internet privacy standards (Vers. 3.6)

datenschutz cert GmbH
1. Januar 2023

datenschutz cert

Inhalt

1. Vorwort zur Neuauflage

Das Gütesiegel ips – internet privacy standards – ist ein bundesweit seit 2001 etabliertes Siegel für Webportale und Webservices. Die Vergabe für das ips Gütesiegel wird nach einem Audit durch lizenzierte ips-Auditor*innen von der unabhängigen Vergabestelle der datenschutz cert GmbH durchgeführt.

Die für Webangebote geltenden datenschutz- und sicherheits-technischen Anforderungen unterliegen einer ständigen Entwicklung. Der ips-Kriterienkatalog wird daher fortlaufend von der Vergabestelle aktualisiert. Die Prüfung eines Webportals oder Webservices mit ips anhand der ständig optimierten Prüfkriterien verdeutlicht die hohe Qualität eines Webangebotes.

Die aktuellen Änderungen betreffen eine weitere Konsolidierung des Kriterienkataloges auf Aspekte des Datenschutzes. Dabei wurde das frühere ips Modul Verbraucherschutz entfernt. Vorgaben des E-Commerce werden daher ab diesem Kriterienkatalog in der Version 3.6 nicht mehr mit geprüft.

Die Autorinnen und Autoren sind für Anregungen, Wünsche und Kritik immer dankbar.

Bremen, im Januar 2023

Dr. Irene Karper LL.M.Eur.

datenschutz cert GmbH

2. Allgemeine Hinweise und Einführung zu ips®

Die internet privacy standards bilden einen Katalog von Qualitätskriterien, der als Grundlage für die Auditierung von Online-Dienstleistungen angewandt wird. Die Qualitätskriterien decken eine Prüfung anhand datenschutzrechtlicher sowie datensicherheits-technischer Anforderungen ab. Mit der Vergabe von ips soll nachgewiesen werden, dass das Webportal bzw. der geprüfte Webservice zum Auditzeitpunkt den rechtlichen Anforderungen entsprechen. Die Prüfung erfolgt dabei durch lizenzierte ips-Auditor*innen, die in den genannten Bereichen nachgewiesen fachkundlich und unabhängig tätig sind. Geprüfte und mit ips ausgezeichnete Anbieter*innen von Webportalen können so ihrer Rechenschaftspflicht nach Art. 5 DSGVO nachkommen. Zugleich soll das Siegel ips den Benutzer*innen des Webportals / Webservices signalisieren, dass es sich um ein vertrauenswürdiges Portal handelt, welches die Einhaltung des Datenschutzes ernst nimmt.

Mit dem Kriterienkatalog werden

- die gesetzgeberische Intention für ein Datenschutzaudit und für Datenschutz-Gütesiegel gezielt und praxisnah umgesetzt,
- die Datenschutzfolgeabschätzung bzgl. der Online-Datenverarbeitung über das Webportal / den Webservice unterstützt,
- Anreize für besonders datenschutzfreundliche Lösungen (privacy by design) geschaffen,
- unterschiedlichste Online-Dienstleistungen bewertet und
- die speziellen Anforderungen der jeweiligen Online-Funktionen berücksichtigt.

2.1. Die Module

Den internet privacy standards liegt der Gedanke zugrunde, dass sämtliche Online-Dienstleistungen in Teilbereiche, sog. Module, aufgespalten und durch Zusammenstellung des jeweils „passenden" Kriterienwerkes abgebildet werden können. Mit dem aktuellen ips Kriterienkatalog gibt es drei Module, mit denen die Prüfung von Online-Shops über Online-Serviceportalen bis hin zum reinen Informationsportal möglich ist. Der oder die im konkreten Verfahren eingesetzte ips-Auditor*in ist dabei aufgefordert, die jeweils anwendbaren Module auszuwählen.

