Anforderungen sind nicht vollständig umgesetzt

- die Unabhängigkeit des DBS ist nicht abgesichert
- dem DSB wird nur unzureichende Arbeitszeit zur Wahrnehmung seiner Aufgaben eingeräumt
- der DSB hat nur geringe technische oder rechtliche Kenntnisse, Schulungen oder Fortbildungen sind unzureichend
- der DSB erhält nur lückenhaft von neuen DV-Verfahren mit Personenbezug Kenntnis

- der DSB erhält nur unvollständige bzw. inaktuelle Kenntnis von dem Verfahrensverzeichnis

2 Punkte: die Bestellung des DSB erfüllt die gesetzlichen Anforderungen

- der DSB ist bestellt und nimmt seine Aufgaben mit dem erforderlichen zeitlichen Aufwand wahr
- die vom DSB geforderten Maßnahmen zur Gewährleistung des Datenschutzes werden im Regelfall zeitnah umgesetzt
- der DSB hat die technische und rechtliche Fachkunde und Zuverlässigkeit
- der DSB bildet sich entsprechend fort, erforderliche Arbeitsmittel werden zur Verfügung gestellt
- es ist ein externer DSB bestellt, dessen Auftragsvolumen die Wahrnehmung der Aufgaben zulässt
- der DSB schult und sensibilisiert die Mitarbeiter

3 Punkte: die Bestellung des DSB ist vorbildlich umgesetzt

- der DSB hat vertiefte, über sein engeres Aufgabengebiet hinausgehende aktuelle technische und rechtliche Kenntnisse zur Gewährleistung des Datenschutzes
- Der DSB führt regelmäßig datenschutzrechtliche Prüfungen im Unternehmen durch
- der DSB kann sich regelmäßig (mind. 1x pro Quartal) im Rahmen von Fortbildungsveranstaltungen schulen lassen
- der DSB hält regelmäßigen Kontakt zur Aufsichtsbehörde
- der DSB hat gute didaktische Fähigkeiten zur Vermittlung datenschutzrechtlicher Informationen
- der DSB wird aktiv in die datenschutzrechtliche Zertifizierung bzw. Auditierung einbezogen

2.2. Auftragsverarbeitung

2.2.1. Rechtliche Grundlagen

Gemäß Art. 28 DSGVO sind in dem Fall, dass personenbezogene Daten im Auftrag durch andere Stellen verarbeitet werden, konkrete Vorgaben durch sowohl Auftraggeber (AG), als auch Auftragnehmer (AN) zu beachten. Eine solche Auftragsverarbeitung liegt immer dann vor, wenn die beauftragte Stelle die Daten ausschließlich für fremde Zwecke verarbeitet. Abzugrenzen hiervon ist eine Datenverarbeitung, bei der die beauftragte Stelle die Daten eigenverantwortlich für bestimmte eigene Zwecke verarbeitet (Funktionsübertragung). Bei der Auftragsverarbeitung verbleibt die datenschutzrechtliche Verantwortlichkeit bei dem AG, während bei der Funktionsübertragung die datenschutzrechtliche Verantwortlichkeit (auch oder ausschließlich) bei der Stelle liegt, der die Aufgabenwahrnehmung übertragen wurde. Ob es sich im konkreten Fall um Auftragsverarbeitung oder um eine Funktionsübertragung handelt, hängt sowohl von den tatsächlichen Verhältnissen als auch von der Vertragsgestaltung zwischen den

beteiligten Stellen ab. So kann es sich beim Web Hosting sowohl um Auftragsverarbeitung als auch um Funktionsübertragung handeln. Wartung oder Fernwartung von insbesondere IT-Strukturen durch externe Dienstleister fällt jedoch, soweit ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, ebenfalls unter die Auftragsverarbeitung.

Ein Auftragsverarbeiter kann auch als Verantwortlicher gelten, wenn er gemäß Art. 28 Abs. 10 DSGVO über die Zwecke und Mittel der Verarbeitung bestimmt. In diesem Fall treffen ihn dieselben Pflichten wie einen Verantwortlichen. Sind Mehrere gemeinsam verantwortlich müssen sie gemäß Art. 26 DSGVO festlegen, wer welche Verpflichtungen der DSGVO erfüllt (Joint Control-Vertrag). Dies betrifft insbesondere die Informationspflichten aus Art. 13, 14 DSGVO.

Bei der Auftragsverarbeitung trifft den Auftraggeber die Pflicht, den Aufragnehmer sorgfältig unter Berücksichtigung der bei ihm gegebenen technischen und organisatorischen Sicherheitsmaßnahmen auszuwählen und ihn während der Dauer des Auftrags zu überwachen. Die Kontrollpflicht des Verantwortlichen, die sich aus Art. 25 Abs. 1 S. 2 und Art. 5 Abs. 2 DSGVO, umfasst auch die Kontrolle der technischen Maßnahmen beim Auftragsverarbeiter. Die Kontrolle ist regelmäßig durchzuführen sowie VOR der erstmaligen Datenverarbeitung des Auftragnehmers. Als vorbildlich erweist es sich, sofern der Auftragnehmer der Datenverarbeitung eine nachhaltige und aussagekräftige Zertifizierung seiner Auftragsverarbeitung aufweisen kann. Dies kann z.B. eine Zertifizierung gemäß ISO 27001 des beauftragten Rechenzentrums sein.

Der Auftragsverarbeiter ist verpflichtet ein Verzeichnis über die Verarbeitungstätigkeiten zu führen.

Da der Auftraggeber trotz der Delegation für die ordnungsgemäße Datenverarbeitung verantwortlich bleibt, hat er gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht (Art. 29 DSGVO).

Die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter erfolgt gemäß Art. 28 Abs. DSGVO auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments in Schriftform – dies kann auch elektronisch geschehen. Dieser beinhaltet die folgenden Aspekte:

ANFORDERUNG	REFERENZ
Gegenstand und Dauer des Auftrags, Art und Zweck der vorgesehenen Verarbeitung die Art der personenbezogenen Daten Kategorien betroffener Personen und Pflichten und Rechte des Verantwortlichen	Art. 28 Abs. 3 Satz 1 DSGVO
Verarbeitung personenbezogener Daten ausschließlich basierend auf Weisung des Verantwortlichen	Art. 28 Abs. 3 Satz 2 Buchstabe a DSGVO
die Pflicht den Verantwortlichen über Ausnahmen von der Weisungspflicht auf Grund von Rechtsvorschriften zu informieren	Art. 28 Abs. 3 Satz 2 Buchstabe a DSGVO

Die Gewährleistung, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen	Art. 28 Abs. 3 Satz 2 Buchstabe b DSGVO
Die gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen	Art. 28 Abs. 3 Satz 2 Buchstabe c DSGVO
Die Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters	Art. 28 Abs. 3 Satz 2 Buchstabe d DSGVO
Die Verpflichtung den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten Mitteln, technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Betroffenenrechte nachzukommen	Art. 28 Abs. 3 Satz 2 Buchstabe e DSGVO
Die Gewährleistung, dass der Auftragsverarbeiter unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt	Art. 28 Abs. 3 Satz 2 Buchstabe f DSGVO
Löschung oder Rückgabe personenbezogener Daten nach Abschluss der Erbringung der Verarbeitungsleistungen sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht	Art. 28 Abs. 3 Satz 1 DSGVO
Die Zurverfügungstellung aller erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten Ermöglichung von und Beitrag zu Überprüfungen, einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden	Art. 28 Abs. 3 Satz 2 Buchstabe a DSGVO
Mitteilungspflicht des Auftragsverarbeiters an den Verantwortlichen, falls er der Auffassung ist, dass eine Weisung gegen die EU_DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten	Art. 28 Abs. 3 Satz 2 Buchstabe a DSGVO

Tabelle Anforderungen Auftragsverarbeitungs-Vertrag

Eine gute bzw. vorbildliche Umsetzung der Vorschriften der DSGVO zur Auftragsverarbeitung in der Praxis drückt sich durch eine vertrauensvolle Zusammenarbeit zwischen Auftragnehmer und Auftraggeber aus. Dies beinhaltet u.a., dass der Auftraggeber nicht nur über die Datenverarbeitungsvorgänge und entsprechenden Sicherheitsvorkehrungen beim Auftragnehmer informiert ist, sondern auch aktiv darauf Einfluss nehmen kann, sei es durch konkrete Vorgaben gegenüber dem Auftragnehmer oder durch gemeinsame Maßnahmen zur Verbesserung des Datenschutzes.

2.2.2. Fragen

- Bedient sich die verantwortliche Stelle zur Verarbeitung personenbezogener Daten eines Dritten? Handelt es sich dabei um Verarbeitung personenbezogener Daten im Auftrag oder um Funktionsübertragung?
- Sind die Verantwortlichkeiten der beteiligten Stellen hinsichtlich der Verarbeitung personenbezogener Daten schriftlich im Sinne der Vorgaben des Art. 28 DSGVO (oder anderer anwendbarer Normen zur Auftragsverarbeitung) festgelegt?
- Ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt worden?
- Werden Aufträge zur Verarbeitung personenbezogener Daten schriftlich erteilt?
- Entspricht der Auftrag den gesetzlichen Vorgaben (insbesondere Festlegung der Datenerhebung, -Verarbeitung und -Nutzung, technischer und organisatorischer Maßnahmen und etwaiger Unterauftragsverhältnisse)?
- Werden Weisungen gegenüber dem Auftragnehmer durchgesetzt?
- Sind Rechtsfolgen an die Nichtdurchführung von Weisungen des Auftraggebers geknüpft (z. B. Konventionalstrafen)?
- Überzeugt sich der Auftraggeber von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen und kommt seiner Kontrollpflicht nach?
- Hat der Auftragnehmer aussagekräftige und anerkannte Zertifikate zur IT-Sicherheit oder Auftragsverarbeitung erworben?
- Wird die Durchführung der Auftragsverarbeitung durch den Auftragnehmer vom Auftraggeber kontrolliert? Gibt es regelmäßige Berichte / Reports durch den Auftragnehmer?
- Wird der Auftraggeber über Änderungen in der Datenverarbeitung und über geänderte technische und organisatorische Maßnahmen beim Auftragnehmer informiert?