M 1 Info-Abruf

Das Modul „Info-Abruf" umfasst Bereiche, die ohne weitere Dateneingabe durch Aufruf der Homepage und Unterseiten abrufbar sind und im Wesentlichen Informationen enthalten. Hier werden insbesondere Aspekte der Transparenz (z.B. Impressum, Datenschutzerklärung) sowie der Umgang mit Nutzungsdaten (IP-Adresse, Cookies, Social Plugins usw.) geprüft.

M 2 Individual-Dienstleistung

Der Bereich Individual-Dienstleistung erfasst den eigentlichen Kern der Online-Dienstleistung, also die dort abrufbaren Online-Services und Webformulare. Unter diesem Modul stehen daher Unterkategorien zur Verfügung, anhand derer eine Individuelle Anpassung der Kriterien an die jeweilige Online-Leistung möglich ist. Etwa werden in diesem Modul – je nach Funktion – spezifische Anforderungen für E-Health-Dienste,

Presseportale, Bürgerportaldienste, Registrierungsvorgänge, Anmeldungen an Online-Accounts oder Online-Einwilligungsfunktionen geprüft.

M 3 Datenschutzmanagement

Das Modul Datenschutzmanagement beinhaltet die Organisation des geprüften Unternehmens mit Blick auf organisatorische und sicherheits-technische Maßnahmen. Hier ist zu prüfen, wie der Datenschutz dort umgesetzt wird, ob und wie Auftragnehmer*innen einer Datenverarbeitung in die Kontrolle einbezogen sind und wie die IT-Sicherheit bezogen auf die relevanten Online-Services umgesetzt wurden. Da das Datenschutzmanagement die Basis für die tatsächliche Umsetzung der rechtlichen Anforderungen darstellt, kommt dem Modul immer eine besondere Bedeutung zu.

2.2. Die Auswahl der Module für die Begutachtung

Der modulare Aufbau der internet privacy standards ermöglicht es, die Audit-Kriterien flexibel anzupassen, wenn eine Dienstleistung inhaltlich umgestellt, erweitert oder beschränkt wird. Darüber hinaus können Unternehmen die Einhaltung der Kriterien vorab selbst überprüfen. Die Module (M1, M2, M3) sind dabei immer einzubeziehen, wobei im Modul M2 eine individual-spezifische Betrachtung des jeweiligen Online-Services erfolgen soll.

Beispiel: Für die Prüfung eines Online-Shops werden i.d.R. die Module Info-Abruf, Individual-Dienstleistung und Datenschutzmanagement angewandt.

Soweit sich die Module inhaltlich überschneiden, ist es zulässig, diese in einem Modul zusammenzufassen und in anderen Modulen darauf zu verweisen (z.B. kommen in M1 und M2 Aspekte der Transparenz vor; hier kann auf die Ausführungen zu Modul M1 verwiesen werden.

Beispiel: Auf dem Webportal werden ein Registrierungsformular, ein User-Account sowie ein Online-Kontaktformular angeboten. In Modul M1 werden u.a. Impressum, Datenschutzerklärung sowie Umgang mit IP-Adresse, Cookies und Social-Plugins und die Verschlüsselung der Webformulare geprüft. In M2 werden die jeweiligen Online-Formulare nach und nach geprüft. Im Modul M3 Datenschutzmanagement die Datenschutzorganisation des Anbieters sowie die von ihm getroffenen technischen und organisatorischen Datensicherheitsmaßnahmen.

2.3. Das Bewertungssystem

Für eine Vergabe des Gütesiegels nach ips sind mindestens zwei Punkte in der Gesamtwertung aller anwendbaren Module zu erreichen. Das Bewertungssystem sieht pro Kriterium eine Punktevergabe von null bis drei Punkten vor:

0 Punkte: die Anforderungen sind nicht erfüllt: diese Bewertung wird erteilt, wenn gesetzliche oder dem Stand der Technik entsprechende Anforderungen entweder überhaupt nicht oder nach dem Stand der Wissenschaft und Rechtsprechung unzureichend umgesetzt wurde. Es handelt sich um eine Abweichung von den geforderten Kriterien. Bei dieser Bewertung als nicht-konform kann insgesamt keine Vergabe des Gütesiegels erfolgen, auch wenn andere Aspekte im Audit besser bewertet wurden.