2.2.3. Bewertung

0 Punkte: die gesetzlichen Vorgaben sind gar nicht bzw. grob unvollständig umgesetzt

- das Auftragsverhältnis ist nicht schriftlich geregelt
- der Auftraggeber ist über die technischen und organisatorischen Maßnahmen beim Auftragnehmer nicht informiert
- es liegt ein Auftragsverhältnis vor, die gesetzlichen Regelungen/ Verantwortlichkeiten sind dem Auftraggeber aber nicht bekannt
- der Auftraggeber hat sich bei der Auswahl des Auftragnehmers nicht von der Gewährleistung angemessener technische und organisatorischer Maßnahmen zur Gewährleistung des Datenschutzes überzeugt
- der Auftragnehmer weicht in wesentlichen Punkten in der täglichen Praxis von den vertraglichen Vorgaben bzw. Aufträgen ab

1 Punkt: die Umsetzung der gesetzlichen Vorgaben weist Defizite auf

- es gibt zwar schriftliche Vereinbarungen, diese weisen jedoch Lücken auf (z. B. unvollständige Nennung von Unterauftragsverhältnissen)
- die Einhaltung der schriftlichen Vorgaben wird nicht ausreichend kontrolliert
- es gibt zwar umfassende schriftliche Vereinbarungen, diese werden jedoch nicht vollständig umgesetzt
- der Auftragnehmer weicht in der täglichen Praxis teilweise von den vertraglichen Vorgaben bzw. Aufträgen ab

2 Punkte: die gesetzlichen Vorgaben werden eingehalten

- die vertraglichen Vereinbarungen beinhalten die gesetzlich vorgesehenen Mindestanforderungen (z.B. Beschreibung der umgesetzten technischen und organisatorischen Maßnahmen)
- Vorgaben des Auftraggebers werden mit dem Auftragnehmer abgestimmt und umgesetzt
- der Auftraggeber ist über die technischen und organisatorischen Einrichtungen des Auftraggebers informiert
- Die Kontrolle wird regelmäßig durchgeführt

3 Punkte: die gesetzlichen Vorgaben werden vorbildlich umgesetzt

- zusätzlich bzw. anstatt des unter 2. Genannten:
  - finden regelmäßige Absprachen zwischen Auftragnehmer und Auftraggeber über aktuelle datensicherheitstechnische Themen und evtl. Verbesserungen der Datenverarbeitung statt
  - Der Auftragnehmer legt regelmäßig einen Datenschutzaudit-Bericht o.Ä. vor.
  - Der Auftragnehmer ist bezogen auf die hier geprüfte Dienstleistung nach einem anerkannten Standard zertifiziert (insb. ISO 27001, IT-Grundschutz, Datenschutz-Audit nach Datenschutzgütesiegelverordnung Schleswig-Holstein etc.)

2.3. Verzeichnis von Verfahrenstätigkeiten

2.3.1. Rechtliche Grundlagen

Gemäß Art. 30 DSGVO muss jeder Verantwortlicher oder gegebenenfalls sein Vertreter alle Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen, in einem Verzeichnis zusammenfassen, es sei denn das Unternehmen oder die Einrichtung beschäftigt weniger 250 Mitarbeiter sofern die Verarbeitung kein Risiko für die Rechte der Betroffenen birgt und nur gelegentlich erfolgt. Von der Pflicht kann nicht abgesehen werden, wenn die Verarbeitung sensible Daten oder Daten über strafrechtliche Verurteilungen und Straftaten i.S.d. Art. 10 DSGVO betrifft. Die Mindestangaben für dieses Verzeichnis umfassen:

1. Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

2. die Zwecke der Verarbeitung;
3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
4. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
5. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Absatz 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
6. (wenn möglich), die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
7. (wenn möglich), eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Absatz 1 DSGVO.

Darüber hinaus sind Auftragsverarbeiter verpflichtet ein Verzeichnis über die im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen, welches die folgenden Angaben enthält:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
2. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
3. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
4. (wenn möglich), eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Absatz 1 DSGVO.

Für jedes Verfahren automatisierter Datenverarbeitung, die unterschiedlichen Zwecken dient – wie etwa Vertragsverarbeitungen, Werbedateien, Personaldatenverarbeitung, Finanzbuchhaltung etc. – sind die entsprechenden Angaben im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

2.3.2. Fragen

- Existiert ein Verzeichnis der Verarbeitungstätigkeiten?
- Entfällt die Pflicht ein Verzeichnis der Verarbeitungstätigkeiten zu führen, weil weniger als 250 Mitarbeiter beschäftigt sind und keine regelmäßige oder kritische Verarbeitung stattfindet?

- Enthält das Verzeichnis der Verarbeitungstätigkeiten die gesetzlichen Mindestangaben?
- Sind die im Verzeichnis der Verarbeitungstätigkeiten angegebenen Informationen zutreffend, stimmt die tägliche Praxis mit den dortigen Angaben überein?
- Sind die Zwecke der Datenverarbeitung genannt?
- Sind Löschfristen aufgeführt?
- Wird das Verzeichnis der Verarbeitungstätigkeiten in regelmäßigen Abständen bei
  - veränderten Unternehmensbedingungen
  - veränderten Risiken aktualisiert?
- Sind die im Verzeichnis der Verarbeitungstätigkeiten genannten Informationen den mit der DV betrauten Mitarbeitern bekannt?
- Werden die Angaben gemäß Art. 30 Abs. 4 DSGVO der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt?
- Stellt im Falle einer Auftrags-DV der Auftragnehmer dem Verantwortlichen die Angaben zur Erfüllung seiner Kontrollpflicht zur Verfügung?

2.3.3. Bewertung

0 Punkte: die gesetzlichen Vorgaben sind nicht eingehalten

- ein Verzeichnis der Verarbeitungstätigkeiten besteht nicht
- das Unternehmen oder die Einrichtung beschäftigt zwar weniger als 250 Mitarbeiter, führt aber regelmäßig oder kritische Verarbeitungen durch
- das Verzeichnis der Verarbeitungstätigkeiten ist grob unvollständig
- die gesetzlichen Meldepflichten gegenüber der Datenschutz-Aufsichtsbehörde werden nicht erfüllt

1 Punkt: die Umsetzung der gesetzlichen Vorgaben weist Defizite auf

- es besteht ein Verzeichnis der Verarbeitungstätigkeiten, dies ist aber entweder veraltet oder weist Lücken oder sonstige Defizite auf
- ein Verzeichnis der Verarbeitungstätigkeiten existiert, dies ist aber bei den verantwortlichen Mitarbeitern nicht bekannt
- ein Verzeichnis der Verarbeitungstätigkeiten existiert, die Praxis im Unternehmen weicht jedoch erheblich von den dortigen Angaben ab
- der Verantwortliche führt ein Verzeichnis gemäß den gesetzlichen Anforderungen aber sein Auftragsverarbeiter nicht
- der Verantwortliche führt ein Verzeichnis gemäß den gesetzlichen Anforderungen aber sein Auftragsverarbeiter stellt dem Verantwortlichen die Angaben nicht zur Verfügung

2 Punkte: die gesetzlichen Vorgaben sind eingehalten

- das Verzeichnis der Verarbeitungstätigkeiten ist vollständig und aktuell
- die verantwortlichen Mitarbeiter kennen das Verfahrensverzeichnis

- die Praxis stimmt mit den Angaben des Verzeichnisses der Verarbeitungstätigkeiten überein

3 Punkte: die gesetzlichen Vorgaben werden vorbildlich umgesetzt

- obwohl keine Pflicht zum Führen eines Verzeichnisses der Verarbeitungstätigkeiten besteht wird eines geführt
- das Verzeichnis der Verarbeitungstätigkeiten enthält mehr als die gesetzlich erforderlichen Angaben
- es gibt eine über die notwendigen Angaben des Verfahrensverzeichnisses hinausgehende (interne) Datenschutzerklärung
- das Verfahrensverzeichnis bzw. die Datenschutzerklärung werden regelmäßig aktualisiert
- die Mitarbeiter sind über den jeweils aktuellen Stand des Verzeichnisses der Verarbeitungstätigkeiten informiert
- die Angaben aus dem Verzeichnis der Verarbeitungstätigkeiten werden im Internet zum Abruf zur Verfügung gestellt

2.4. Datenschutzfolgeabschätzung

2.4.1. Rechtliche Grundlagen

Unter den Vorgaben des Art. 35 DSGVO bedarf es einer Datenschutzfolgeabschätzung (DSFA). Dies umfasst insbesondere Fälle der systematischen Bewertung persönlicher Aspekte die auf automatisierte Verarbeitung (einschließlich Profiling) beruht, wie etwa die Ablehnung eines Vertragsschlusses auf Grund eines vorhergehenden Scorings. Auch bei einer umfangreichen Verarbeitung besonderer personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO muss eine Datenschutz-Folgenabschätzung vorgenommen werden, da hier hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Wird keine DSFA durchgeführt, so ist auch dies zu begründen.

2.4.2. Fragen

- Ist eine Datenschutzfolgeabschätzung nach Art. 35 für die Individual-Dienstleistung notwendig und falls ja, wurde sie durchgeführt?
- Wird die Prüfung dokumentiert und das Ergebnis begründet?

2.4.3. Bewertung

0 Punkte: Anwendbare Rechtsvorschriften wurden nicht beachtet

- eine Datenschutzfolgeabschätzung war notwendig, fand aber nicht statt
- das Prüfungsergebnis enthält grobe Fehler in der Einordnung der rechtlichen Zulässigkeit der Datenverarbeitung

1 Punkt: Von den gesetzlichen Vorgaben wird geringfügig abgewichen

- das Verfahren wurde nur oberflächlich durchgeführt
- das Ergebnis enthält leichtere Mängel

- Prüfung und Ergebnis wurden nicht dokumentiert

2 Punkte: die anwendbaren Rechtsvorschriften werden eingehalten

- das Verfahren wurde ordnungsgemäß geprüft und schriftlich bewertet
- Es liegt eine begründete und detaillierte Stellungnahme, z.B. des Datenschutzbeauftragten vor

3 Punkte: Es werden zusätzliche, über das gesetzlich vorgeschriebene Maß hinausgehende Maßnahmen getroffen

- Über die Voraussetzungen des zuvor genannten Punktes hinaus werden zusätzliche Maßnahmen getroffen, z.B.
- Das Prüfungsergebnis ist öffentlich einsehbar

2.5. Betriebliche Organisation

2.5.1. Rechtliche Grundlagen

Unter dem Punkt „Betriebliche Organisation“ sind vorliegend die sonstigen gesetzlichen Anforderungen zusammengefasst, deren Einhaltung die „Datenschutz-kultur“ des auditierten Unternehmens vervollständigen. Die Kriterien betreffen zum Teil die durch die Geschäftsleitung vorgegebene Organisation selbst, zum Teil auch die dem betrieblichen Datenschutzbeauftragten obliegenden Pflichten. Da eine „Datenschutzkultur“ jedoch nicht allein durch gesetzliche oder unternehmerische Vorgaben entsteht, ist nicht zuletzt die persönliche Einstellung der Mitarbeiter zum Thema Datenschutz ausschlaggebend für die Beurteilung der Unternehmensorganisation aus datenschutzrechtlicher Sicht insgesamt.

Von besonderer Bedeutung sind in diesem Zusammenhang systematische Regelungen zum Umgang mit personenbezogenen Daten (Datenschutzpolitik bzw. Privacy Policy). Diese Regelungen richten sich zum einen an die Mitarbeiter, die mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten erfasst sind; zum anderen haben sie zentrale Bedeutung für die Gewährleistung der Transparenz gegenüber Nutzern elektronischer Dienstleistungen. Die Datenschutzpolitik soll dem Nutzer die Entscheidung darüber erleichtern, ob er dem Unternehmen im konkreten Fall personenbezogene Daten offenbart.

Die Entwicklung einer Datenschutzpolitik gibt dem Unternehmen die Chance, selbst ein klares Bild von seinem eigenen Umgang mit personenbezogenen Daten zu gewinnen. Soweit die Datenschutzpolitik eines Unternehmens im Internet veröffentlicht wird, bietet es sich an, diese Informationen standardisiert auszuwerten und mit Nutzerpräferenzen in Verbindung zu bringen. Dies ist das Anliegen des Plattform for Privacy Preferences Project (P3P).

2.5.2. Fragen

- Wirkt der DSB bei der Auswahl der für die Datenverarbeitung vorgesehenen Mitarbeiter mit?
- Sind alle mit der Datenverarbeitung betrauten Mitarbeiter auf die Einhaltung des Datenschutzes und die Vertraulichkeit verpflichtet oder belehrt worden?

- Gibt es Dienstanweisungen für die das Thema Datenschutz betreffenden Fragen?
- Erfolgen regelmäßig Schulungen zu allgemeinem Datenschutz und jeweils aktuellen datenschutzrechtlichen Themen?
- Sind Geschäftsbereiche / Mitarbeiter, soweit unterschiedliche Datenarten verarbeitet werden, auch organisatorisch getrennt?
- Gibt es Regelungen für die Behandlung ausscheidender Mitarbeiter?
- Wie ist die persönliche Einstellung der Mitarbeiter zum Thema Datenschutz? Herrscht eine angemessene Sensibilität? Wird Datenschutz als notwendiges Übel bzw. Arbeitshindernis verstanden?
- Gibt es eine Datenschutzpolitik / interne Richtlinien?
- Ist die Datenschutzpolitik umfassend? Umschreibt sie sämtliche wesentlichen Aspekte des Umgangs mit personenbezogenen Daten?
- Wird die Datenschutzpolitik im Internet veröffentlicht?
- Ist die Datenschutzpolitik P3P-kompatibel?
- Entspricht die Datenschutzpolitik der betrieblichen Praxis?

2.5.3. Bewertung

0 Punkte: die betriebliche Organisation lässt Datenschutzaspekte unberücksichtigt

- Mitarbeiter sind nicht auf die Einhaltung des Datenschutzes verpflichtet oder nachweisbar belehrt worden
- Mitarbeiter sind nicht über die gesetzlichen Anforderungen zum Datenschutz informiert
- verschiedene Datenarten werden einheitlich und ohne Trennung verarbeitet
- der betriebliche Datenschutzbeauftragte wird seinen Aufgaben nicht gerecht
- es gibt keine betriebsinternen Vorgaben oder ähnliche Arbeitshilfen zum Datenschutz und keine Datenschutzpolitik
- die betriebliche Praxis weicht in wesentlichen Punkten von der veröffentlichten Datenschutzpolitik ab.

1 Punkt: Datenschutzaspekte werden in der betr. Organisation berücksichtigt, sind aber verbesserungsbedürftig

- die Mitarbeiter sind auf einmalig auf die Einhaltung des Datenschutzes verpflichtet bzw. nachweisbar belehrt worden, eine weitere Schulung bzw. Information fand aber nicht mehr statt
- es bestehen betriebsinterne Vorgaben, diese sind aber entweder nicht umfassend bekannt oder werden aus sonstigen Gründen nicht umgesetzt
- die bestehenden betriebsinternen Vorgaben werden wg. des verbundenen Arbeitsaufwandes nicht eingehalten
- die betriebliche Praxis weicht teilweise von der Datenschutzpolitik ab

2 Punkte: datenschutzrechtliche Belange sind in der betrieblichen Organisation angemessen berücksichtigt worden

- die Mitarbeiter sind auf die Einhaltung des Datenschutzes verpflichtet bzw. nachweisbar belehrt worden
- es finden regelmäßige Schulungen zum Datenschutz statt
- die Mitarbeiter sind für das Thema Datenschutz sensibilisiert
- die wesentlichen datenschutzrechtlichen Aspekte sind verbindlich geregelt; die Einhaltung der Vorgaben wird angemessen kontrolliert

3 Punkte: datenschutzrechtliche Belange sind in der betrieblichen Organisation vorbildlich berücksichtigt worden

- der DSB wird in alle Entscheidungen zum Thema Datenverarbeitung mit einbezogen
- zusätzlich zur Verpflichtung / Belehrung gibt es ausführliche Dienstanweisungen, die in der Praxis auch umgesetzt werden
- es finden regelmäßige Schulungen zum Datenschutz statt
- die wesentlichen datenschutzrechtlichen Aspekte sind verbindlich in einer umfassenden Datenschutzpolitik geregelt; die Einhaltung der Vorgaben wird angemessen kontrolliert;
- die Datenschutzpolitik wird im Internet veröffentlicht und ist P3P-kompatibel
- es werden Nachweise durch Verhaltensregeln oder Zertifizierungen i.S.d. Art. 40ff DSGVO erbracht

3. Technische und organisatorische Maßnahmen

3.1. Rechtliche Grundlagen

Wer personenbezogene Daten erhebt, verarbeitet oder nutzt, hat dafür Sorge zu tragen, dass die Datenschutzvorschriften eingehalten werden. Neben der inhaltlichen Gestaltung der Datenverarbeitungsprozesse kommt es darauf an, die technischen Systeme so zu gestalten und zu betreiben, dass die Daten nur in dem zulässigen Rahmen verwendet werden. Dies ist gemäß Art. 5 DSGVO durch technische und organisatorische Maßnahmen abzusichern. Dabei sind insbesondere die Grundsätze des Datenschutzes durch Technik (data protection by Design) und benutzerfreundliche Voreinstellungen (data protection by Default) gemäß Art. 25 DSGVO zu beachten.

Art. 32 DSGVO enthält die allgemeinen Maßnahmen, die den Unternehmen zur Erreichung eines einheitlichen gesetzlichen Mindeststandards an Datensicherheit die Einrichtung von technischen und organisatorischen Sicherheitsmaßnahmen auferlegen, ihnen aber hinsichtlich der Ausgestaltung dieser Maßnahmen mit Rücksicht auf die jeweiligen finanziellen und organisatorischen Ressourcen einen gewissen Spielraum lassen. Die Vorgaben zu den Sicherheitsmaßnahmen sind aus diesem Grunde allgemein gefasst und überlassen der verantwortlichen Stelle die konkrete Ausgestaltung. Auf Grund des Verhältnismäßigkeitsgrundsatzes aus Art. 24 DSGVO hat jedes Unternehmen für jede Maßnahme zu prüfen, wie sensibel die zu verarbeitenden Daten sind und mit welcher Intensität sie genutzt und verarbeitet werden. Gegenüberzustellen sind damit technischer und personeller (= finanzieller)

Aufwand sowie das erforderliche Schutzniveau, wobei insbesondere die Schutzinteressen des Betroffenen zu berücksichtigen sind.

Bei der Bewertung der technischen und organisatorischen Maßnahmen ist nicht nur die Gewährleistung der einzelnen in Art. 32 DSGVO genannten Maßnahmen maßgeblich; entscheidend ist vielmehr ihr Zusammenspiel. Zur Vermeidung von Sicherheitslücken ist es deshalb von entscheidender Bedeutung, dass die Schutzbedarfe und Gefährdungen für die personenbezogenen Daten und die Datenverarbeitungsverfahren systematisch untersucht und bewertet werden (Risikoanalyse). Auf Basis der Risikoanalyse müssen Schutzkonzepte erstellt werden, die ein angemessenes Schutzniveau für die verarbeiteten personenbezogenen Daten gewährleisten. Die erforderlichen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO umfassen die Pseudonymisierung und Verschlüsselung, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Anmerkung zur nachfolgenden Bewertung:

Bei den nachfolgend aufgeführten technischen und organisatorischen Sicherheitsmaßnahmen sind im Gegensatz zu den bisherigen gesetzlichen Anforderungen auf Grund der Vielzahl möglicher Szenarien die Mindestanforderungen nicht explizit genannt. Es ist daher Aufgabe des Gutachters, festzustellen, ob Mindestsicherheitsanforderungen im Unternehmen erfüllt sind. Soweit sich die umgesetzten Sicherheitsmaßnahmen überwiegend im Bereich von 0 bis 1 Punkt bewegen, bleibt es dem Gutachter überlassen, die Mindestanforderungen als nicht erfüllt anzusehen und eine Zertifizierung erst dann vorzunehmen, wenn grobe Mängel behoben sind.

Liegen sicherheitsrelevante, anerkannte und gültige Zertifikate vor (z.B. ISO 27001, IT-Grundschutz eines Rechenzentrums, in denen die Webserver untergebracht sind), dann kann auf die nachweisbaren Ergebnisse auch verwiesen werden.

3.2. Fragen

Datenschutz durch Technikgestaltung (Art. 25 Abs. 1 DSGVO)

Datenschutz durch Technikgestaltung meint die proaktive Verankerung von datenschutzrechtlichen Grundsätzen in Systemen zur Datenverarbeitung. Datenschutzanforderungen sollen schon bei der Entwicklung und dem Einsatz von IT-Systemen berücksichtigt werden. Das Ziel ist die Minimierung von Risiken für personenbezogene Daten. Zu den möglichen Maßnahmen zählen solche technischer als auch organisatorischer Natur, etwa die Durchführung einer Datenschutzfolgeabschätzung oder Pseudonymisierung.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Datenschutzfreundliche Voreinstellungen ermöglichen dem Nutzer, ohne weitere Einstellungen vornehmen zu müssen, ein möglichst hohes Maß an Datenschutz. Dies kann erreicht werden durch Datensparsamkeit, sichere Nutzer-Authentifizierungslösungen, Anonymisierung und Pseudonymisierung.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Unternehmen haben Maßnahmen zu treffen, durch die Unbefugten der Zutritt zu Datenverarbeitungsanlagen verwehrt wird. Die Maßnahmen zur Sicherung der Vertraulichkeit erfassen damit Sicherheitsmaßnahmen, um den räumlichen Bereich rund um Datenverarbeitungsanlagen vor dem (körperlichen) Zutritt Unbefugter zu schützen.