1 Punkt: die Anforderungen sind zwar noch konform umgesetzt, jedoch besteht aus Sicht der Auditoren Verbesserungsmöglichkeit. Diese Bewertung kann bei einer Bewertung eines anderen Aspektes des Moduls mit „3“ ausgeglichen werden.

2 Punkte: die Anforderungen sind adäquat / konform zu den Anforderungen erfüllt: diese Bewertung erfordert eine zum Audit-Zeitpunkt bereits erfolgte Umsetzung aller gesetzlichen und technischen Mindestanforderungen.

3 Punkte: die Anforderungen sind vorbildlich erfüllt: drei Punkte können vergeben werden, wenn das geprüfte Unternehmen über die gesetzlichen Erfordernisse hinaus weitergehende Anstrengungen unternommen hat, durch welche die Verbraucher- und Datenschutz-Belange unterstützt oder gefördert werden (privacy by design).

Dem Bewertungssystem liegt der Gedanke zugrunde, dass Verbesserungsmöglichkeiten bei einzelnen Aspekten mit überobligatorischer Umsetzung von Anforderungen bei anderen Aspekten ausgeglichen werden können. Dies soll ein Hilfsmittel sein, um den Gesamtkonformität des Webportals / Webservices zu den Anforderungen „messbar“ zu machen. Überall dort, wo gesetzliche Anforderungen nicht eingehalten werden, können Punkte aber erst vergeben werden, wenn die Abweichung beseitigt ist.

Beispiel: Ein Impressum, das die gesetzlichen Mindestangaben nicht enthält, kann erst dann mit zwei Punkten bewertet werden, wenn die fehlenden Angaben nachgeholt wurden. Auch die Vergabe nur eines Punktes ist vorher nicht möglich.

2.4. Die Gewichtung der Module

Das Bewertungssystem basiert neben der Punktevergabe auf dem Gedanken, dass die oben genannten Module unterschiedliche Gewichtung aufweisen. Die Gewichtung beruht auf der Schutzbedürftigkeit der in dem betreffenden Modul erhobenen und verarbeiteten Daten. Einbeziehung und Gewichtung von Modulen ist Aufgabe des Auditors und muss nachvollziehbar begründet werden.

Beispiel: Für einen Online-Shop sind die Module „Informations-Abruf“, „Individual-Dienstleistung“ und „Datenschutzmanagement“ anwendbar. Diese könnten z.B. mit 20% „M1“, 30% „M2“ und 50% „M3“ gewichtet werden, da es vor allem auf das grundsätzliche Datenschutzmanagement ankommt, weniger jedoch auf die reinen (Datenschutz-) Informationen der Webseite.

Eine Anmerkung zum Bewertungssystem: Die internet privacy standards sollen kein starres Korsett sein, in das eine Bewertung von Online-Dienstleistungen „hineingepresst“ werden muss. Es soll vielmehr als Hilfsmittel zur Begutachtung dienen, um ein möglichst homogenes Niveau sowie eine Vergleichbarkeit der Umsetzung von rechtlichen und technischen Anforderungen zu schaffen. Die Auditor*innen sind dabei aufgefordert, eigene Kenntnisse und Erfahrungen einfließen zu lassen und wenn es in Einzelfällen erforderlich erscheint, von dem vorgegebenen Bewertungsraster – mit entsprechender Begründung - abzuweichen.

2.5. Der Ablauf eines Audits nach den internet privacy standards

2.5.1. Zusammenstellung und Gewichtung der Module

Im ersten Schritt wird das Webportal vom lizenzierten ips-Auditor*innen gesichtet und die anwendbaren Module festgelegt. Im Anschluss erfolgt die Gewichtung der Module. Damit ist das „Prüfungsgerüst“ erstellt.