Zugangskontrolle

Durch die für Telemedien obligatorische Anbindung der internen Datenverarbeitungssysteme an das Internet drohen aus dieser Richtung erhebliche Risiken für die Sicherheit und Vertraulichkeit der personenbezogenen Daten: durch Einschleusen von Viren, Trojanischen Pferden und ähnlichen Dateien oder durch das bloße Eindringen (Hacken) in die Datenverarbeitungs-anlagen von außen können Daten unbefugt gelöscht, verändert, gelesen oder vervielfältigt werden, dies u.U. sogar ohne oder erst mit verspäteter Kenntnis der verantwortlichen Stelle. Aus diesem Grund sind an die gemäß geforderte Zugangskontrolle aus Datensicherheitsgründen die höchsten Anforderungen zu stellen, die Qualität der Zugangskontrolle bestimmt im Wesentlichen die Qualität der Datensicherheit im Unternehmen insgesamt. Die Zugangskontrolle umfasst jedoch nicht nur Schutzmaßnahmen gegen Gefahren, die von „außen“ drohen, sondern erfordert daneben auch Sicherheitsvorkehrungen gegen den internen unbefugten Zugang. Auch wenn Schäden durch internen Missbrauch nicht in der gleichen Weise publik werden wie das Eindringen oder Lahmlegen von EDV-Systemen bekannter Unternehmen durch Angriffe von außen, sind die bestehenden Risiken durch internen Missbrauch mindestens ebenso hoch.

Zugriffskontrolle

Die Zugriffskontrolle betrifft die Einrichtung von Sicherheitsmaßnahmen, die die DV-Anlagen gegen den unbefugten Zugriff grds. Berechtigter schützen. Zentrales Merkmal solcher Schutzmaßnahmen sind Berechtigungskonzepte (abgestufte Zugangskennungen mit entsprechendem Passwort). Teilweise überschneiden sich die u.g. Anforderungen mit denen der Zugangskontrolle, da bspw. ein zur Bearbeitung von Bestandsdaten Berechtigter bei einem Zugriffsversuch auf Abrechnungsdaten zum Unbefugten „mutiert“ und die Unterscheidung zwischen berechtigtem und unberechtigtem Zugriff damit nur objektbezogen getroffen werden kann.

Trennungskontrolle

In Anlehnung an § 13 Abs. 2 Nr. 4 TMG fordert auch das Trennungsgebot gemäß Art. 32 Abs. 1 lit. b DSGVO, dass Daten, die für unterschiedliche Zwecke erhoben werden, grundsätzlich getrennt verarbeitet werden sollen. Ferner ist das Verbot der

Verkettbarkeit von personenbezogenen Daten zu beachten. Um eine Nicht-Verkettbarkeit sowie das Trennungsgebot zu gewährleisten, sind Maßnahmen zu treffen, die es verhindern oder zumindest erschweren, das personenbezogene Daten eines Verfahrens zu anderen als den ausgewiesenen Zwecken erhoben, verarbeitet oder genutzt werden können. Hier kann im Wesentlichen auf Maßnahmen des Zugriffs- oder Zutrittsschutzes eingegangen werden (z.B. durch ein stringentes und restriktives Rollen- und Berechtigungskonzept). Für die verantwortliche Stelle bedeutet dies im Zweifel einen hohen technischen und organisatorischen (damit finanziellen) Aufwand, der vor dem Hintergrund des Verhältnismäßigkeitsgrundsatzes nur dann gerechtfertigt sein wird, wenn dadurch ein erhebliches Mehr an Datenschutz für den Betroffenen erreicht wird.

Fragen

- Gibt es Sicherheitsschlösser mit Schlüsselregelung?
- Sind die Türen bei Abwesenheit verschlossen?
- Gibt es eine Fenstersicherung?
- Gibt es bestimmte Sicherheitsbereiche mit entsprechenden Zutrittssicherungen?
- Gibt es (abgestufte) Zutrittsberechtigungsregelungen? Sind diese hinreichend dokumentiert?
- Gibt es Ausweisleser oder ein Codeschloss?
- Werden Zu- und Abgänge protokolliert?
- Gibt es eine Zutrittsregelung für betriebsfremde Personen? (Empfang?)
- Wird die Einhaltung der Zutrittsregeln überwacht und protokolliert? Gibt es einen Wachdienst?
- Gibt es Tastatursicherungen (elektronisches Schloss)?
- Gibt es ein Identifizierungs- bzw. Authentisierungskonzept?
- Erfolgt eine Protokollierung der Zugriffe / Zugriffsversuche?
- Ist eine Zuordnung Benutzer/Funktionen/Befugnisse vorhanden?
- Ist gewährleistet, dass jeder DV-Benutzer über einen eigenen Benutzercode einschließlich Passwort verfügt?
- Kann der Anwender die Passwörter selbst wählen?
- Existieren Vorgaben für sichere Passwörter (Mindestlänge, Aufbau)? Werden Passwörter, die den Vorgaben nicht entsprechen, zurückgewiesen?
- Wird ein Passwortwechsel maschinell erzwungen?
- Wird die Passworthistorie überprüft?
- Erfolgt eine Verschlüsselung des Passworts?
- Erfolgt nach einer bestimmten Anzahl von Fehlversuchen ein Abbruch der Verbindung?
- Gibt es für wichtige Funktionen (insb. die Administration) das „Vier – Augen – Prinzip“?
- Gibt es Regelungen für den Zugriff durch Fernwartung?

- Erfolgt eine Dunkelschaltung der Bildschirme bei längerer Inaktivität? Ist der Bildschirmschoner passwortgeschützt?
- Wurde vor der Inbetriebnahme des Dienstes eine Risikoanalyse durchgeführt?
- Existiert eine Firewall? Ist eine DMZ eingerichtet?
- Welche Methode zur Realisierung der Firewall wird eingesetzt (Paket-Filter, Application Level Gateway, sonstige (Hybrid))?
- Existieren Maßnahmen gegen Vortäuschung falscher Identität?
- Ist bei der Konfiguration der Firewall (FW) gewährleistet, dass
  - die FW keine anwendungsorientierten Dienste/Programme unterstützt?
  - die FW nicht den Anwendern für den direkten Zugriff zur Verfügung steht?
  - außer dem Administrator kein Anwender Zugriff hat?
  - alle Systemaktivitäten (auch des Administrators) vollständig protokolliert werden?
  - Analyseprogramme vorhanden sind?
  - ständige Kontrollen der Integrität der Sicherheitsmaßnahmen durchgeführt werden?
- Sind Maßnahmen gegen den Schutz vor Viren und Trojanischen Pferden getroffen?
- Wie sieht das Sicherheitskonzept für den Betrieb der Server und Anwendung aus?
- Wie wird die aktuelle Konfiguration der Server und Anwendung dokumentiert?
- Wie erfolgt das Änderungsmanagement (Changemanagement) für Änderungen an der Konfiguration bzw. der eingesetzten Software?
- Wie wird sichergestellt, dass die Administratoren ausreichend qualifiziert und ausgebildet, um den sicheren Betrieb der Webseite sicherzustellen?
- Wie wird sichergestellt, dass nur aktuelle Softwareversionen eingesetzt werden und Aktualisierungen zeitnah erfolgen?
- Wie erfolgt der Freigabeprozess für Softwareänderungen?
- Wie werden Codereviews für die Entwicklung und jede Änderung realisiert?
- Wie erfolgen die Softwaretests?
- Wie sehen die Codeing-Standards aus nach denen gearbeitet werden muss?
- Wie wird sichergestellt, dass Entwickler ausreichend qualifiziert und ausgebildet sind, um die sichere Entwicklung und Weiterentwicklung der Webseite sicherstellen zu können?
- Wie oft und in welcher Form erfolgen Revisionen, ob die Regelungen eingehalten werden?
- Gibt es ein Berechtigungskonzept? Gibt es ein Rollenkonzept?
- Ist eine Zuordnung Benutzer/Funktionen/Befugnisse vorhanden?
- Ist gewährleistet, dass jeder DV-Benutzer über einen eigenen Benutzercode einschließlich Passwort verfügt?
- Sind aktuelle Betriebssystem installiert?

- Kann der Anwender die Passwörter selbst wählen?
- Existieren Vorgaben für sichere Passwörter (Mindestlänge, Aufbau)? Werden Passwörter, die den Vorgaben nicht entsprechen, zurückgewiesen?
- Wird ein Passwortwechsel maschinell erzwungen?
- Wird die Passworthistorie überprüft?
- Erfolgt eine Verschlüsselung des Passworts?
- Erfolgt nach einer bestimmten Anzahl von Fehlversuchen ein Abbruch der Verbindung?
- Wie erfolgen sonst die Identifizierung und Authentisierung?
- Gibt es alternative Authentifizierungsmöglichkeiten: Chipkarte, Fingerabdruck, Stimme etc.?
- Ist die Aktualität der Zugriffsberechtigungen gewahrt? Werden Zugriffsberechtigungen eines ausscheidenden Benutzers umgehend gelöscht?
- Gibt es Sanktionen für unberechtigte Zugriffsversuche?
- Werden Clients nach Arbeitsende verschlossen?
- Werden Daten für unterschiedliche Zwecke erhoben?
- Berücksichtigt das Berechtigungskonzept die Erhebung bzw. Verarbeitung für unterschiedliche Zwecke?
- Ist technisch gewährleistet, dass die personenbezogenen Daten über die Inanspruchnahme verschiedener Telemedien durch einen Nutzer getrennt verarbeitet werden?
- Können für unterschiedliche Zwecke erhobene Daten zusammengeführt werden? Welcher Aufwand ist dafür erforderlich?
- Sind organisatorische Maßnahmen getroffen, dass Daten, die für unterschiedliche Zwecke erhoben werden, getrennt verarbeitet werden?

Bewertung

0 Punkte: Maßnahmen zur Zutrittskontrolle existieren nicht oder sind ungenügend

- Vorkehrungen zum Schutz vor dem Zutritt Unbefugter sind nicht getroffen
- Türen bzw. Schlösser sind oft unverschlossen bzw. Schlösser sind veraltet
- Betriebsfremde Personen gelangen unbemerkt bis zu DV-Anlagen
- es gibt kein Berechtigungs- / Sicherheitskonzept
- es werden Gruppen- / Sammelpasswörter verwendet, so dass auch unberechtigte Mitarbeiter auf personenbezogene Daten zugreifen können
- individuelle Passwörter sind anderen (unberechtigten) Mitarbeitern bekannt
- eine Firewall existiert nicht oder ist nicht konfiguriert
- es werden keine Sicherungen gegen Viren und trojanische Pferde getroffen
- das System wird nicht regelmäßig getestet
- es gibt kein Berechtigungskonzept, es fehlen sonstige Identifizierungsmöglichkeiten

- es gibt nur Sammel- / Gruppenpasswörter
- Zugriffe werden nicht protokolliert
- die installierten Betriebssysteme sind veraltet
- es gibt kein zentrales Dateisystem, eine Zuordnung Benutzer/ Funktion /Befugnisse erfolgt nicht
- obwohl Daten für unterschiedliche Zwecke erhoben werden, werden sie sämtlich einheitlich verarbeitet
- weder organisatorische, noch technische Maßnahmen zur getrennten Verarbeitung sind getroffen
- für unterschiedliche Zwecke erhobene Daten werden zusammengeführt

1 Punkt: Maßnahmen zur Zutrittskontrolle sind eingerichtet, weisen aber Defizite auf

- die Türschlösser sind veraltet
- Büroräume sind auch für betriebsfremde Personen zugänglich
- es gibt nur eine Art der Zugangsberechtigung (Schlüssel)
- zentrale DV-Systeme (Serverraum) sind nicht gesondert gesichert
- es bestehen nur lokale Sicherungen (Virenscanner)
- es existiert eine zentrale Firewall, diese ist aber unzureichend konfiguriert oder weist sonstige Schwachstellen auf
- das Berechtigungskonzept ist nicht ausgereift
- es bestehen keine Vorgaben für Passwörter (beliebig viele Einlogg-Versuche sind möglich; keine Verfallsdauer, keine Sicherung der Passwortqualität)
- die Mitarbeiter mit Zugriff auf personenbezogene Daten haben nicht die Möglichkeit, den Zugriff bei temporärer Abwesenheit zu sperren
- Administration und Entwicklung finden nur unregelmäßig statt
- ein Berechtigungs-/Sicherheitskonzept ist nicht dokumentiert
- das Berechtigungskonzept ist nicht ausgereift
- Passwörter sind beliebig
- Zugriffsberechtigungen werden nicht kontrolliert
- Technische Vorkehrungen zur getrennten Verarbeitung von Daten sind vorhanden, werden aber in der Praxis nicht umgesetzt
- das Berechtigungskonzept unterscheidet nicht zwischen Daten, die für unterschiedliche Zwecke erhoben werden

2 Punkte: die Maßnahmen zur Zutrittskontrolle sind angemessen

die Schließanlagen sind auf aktuellem Stand

- es gibt ein abgestuftes Berechtigungskonzept
- zu den zentralen DV-Anlagen (Serverraum) haben nur Berechtigte Zutritt (Spezialschloss bzw. Codecartenleser oder ähnliche Zutrittssicherung
- es gibt ein nachvollziehbares und dokumentiertes Sicherheitskonzept

- gestuftes Berechtigungskonzept, das den Zugriff auf personenbezogene Daten auf den erforderlichen Umfang beschränkt
- es gibt angemessene betriebliche Vorgaben für die Verwendung von Passwörtern (Passworthistorie, Mindestlänge acht Zeichen, Beschränkung der ein Einlogg-Versuche mit unzutreffendem Passwort auf max. 5; maximale Verwendungsdauer eines Passworts auf 3 Monate)
- die Einhaltung der Vorgaben wird technisch gewährleistet
- die zentrale Firewall (Paketfilter oder Application Gateway) ist auf dem aktuellen Stand der Technik und wird regelmäßig aktualisiert
- die Systeme werden regelmäßig gewartet
- ein Change-Management ist vorhanden
- es gibt ein gestuftes Berechtigungskonzept
- es gibt betriebliche Vorgaben für die Verwendung von Passwörtern
- es gibt eine Passworthistorie und max. 3 Einlogg-Versuche
- alle Zugriffe werden protokolliert
- das Berechtigungskonzept berücksichtigt eine differenzierte Bearbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
- Daten werden getrennt erhoben und verarbeitet
- eine Zusammenführung von Daten wird durch technische oder organisatorische Maßnahmen erschwert

3 Punkte: die Maßnahmen zur Zutrittskontrolle sind vorbildlich

- die Arbeitsplatzrechner sind zusätzlich mit einem Schlüssel abschließbar
- die Türen zu den zentralen DV-Anlagen sind mit Codekartenleser, Fingerabdruckscanner o.ä. versehen
- es gibt Fensterschlösser
- betriebsfremde Personen können nur in Begleitung eines Mitarbeiters in die Büroräume
- die Zutrittsregelungen werden überwacht, Zu- und Abgänge werden protokolliert
- es gibt vorbildliche betriebliche Vorgaben für die Verwendung von Passwörtern (Passworthistorie, Mindestlänge zehn Zeichen, obligatorische Verwendung von Ziffern und Sonderzeichen, Ausschluss von Trivialpasswörtern, Beschränkung der Einlogg-Versuche mit unzutreffendem Passwort auf max. 3, maximale Verwendungsdauer eines Passworts 30 Tage)
- die Zugangskontrolle erfolgt durch angemessene biometrische Maßnahmen; die biometrischen Merkmale sind lokal (z. B. auf Chipkarten) gespeichert
- Vier-Augen-Prinzip für sicherheitsrelevante Zugriffe, Änderungen an der Netztopologie bzw. der Firewall sind nur durch zwei Administratoren möglich
- Administrationsvorgänge werden vollständig und revisionssicher protokolliert
- stichprobenartige Protokollierung von berechtigten Zugriffen
- vollständige Protokollierung unberechtigter Zugriffsversuche

- besondere Qualität der Firewall (z.B. zwei Firewalls - ein Paketfilter, ein Application Gateway; es ist eine DMZ zwischen den Firewalls eingerichtet
- Administratoren müssen sich zusätzlich zum Passwort mit Codekarte o.ä. identifizieren
- Fernwartungen können nur unter Freischaltung einer festen IP-Nr. und unter Beobachtung des Administrators vorgenommen werden; alle Fernwartung Aktivitäten sind durch kryptographische Verschlüsselung geschützt
- Berechtigungskonzept, Sicherheitskonzept und sonstige Unterlagen liegen in aktueller Fassung vor
- Mitarbeiter werden regelmäßig geschult
- es gibt ein dezidiertes Berechtigungskonzept
- es gibt einen maschinell erzwungenen Passwortwechsel
- zusätzlich zu Passwörtern gibt es weitere Authentifizierungserfordernisse
- alle Zugriffe und Zugriffsversuche werden protokolliert, das Protokoll umfasst auch die durchgeführten Aktionen
- Zugriffsberechtigungen werden regelmäßig kontrolliert und angepasst
- Arbeitsplatz-PCs werden nach Arbeitsende lokal verschlossen
- die Zuständigkeiten von Mitarbeitern sind nach unterschiedlichen Datenarten verteilt
- Daten werden freiwillig pseudonymisiert, um eine Zusammenführung zu verhindern

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Der Verantwortliche hat entsprechend dem Stand der Technik die Pseudonymisierung und Verschlüsselung der personenbezogenen Daten vorzunehmen. Dabei sollen die Implementierungskosten und das Risiko, dass die Rechte und Freiheiten der Betroffenen verletzt werden berücksichtigt werden.

Pseudonymisierung meint gemäß Art. 4 Abs. 5 DSGVO, dass bei der Verarbeitung personenbezogener Daten ohne Hinzuziehung zusätzlicher Informationen die Zuordnung zu einer spezifischen betroffenen Person nicht mehr möglich ist. Darüber hinaus muss durch technische und organisatorische Maßnahmen gesichert werden, dass diese zusätzlichen Informationen, sofern sie gesondert aufbewahrt werden, nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können.

Verschlüsselung meint einen Vorgang, mit dem eine klar lesbare Information durch ein kryptographisches Verfahren verändert wird und damit nicht mehr klar lesbar ist.

Fragen

- Werden personenbezogene Daten dem angestrebten Schutzzweck entsprechend pseudonymisiert?
- Sind die Daten einer identifizierbaren natürlichen Person zuzuordnen?

- Unterliegen die zusätzlichen Daten, die eine Zuordnung bei der Pseudonymisierung möglich machen geeigneten technischen und organisatorischen Maßnahmen?
- Werden personenbezogene Daten dem angestrebten Schutzzweck entsprechend verschlüsselt?

Bewertung

0 Punkte

- personenbezogene werden nicht verschlüsselt oder nicht ausreichend verschlüsselt (gemessen am aktuellen Stand der Technik)
- personenbezogene werden nicht pseudonymisiert, obwohl dies einfach möglich wäre
- identifizierbare Daten und pseudonymisierten Daten sind nicht voneinander getrennt und können leicht zusammengeführt werden

1 Punkt

- personenbezogene werden zwar dem Stand der Technik nach angemessen verschlüsselt, jedoch läuft z.B. das Zertifikatsgültigkeit in wenigen Tagen aus oder es erscheinen bei der Nutzung gängiger Browserversionen Fehlermeldungen (z.B. oftmals bei eigen-ausgestellten Zertifikaten)

2 Punkte

- personenbezogene werden dem Stand der Technik entsprechend in einem angemessenen Verhältnis zum Schutzweck verschlüsselt
- personenbezogene werden dem Stand der Technik entsprechend in einem angemessenen Verhältnis zum Schutzweck pseudonymisiert

3 Punkte

- die Verschlüsselungsverfahren gehen über den Stand der Technik hinaus
- personenbezogene Daten werden anonymisiert

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Durch die Weitergabekontrolle soll sichergestellt werden, dass die Daten bei der elektronischen Übertragung (oder während anderweitigen Transports auf Datenträgern bzw. bei der Speicherung) nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Maßnahmen sind vom Versender bzw. von demjenigen zu treffen, der den Transport initiiert oder für die Speicherung der Daten verantwortlich ist. Die Weitergabekontrolle erfasst nicht nur die mittels elektronischer Übertragung weitergegeben Daten, sondern auch die auf portablen Datenträgern gespeicherten Daten.

Eingabekontrolle

Maßnahmen zur Gewährleistung der Eingabekontrolle sollen sicherstellen, dass zu jedem Zeitpunkt nachvollzogen werden kann, wer welche Daten wann eingegeben

und wie verändert hat. Eine solche Kontrolle kann nur durch eine lückenlose, detaillierte Protokollierung der schreibenden, ändernden und löschenden Zugriffe erreicht werden, wobei die Protokolldaten selbst wiederum vor unbefugtem Zugriff zu schützen sind.

Fragen

- Sind Datenträger (DT) gekennzeichnet?
- Sind die Daten auf den DT verschlüsselt?
- Werden E-Mails verschlüsselt?
- Gibt es Regelungen für den Transport von DT? Gibt es bestimmte Berechtigte, die den Transport durchführen dürfen?
- gibt es ein Bestandsverzeichnis der DT?
- sind die Abgabepersonen und die Empfänger bestimmt?
- Werden Datenübermittlungen protokolliert?
- Werden Daten über das Internet verschlüsselt übertragen? Welcher Verschlüsselungsstandard wird benutzt? Wie ist der Authentifizierungsschlüssel aufbewahrt?
- Ist eine Protokollierung aller schreibenden bzw. ändernden oder löschenden Zugriffe sichergestellt?
- Werden folgende Daten protokolliert?
  - Benutzer
  - Datum
  - Uhrzeit
  - Daten
  - Aktivität
- Kann durch (ggf. automatische) Auswertungen festgestellt werden, ob die Benutzer befugt waren, die aufgezeichneten Aktivitäten auszuführen?
- Wie werden die Protokolldaten gespeichert?
- Wann werden die Protokolldaten gelöscht?

Bewertung

0 Punkte: Maßnahmen zur Weitergabekontrolle sind nicht getroffen

- Daten und Datenträger mit personenbezogenen Daten werden unverschlüsselt weitergeben
- es gibt keine Dokumentation der verwendeten Datenträger
- es kann nicht festgestellt werden, welche Personen wann welche Daten eingegeben hat (Eingaben werden nicht protokolliert)

1 Punkt: die Maßnahmen zur Weitergabekontrolle sind verbesserungsbedürftig

- es gibt keine internen Vorgaben, welche Daten nur verschlüsselt zu übertragen sind, die Verschlüsselung erfolgt willkürlich

- Datenträger sind nicht dokumentiert
- Eingaben werden nur unvollständig protokolliert
- die Protokolldatei kann nicht angemessen ausgewertet werden
- die Integrität der Protokolldateien ist nicht ausreichend gewährleistet
- die Protokolldateien sind nicht angemessen gegen unbefugten Zugriff gesichert

2 Punkte: die Maßnahmen zur Weitergabekontrolle entsprechen dem Stand der Technik

- es gibt eine unternehmensinterne Vorgabe, welche Daten verschlüsselt zu übertragen sind
- personenbezogene Daten werden per E-Mail nur verschlüsselt übersandt
- (mobile) Datenträger sind dokumentiert
- alle schreibenden, ändernden und löschenden Zugriffe werden protokolliert
- der Protokolldatei kann auch entnommen werden, welche Daten verändert wurden
- die Integrität der Protokolldateien ist gewährleistet
- die Protokolldateien sind angemessen gegen unbefugten Zugriff gesichert
- die Protokolldaten werden regelmäßig stichprobenartig ausgewertet und die Rechtmäßigkeit der Zugriffe nachgeprüft

3 Punkte: die Maßnahmen zur Weitergabekontrolle sind vorbildlich

- Daten werden ohne Unterschied ausschließlich verschlüsselt übertragen
- soweit personenbezogene Daten auf intern allgemein zugänglichen Daten gespeichert werden, erfolgt auch die Speicherung verschlüsselt
- soweit personenbezogene Daten auf mobilen DT transportiert werden, gibt es hierfür speziell Berechtigte
- die Protokolldatei enthält alle erforderlichen Angaben
- durch Auswertung der Protokolldatei wird festgestellt, ob der Nutzer zur Nutzung berechtigt war
- es werden automatisierte Tools zur Protokollauswertung eingesetzt

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle erfordert gemäß Art. 32 Abs. 1 lit. b DSGVO Sicherheitsmaßnahmen, die die Daten gegen die zufällige Zerstörung bzw. Verlust schützen. Gefahren in diesem Bereich können durch Blitzschlag, Stromausfall, Wasserschaden und ähnliche Einflüsse von außen drohen. Die zur Gewährleistung der Verfügbarkeitskontrolle zu treffenden Maßnahmen betreffen damit sowohl technische, als auch organisatorische Vorkehrungen zur Abwehr der o.g. Gefahren.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DGSVO)

Bei einem physischen Zwischenfall sollen personenbezogene Daten unverzüglich wiederhergestellt werden können. Dies wird insbesondere durch Notfallpläne, Backups und Risikoabschätzungen erreicht.

Fragen

- Gibt es ein Backupkonzept?
- In welchen Zeitabständen werden Backups durchgeführt? Auf welchen Speichermedien?
- Wie und wo werden die Speichermedien aufbewahrt? Wer hat Zugang dazu?
- Gibt es eine USV?
- Wie schnell können eingesetzte Systeme im Störungsfall wiederhergestellt werden?
- Gibt es einen Brandmelder?
- Gibt es Notrufnummern?
- Gibt es Stellvertretungsregelungen für das Administrationspersonal?

Bewertung

0 Punkte: Maßnahmen gegen die zufällige Zerstörung / Verlust der Daten sind nicht getroffen

- der Serverraum ist gänzlich ungesichert trotz eines Risikos
- der Serverraum dient als Arbeitsplatz mit leicht entzündbaren Materialien
- es gibt kein Backup oder eine sonstige Sicherung der Daten
- es gibt kein Konzept für Notfälle

1 Punkt: die zur Verfügbarkeitskontrolle getroffenen Maßnahmen weisen Defizite auf

- ein Backup wird in unregelmäßigen Abständen durchgeführt
- es gibt ein Notfallkonzept, dies ist aber nur wenigen Mitarbeitern bekannt
- Backups werden unzureichend geschützt (z.B. Aufbewahrung im selben Raum wie Originaldaten)
- eine Wiederherstellung der eingesetzten Systeme dauert unverhältnismäßig lang

2 Punkte: zur Verfügbarkeitskontrolle sind angemessene Maßnahmen getroffen worden

- es werden regelmäßige Backups durchgeführt; dabei werden mehrere Generationen des Datenbestands systematisch gesichert
- die Backups werden in einem anderen Raum aufbewahrt und dort angemessen gesichert (Stahlschrank bzw. Safe - abhängig von der Sensibilität der personenbezogenen Daten)
- die Verwendbarkeit der Backups wird regelmäßig überprüft; die Verwendungsdauer von Backup-Datenträgern wird begrenzt
- es gibt eine USV
- es gibt einen Brandmelder

- es gibt Stellvertretungsregelungen für die Administratoren
- es gibt Notrufnummern
- die Wiederherstellung der eingesetzten Systeme ist im Störungsfall unverzüglich möglich

3 Punkte: die Maßnahmen zur Verfügbarkeitskontrolle sind vorbildlich

- zusätzlich zu den o.g. Maßnahmen:
- es werden tägliche Backups durchgeführt
- die Backups werden in einem feuerfesten anderen Raum aufbewahrt besonders gesichert (Safe) aufbewahrt

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Der Verantwortliche muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der getroffenen technischen und organisatorischen Maßnahmen einrichten. Dies kann durch die regelmäßige Durchführung von Datenschutz-Folgeabschätzungen, Penetrationstests sowie die Einführung eines IT-Sicherheitsmanagement-Systems nach ISO 27001 erfolgen. Wichtig ist, dass sowohl Datenschutzmanagement als auch Incident-Response-Management umfassende Beachtung im Unternehmen erfährt.

Auftragskontrolle

Soweit die verantwortliche Stelle Daten im Auftrag verarbeiten lässt hat der Auftraggeber geeignete Maßnahmen zu ergreifen, um die Datenverarbeitung beim Auftragnehmer in ähnlicher Weise zu kontrollieren, als wenn sie durch den Auftraggeber selbst verarbeitet würden. Die Auftragskontrolle ergibt sich aus Art. 25 Abs. 2 i.V.m. Art 28 Abs. 1 DSGVO. Hier kann ggf. auf die Bewertung unter dem Punkt Auftragsverarbeitung verwiesen werden.

Penetrationstest: Zur Erfüllung dieses Kriteriums wird die Vorlage der Ergebnisse eines maximal 12 Monate alten Penetrationstestes gefordert. Sofern der Penetrationstest Feststellungen über potentielle Schwachstellen aufzeigt, muss der der Anbieter zudem einen Maßnahmenplan vorlegen, welcher geplante Maßnahmen zur Behebung der Schwachstellen beschreibt.

Fragen

- Werden die getroffenen technischen und organisatorischen Maßnahmen regelmäßig überprüft und bei Bedarf angepasst?
- Erfolgt eine Auftragskontrolle durch den Verantwortlichen
- Erfolgt eine Erteilung von Weisungsbefugnissen durch den Verantwortlichen?
- Werden ausschließlich auf Grund von Weisungen Verarbeitungstätigkeiten durchgeführt?
- Führt der Verantwortliche Vor-Ort Kontrollen zur Überprüfung durch?

Bewertung

O Punkte: Es gibt keine angemessenen Maßnahmen zur Überprüfung, Bewertung und Evaluierung

- die bestehenden Maßnahmen werden nicht überprüft
- der Verantwortliche führt keine Auftragskontrolle durch

1 Punkt: Es bestehen Maßnahmen zur Überprüfung, Bewertung und Evaluierung, diese unterschreiten aber die gesetzlichen Vorgaben

- die bestehenden Maßnahmen werden nur unregelmäßig überprüft
- die bestehenden Maßnahmen werden geprüft aber nicht angepasst, obwohl ein Bedarf besteht
- der Verantwortliche erfragt die eingesetzten Maßnahmen bei dem Auftragsverarbeiter, kontrolliert aber nicht, ob diese tatsächlich umgesetzt werden

2 Punkte: Es bestehen angemessene Maßnahmen zur Überprüfung, Bewertung und Evaluierung

- der Verantwortliche überprüft regelmäßig die bestehenden technischen und organisatorischen Maßnahmen bei den eingesetzten Auftragsverarbeitern auch durch vor-Ort-Kontrollen
- die Maßnahmen beim Auftragsverarbeiter werden regelmäßig bei Bedarf angepasst

3 Punkte: Die Maßnahmen zur Überprüfung, Bewertung und Evaluierung sind vorbildlich

- der Anbieter lässt sich regelmäßig durch unabhängige Prüfstellen kontrollieren und ggf. auch zertifizieren

4. Spezialfall: technische und organisatorische Maßnahmen für Online-Videosprechstunden und im E-Health Bereich

Merker für Online-Videosprechstunden und andere E-Health Dienstleistungen: Im Bereich von E-Health-Leistungen gelten zudem zahlreiche Sonderregelungen für die IT-Sicherheit, z.B. in Landeskrankenhausgesetzen oder berufsständischen Verordnungen. Für behandelnde Ärzte gilt etwa § 10 Abs. 5 MBO-Ä. Darin heißt es:

> *„Aufzeichnungen auf elektronischen Datenträgern oder anderen Speichermedien bedürfen besonderer Sicherungs- und Schutzmaßnahmen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Der Arzt hat hierbei die Empfehlungen der Ärztekammer zu beachten.“*

Angesichts des Umstands, dass nahezu alle verarbeiteten personenbezogenen Daten im E-Health-Angebot einem besonderen Berufsgeheimnis unterliegen und diesen Daten eine hohe Schutzbedürftigkeit zukommt, bedarf es äußerst wirksamer Datensicherungsvorkehrungen. Bei digital geführten, online abrufbaren Patientenakten sind insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und die Transparenz der Datenverarbeitung zu

sichern. Die hierzu entwickelten nachfolgenden Kriterien sind z.T. redundant mit denen anderer Module (insbesondere der des Moduls Datenschutzmanagement). Sie sollen daher zusammenfassend aufgeführt und bewertet werden.

4.1. Authentizität

Die Authentizität der erhobenen, gespeicherten, übermittelten oder verarbeiteten Daten muss gewährleistet sein. Demnach muss der Urheber oder Verantwortliche von bzw. der für patientenbezogene Daten jederzeit eindeutig feststellbar sein. Übertragene Daten müssen immer dem behandelnden Arzt zugeordnet werden können, z.B. anhand einer elektronischen Signatur. Medizinische Dokumente, die ihren Urheber bzw. Verantwortlichen nicht erkennen lassen, sind als Grundlage für Behandlungen und Begutachtungen ungeeignet. Bei der Authentizität unterscheidet man nach Authentizität der Daten und Authentizität des Kommunikationspartners. Die Authentizität von Inhalts- und Nutzungsdaten stellt sicher, dass die Daten tatsächlich von dem vermeintlichen Kommunikationspartner stammen. Die Authentizität des Kommunikationspartners stellt sicher, dass der Partner tatsächlich auch derjenige ist, der er vorgibt zu sein.

Bei herkömmlicher Kommunikation wird die Authentizität der Daten z.B. durch die Unterschrift des Absenders eines Briefes oder unmittelbar durch ein persönliches Gespräch gewährleistet, bereits hier sind verschiedene Ausprägungen der Authentizität möglich. Bei der elektronischen Kommunikation dienen insbesondere elektronische Signaturen zur Authentisierung der übermittelten Daten. Daneben ist die Authentizität der Kommunikationspartner sicherzustellen. Auch hierbei ist die elektronische Signatur das angemessene Mittel.

4.2. Revisionsfähigkeit

Die Revisionsfähigkeit stellt sicher, dass Verarbeitungsprozesse lückenlos nachvollzogen werden können. Dazu muss genau festgestellt werden können, wer wann welche patientenbezogenen Daten auf welche Weise verarbeitet hat. Nach der Berufsordnung gilt für Ärzte bzw. als Arbeitgeber mittelbar auch für das Krankenhaus die Pflicht zur Dokumentation der Behandlung. Sie ist eine Nebenpflicht zum Behandlungsvertrag. Lücken in der Dokumentation können im Falle eines Haftungsprozesses eine Beweislastumkehr zugunsten des Patienten nach sich ziehen. Der gesamte Behandlungsverlauf muss daher nachvollzogen werden können. Eine notwendige Voraussetzung für die Gewährleistung der Revisionsfähigkeit ist die Sicherstellung der Authentizität, deren unter Punkt 4.4 angesprochene Voraussetzungen mit denen der Revisionsfähigkeit weitgehend redundant sind.

4.3. Transparenz der Datenverarbeitung

Schließlich muss die Verarbeitung personenbezogener Patientendaten transparent sein, was im Wesentlichen die Protokollierung der Verarbeitungsschritte sowie der Datenart und der Nutzer betrifft. Erhebung, Speicherung, Nutzung, Übermittlung etc. von personenbezogenen Patientendaten sollten dem Betroffenen zudem vor Beginn dieser Verarbeitungsschritte anhand der entsprechenden Einwilligungserklärung verdeutlicht werden.

Fragen:

- Welche Maßnahmen zur Sicherung der Vertraulichkeit von Patientendaten sind getroffen?
- Erfolgt die Übermittlung personenbezogener Daten verschlüsselt?
- Welche kryptographischen Verfahren werden eingesetzt?
- Entsprechen die Schlüssellängen bei Einsatz symmetrischer, asymmetrischer oder hybrider Verschlüsselung dem aktuellen Stand der Sicherheitstechnik?
- Werden aktuelle Verschlüsselungsprotokolle eingesetzt?
- Ist das eingesetzte System offen für den Einsatz verschiedener Zertifikate?
- Entsprechen die eingesetzten Sicherheitsmechanismen dem aktuellen Stand der Technik?
- Ist dem Nutzer der Zugang zu dem Dienst und insb. die Bestellung bzw. Übertragung sonstiger personenbezogener Daten in einem gegen unberechtigte Kenntnisnahme gesicherten Verfahren (z. B. SSL-Verschlüsselung) möglich?
- Ist die Verfügbarkeit personenbezogener Daten der Nutzer (z. B. protokollierte Einwilligungserklärungen, Bestandsdaten) gewährleistet?
- Sind ausreichende Maßnahmen gegen einen unberechtigten Zugriff und die Verfälschung des Angebots und des personenbezogenen Datenbestandes getroffen (Firewall, Schutz gegen Viren und trojanische Pferde)?
- Werden die Daten auf den Servern verschlüsselt, d.h. ohne Zugriffsmöglichkeit durch Dritte, gespeichert?
- Wie ist die Integrität der Daten gesichert?
- Können die übermittelten Daten nachträglich verändert werden? Welche Maßnahmen verhindern dies?
- Bestehen Backup- oder Sicherungskonzepte zur Verfügbarkeitskontrolle?
- Welche Maßnahmen sind getroffen, um Dokumente ihrem Urheber bzw. dem behandelnden Arzt zuordnen zu können?
- Wird die Authentizität des Diensteanbieters durch ein anerkanntes Zertifikat gewährleistet?
- Wird bei der Übermittlung von Daten eine elektronische Signatur verwendet?
- Ist die Revisionsfähigkeit sichergestellt, z.B. durch lückenlose Dokumentation des Behandlungsverlaufs?
- Welche Maßnahmen zur Umsetzung der Transparenz der Datenverarbeitung sind getroffen?

Bewertung

o **Punkte:** es werden keine derartigen Maßnahmen getroffen

- die Übertragung von Patientendaten über das Internet erfolgt ohne besondere Sicherungsvorkehrungen, insb. ohne Verschlüsselung
- eine bestehende Firewall ist unzureichend konfiguriert oder unzureichend administriert

- es werden Maßnahmen zur gesicherten Übertragung personenbezogener Daten über das Internet getroffen; diese sind jedoch nicht ausreichend
- Verschlüsselungsverfahren entsprechen nicht dem Stand der Technik
- Patientendaten sind für jede Person frei zugänglich
- der Urheber eines Patientendokuments kann nicht festgestellt werden
- Patientendokumente können ohne Weiteres nachträglich verändert werden

1 Punkt: die getroffenen Maßnahmen weisen Defizite auf

- es findet keine Prüfung von Berechtigungen zum Zugriff auf die Patientendaten statt
- die Berechtigungen zum Zugriff auf Patientendaten werden unzureichend geprüft

2 Punkte: es wurden angemessene Maßnahmen getroffen

- das operative System ist durch eine Firewall vom Internet abgeschottet,
- die Übertragung personenbezogener Daten über das Internet wird angemessen gesichert
- es besteht eine angemessene Berechtigungsprüfung
- Verschlüsselungsverfahren entsprechen dem Stand der Technik

3 Punkte: es wurden vorbildliche Maßnahmen getroffen

- Datenschutzkonzept und Maßnahmen werden ständig dem Stand der technischen Entwicklung und der Bedrohungslage angepasst.
- Berechtigungen werden in kurzen regelmäßigen Intervallen überprüft und Passwörter geändert
- unberechtigte Eindringversuche werden durch ein Intrusion Detection System überwacht
- Nutzer werden auf verbleibende Datenschutzrisiken und auf Selbstschutzmaßnahmen hingewiesen
- die Verschlüsselung ist auf dem höchsten technischen Niveau
- Zur Übermittlung werden elektronische Signaturen eingesetzt

5. Gewährleistung der allgemeinen Betroffenenrechte

Zu einem vorbildlichen Datenschutzmanagement gehören neben den Sicherheitsvorkehrungen zum Schutz vor Risiken durch internen wie externen Missbrauch der Daten, auch die Einrichtung von technischen und organisatorischen Maßnahmen zur effizienten Gewährleitung der gesetzlichen Betroffenenrechte. Nur wenn die Betroffenen ihre Rechte gegenüber der verantwortlichen Stelle einfach und unkompliziert geltend machen können, kann sich das Unternehmen im Bereich Datenschutz auszeichnen. Mit dieser Intervenierbarkeit soll der Betroffene eine Möglichkeit erhalten, seine Rechte auszuüben. Dies kann z.B. realisiert werden durch einen (einheitlichen) Ansprechpartner in Sachen Datenschutz sowie durch organisatorische Maßnahmen zur Datenberichtigung, Datensperrung oder Datenlöschung. Das Bild, welches der Betroffene von der Qualität des im jeweiligen Unternehmen praktizierten Datenschutzes erhält, wird dabei zum nicht geringen

Maße davon bestimmt, wie es auf Anfragen, seien es solche allgemeiner Art zum Thema Datenschutz, spezielle Auskunftsersuchen zu personenbezogenen Daten oder bei der Geltendmachung von Berichtigungs- oder Widerspruchsrechten, reagiert. Ein gut organisiertes „Auskunftsmanagement“ kann dabei für viele Unternehmen zum Aushängeschild für vorbildlichen Datenschutz sein.

5.1. Allgemeine rechtliche Grundlagen

Rechte der Betroffenen ergeben sich insbesondere aus den Art. 12ff. DSGVO. Diese sind:

- Informationsrecht
- Recht auf Auskunft
- Recht auf Löschung („Vergessenwerden“)
- Recht auf Datenportabilität
- Widerspruchsrecht in Art. 21 DSGVO
- Recht auf Einschränkung der Verarbeitung in Art. 18 DSGVO
- Recht auf Berichtigung in Art. 16 DSGVO.

5.1.1. Fragen

Auskunft

- Ist gewährleistet, dass die Betroffenen ihre Rechte geltend machen können?
- Sind auf den Webseiten entsprechende Formulare vorgesehen?
- Werden entsprechende Begehren von Betroffenen, die Auftragnehmern bei der Verarbeitung personenbezogener Daten im Auftrag (Art. 28 DSGVO) eingehen, unverzüglich an die verantwortliche Stelle weitergeleitet?
- Wird die Auskunft auch hinsichtlich der Herkunft der personenbezogenen Daten erteilt?
- Umfasst die Auskunft auch die Empfänger, denen personenbezogene Daten übermittelt oder offengelegt wurden?
- Wird Auskunft über die Kategorien personenbezogener Daten die verarbeitet werden erteilt?
- Umfasst die Auskunft auch die Dauer der Speicherung der personenbezogenen Daten?
- Ist gewährleistet, dass auch Auskunft über den Zweck der Speicherung der personenbezogenen Daten gegeben wird?
- Wird über das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde Auskunft erteilt?
- Erfolgt die Auskunftserteilung an den Betroffenen in verständlicher Form?
- Wird auch Auskunft über solche Daten des Nutzers erteilt, die unter Pseudonym gespeichert sind?

- Umfasst die Auskunft auch die Daten, die durch den Diensteanbieter auf dem Rechner des Nutzers abgelegt wurden (z. B. in Cookies)?
- Wird Auskunft darüber erteilt, ob eine automatisierte Entscheidungsfindung oder Profiling stattfindet und die damit verbundene Reichweite und Auswirkungen erklärt?
- Erfolgt die Auskunftserteilung über Bestands- und Nutzungsdaten unentgeltlich?
- Wird die Auskunft auf Verlangen des Nutzers auch elektronisch erteilt?
- Wird bei elektronischer Auskunftserteilung die Authentizität des Betroffenen gewährleistet?
- Wird bei elektronischer Auskunftserteilung die unberechtigte Kenntnisnahme der Auskunft durch unberechtigte Dritte ausgeschlossen?
- Erfolgt eine Verschlüsselung bei elektronischer Auskunftserteilung?
- Erfolgt die Auskunft in einem strukturierten, gängigen und maschinenlesbaren Format?
- Werden Auskunftsersuchen innerhalb der einmonatigen Frist gemäß Art. 12 Abs. 3 DSGVO beantwortet?

Berichtigung / Einschränkung der Verarbeitung / Löschung

- Ist gewährleistet, dass unrichtige Bestands- oder Nutzungsdaten entsprechend den gesetzlichen Vorgaben berichtigt, vervollständigt, gesperrt oder gelöscht werden?
- Ist gewährleistet, dass unrichtige personenbezogene Daten, die als Inhalt des Dienstes veröffentlicht werden, berichtigt, vervollständigt, aktualisiert, gesperrt oder gelöscht werden?
- Ist gewährleistet, dass die Verarbeitung für die Dauer eingeschränkt werden kann, die benötigt wird,
  - um die Richtigkeit der Daten zu überprüfen, wenn ein Betroffener diese bestreitet?
  - Um die Abwägung der Interessen vorzunehmen, wenn er Betroffene Widerspruch gegen die Verarbeitung eingelegt hat?
- Erfolgt die Löschung bzw. Sperrung personenbezogener Bestands- und Nutzungsdaten unverzüglich?
- Ist gewährleistet, dass personenbezogene Daten auch physikalisch gelöscht werden?
- Werden bei öffentlich gemachten Daten andere Dritte durch den Verantwortlichen gemäß Art. 19 DSGVO über das Löschungsverlangen oder Einschränkung der Verarbeitung informiert?

Widerspruch

- Ist gewährleistet, dass die Betroffenen Widerspruchsrechte (Art. 21 DSGVO) jederzeit geltend machen können?
- Hat der Anbieter darauf geachtet, dass das Widerspruchsrecht möglichst einfach (E-Mail, Link) geltend gemacht werden kann?

- Wird der Betroffene ausdrücklich über das Widerspruchsrecht informiert?

Sonstige Betroffenenrechte

- Ist die Datenübertragbarkeit gemäß Art 20 DSGVO gewährleistet?
- Sind die in der DSGVO, dem BDSG oder anderen Vorschriften vorgesehenen sonstigen Rechte der von der Datenerfassung und –nutzung betroffenen Personen beachtet?

5.1.2. Bewertung

0 Punkte: für die Durchsetzung der Betroffenenrechte sind keine bzw. unzureichende Maßnahmen getroffen

- es fehlen Zuständigkeiten für die Bearbeitung von Auskunftsersuchen
- Auskünfte werden nicht erteilt
- Widersprüche werden nicht berücksichtigt
- unrichtige Daten werden nicht gelöscht bzw. berichtigt
- Auskünfte werden unrichtig erteilt
- die Auskunft ist unverständlich
- Technische Einrichtung oder Organisation des Unternehmens lassen keine zügige Auskunftserteilung zu
- die Daten werden trotz gesetzlicher Löschungspflicht nicht endgültig gelöscht
- die Datenverarbeitung wird entgegen der gesetzlichen Vorgaben nicht eingeschränkt
- die Frist zur Beantwortung von Auskunftsanfragen wird nicht eingehalten
- die Datenübertragbarkeit wird nicht gewährt

1 Punkt: Maßnahmen zur Durchsetzung der Betroffenenrechte sind getroffen, aber verbesserungsbedürftig

- die Auskunft ist unvollständig, es fehlen gesetzlich erforderliche Daten (z.B. Herkunft, Speicherungszweck, Empfänger)
- Auskunftsersuchen, Berichtigungsersuchen und Widersprüche werden zwar bearbeitet, die Bearbeitung dauert aber unverhältnismäßig lang
- die Auskunft ist für den typischen Empfänger schwer verständlich
- gesperrte Daten werden unzureichend gegen eine Verknüpfung mit dem operativen Datenbestand geschützt
- Dritte werden bei öffentlich gemachten Daten nicht über Löschungsverlangen betroffener Personen informiert
- die Datenübertragbarkeit wird nicht gewährt

2 Punkte: die Betroffenenrechte können auf Grund organisatorischer Maßnahmen in angemessener Weise durchgesetzt werden

- Auf Grund Organisation oder betrieblicher Übung bestehen klare Zuständigkeiten für die Bearbeitung von Auskunftsersuchen, Widersprüche und Berichtigungsersuchen

- es ist eine elektronische Auskunftserteilung möglich
- die elektronische Auskunftserteilung erfolgt verschlüsselt; die Authentizität des Auskunftsersuchenden ist sichergestellt
- die Auskunft ist unentgeltlich
- Löschungsfristen werden eingehalten
- unrichtige Daten werden berichtigt
- bei Vorliegen gesetzlicher Voraussetzungen erfolgt die Einschränkung der Verarbeitung der Daten

3 Punkte: die Durchsetzung der Betroffenenrechte wird durch zusätzliche Maßnahmen bzw. Informationen erleichtert

- für Datenschutzanfragen gibt es eine spezielle interne Zuständigkeit
- das Web-Angebot enthält Formulare, mit deren Hilfe entsprechende Anfragen gestellt werden können
- die Bearbeitung von Anfragen erfolgt sehr zügig (schriftl. Auskünfte dauern i.d.R. nicht mehr als 3 Werktage)
- die elektronisch mögliche Auskunftserteilung erfolgt durch elektronische Einsichtnahme des Betroffenen in seine Daten
- dem Betroffenen wird generell die Möglichkeit eingeräumt, der Verarbeitung seiner Daten auf elektronischem Wege zu widersprechen
- über die Behandlung und Beantwortung von Auskunftsersuchen gegenüber Auftragnehmern (Art. 28 DSGVO) gibt es klare vertragliche Regelungen

5.2. Spezialfall: Betroffenenrechte für Patienten

Neben allgemeineren Rechten für alle Nutzergruppen von E-Health-Portalen gelten insbesondere für Patienten besondere Bestimmungen zur Durchsetzung ihrer informationellen Datenschutzrechte. Allen voran steht das vom Bundesverfassungsgericht bestätigte Recht des Patienten auf Einblick in seine Gesundheitsakte. Internetportale, die zugleich Einblick in elektronisch geführte Patientenakten anbieten, dienen der optimalen Umsetzung dieses Rechts und entsprechen in der Regel unproblematisch diesen Vorgaben. Hier ist zu beachten, dass die Handhabbarkeit auch für ältere Menschen, Personen mit Behinderungen oder mit wenig Computererfahrung leicht und verständlich gestaltet ist.

Von großer Relevanz im E-Health-Bereich sind zudem Auskunftsrechte, Benachrichtigungsrechte, Ansprüche auf Datenkorrektur, -löschung, -sperrung, Schadensersatz bei unzulässiger Datenverarbeitung, sowie Widerspruchsmöglichkeiten. Grundlagen hierfür sind z.B. die Art. 12 ff. DSGVO. Zum Teil erfahren diese Rechte wiederum Einschränkungen durch landesgesetzliche Regelungen im Gesundheitsbereich, etwa auf Grund ärztlichen Ermessens oder bei Geheimhaltungsinteressen. Da mit einem Datenschutzverstoß i.d.R. zugleich eine Verletzung der ärztlichen Schweigepflicht oder von sonstigen Standespflichten verbunden ist, kann außerdem nach den Vorschriften der Landesberufsregelungen eine Anrufung der Ärztekammer des jeweiligen Landes erfolgen. Nur wenn der Betroffene diese Rechte bei der

verantwortlichen Stelle schnell und unkompliziert geltend machen kann, zeichnet sich das Unternehmen als vorbildlich aus.

5.2.1. Fragen

Ist neben den allgemeinen Betroffenenrechten gewährleistet, dass

- die zuständige Berufskammer für Beschwerden genannt wird?
- Wird der Nutzer angemessen und verständlich über die Bedienung bzw. den Umgang mit einer Patientenakte oder einem Telematiksystem informiert oder geschult?
- Besteht eine Hotline und ist diese leicht zugänglich?

5.2.2. Bewertung

0 Punkte: für die Durchsetzung der Betroffenenrechte sind keine bzw. unzureichende Maßnahmen getroffen

- es fehlt eine Funktionsbeschreibung oder eine Bedienungsanleitung für den Zugriff auf die Patientenakte bzw. diese sind unverständlich formuliert
- die zuständige Berufskammer wird nicht genannt, obwohl die Angabe erforderlich ist

1 Punkt: Maßnahmen zur Durchsetzung der Betroffenenrechte sind getroffen, aber verbesserungsbedürftig

- die Auskunft über Daten aus der Gesundheit unvollständig, es fehlen gesetzlich erforderliche Daten (z.B. Herkunft, Speicherungszweck, Empfänger)
- Auskunftsersuchen, Berichtigungsersuchen und Widersprüche werden zwar bearbeitet, die Bearbeitung dauert aber unverhältnismäßig lang
- die Auskunft ist für den typischen Empfänger schwer verständlich
- die Auskunft ist entgeltlich
- Anleitungen zur Nutzung von Telematikdiensten oder Gesundheitsportalen sind nicht vorhanden oder nur schwer verständlich

2 Punkte: die Betroffenenrechte können in angemessener Weise durchgesetzt werden

- Auf Grund Organisation oder betrieblicher Übung bestehen klare Zuständigkeiten für die Bearbeitung von Auskunftsersuchen, Widersprüche und Berichtigungsersuchen
- es ist eine elektronische (verschlüsselte) Auskunftserteilung möglich, die Authentizität des Auskunftsersuchenden ist sichergestellt
- es besteht eine telefonische Hotline, die zu üblichen Geschäftszeiten genutzt werden kann
- Löschungsfristen werden eingehalten, unrichtige Daten werden berichtigt, bei Vorliegen gesetzlicher Voraussetzungen erfolgt die Sperrung der Daten
- Anleitungen zur Benutzung von Diensten (Telematik/elektronische Patientenakte etc.) sind verständlich formuliert und leicht zugänglich

3 Punkte: die Durchsetzung der Betroffenenrechte wird durch zusätzliche Maßnahmen bzw. Informationen erleichtert

- für Datenschutzanfragen von Patienten gibt es eine spezielle interne Zuständigkeit
- das Web-Angebot enthält Formulare, mit deren Hilfe entsprechende Anfragen gestellt werden können
- die Bearbeitung von Anfragen erfolgt sehr zügig (schriftliche Auskünfte dauern i.d.R. nicht mehr als 3 Werktage)
- die elektronisch mögliche Auskunftserteilung erfolgt durch elektronische Einsichtnahme des Betroffenen in seine Daten
- es besteht eine telefonische kostenlose Hotline, die jederzeit besetzt ist
- der Nutzer wird umfassend zur Benutzung des Systems geschult
- dem Betroffenen wird generell die Möglichkeit eingeräumt, der Verarbeitung seiner Daten auf elektronischem Wege zu widersprechen
- die zuständige Berufskammer wird für Beschwerden benannt und die Patientenrechte erläutert.