2.5.2. Kriterienprüfung, Punktevergabe und Berechnung des Ergebnisses

Nun erfolgt die eigentliche Prüfung anhand der Kriterien und die Dokumentation der Ergebnisse. Die jeweils erreichten Punkte werden am Ende eines jeden Moduls zusammengezählt. Anhand der zuvor bestimmten Gewichtung wird aus den erreichten Punkten eine Durchschnittspunktzahl (Ø-Punktzahl) für das jeweilige Modul errechnet. Die Ø-Punktzahl wird sodann in Relation zu der festgelegten Gewichtung des Moduls gesetzt und daraus ein Punktanteil ermittelt.

Beispiel: im Durchschnitt wurden im Modul 1 insg. 2,71 Punkte erreicht. Gewichtet wird M1 mit 20 %. Der Anteil der Punkte beträgt daher 0,54 Punkte.

Anschließend wird der Punktanteil aller Module zusammengerechnet. Diese Gesamtpunktzahl muss mindestens den Wert „2“ ergeben, anderenfalls gilt die Auditierung als nicht bestanden. Die Berechnung kann in einer Übersicht dargestellt werden, die z.B. wie folgt aussieht:

MODUL INFO-ANGEBOT	PUNKTE
Anbieterkennzeichnung	3
Datenschutzerklärung	3
Weiterleitung	2
Verantwortung f. Inhalte	2
Nutzungsdatenumgang	3
Kommerzielle Kommunikation	3
Datenvermeidung/-sparsamkeit	3
Gesamtpunkte/Maximalpunkte	19/21
Ø - Punktzahl	2,71
Gewichtung	10 %
Punktanteil M1	0,54
MODUL INDIVIDUALLEISTUNG	**PUNKTE**
Transparenz	3

materielle Voraussetzungen	2
Datenvermeidung/-sparsamkeit	2
Technisch-organisat. Sicherheit	3
Gesamtpunkte/Maximalpunkte	10 / 12
Ø - Punktzahl	2,5
Gewichtung	15 %
Punktanteil M2	0,375
Modul Datenschutzmanagement	**PUNKTE**
Betriebl. Datenschutzbeauftragte	3
Auftragskontrolle	2
Verfahrensverzeichnis	3
Datenschutzorganisation	3
Techn.-org. Sicherheit	3
Umsetzung von Betroffenenrechten	3
Gesamtpunkte / Maximalpunkte	17 / 18
Ø - Punktzahl	2,83
Gewichtung	45%
Punktanteil M3	1,274
Gesamtpunktergebnis	xxx

2.5.3. Dokumentation / Auditreport

Die Dokumentation (Audit-Report) muss – auch zur Erleichterung des Prüf-Aufwands der Vergabestelle – den Aufbau des Kriterienkataloges berücksichtigen, wobei ansonsten jedoch keine weitere Form vorgegeben ist. Im Audit-Report müssen die gefundenen Ergebnisse sowohl mit den aufgefundenen Abweichungen oder Empfehlungen aber auch mit den vorbildlichen Umsetzungen dargestellt werden. Dabei können auch Abbildungen der Web-Funktionen (z.B. Screenshots) hilfreich sein. Soweit negative Bewertungen erfolgen, müssen diese besonders begründet werden.

Der Audit-Report endet mit einer Empfehlung gegenüber der Vergabestelle, das ips Gütesiegel zu erteilen oder nicht.

Ferner erstellen die ips-Auditor*innen einen Entwurf für ein Kurzgutachten zur Vorlage bei der Vergabestelle. Dieses dient dazu, den Nutzer*innen des Web-Angebotes die Prüfergebnisse im Überblick zu erläutern. Das Kurzgutachten wird von der Vergabestelle ergänzt und bei erfolgreicher Vergabe des Gütesiegels veröffentlicht.

2.5.4. Vergabe des ips-Gütesiegels und Veröffentlichung des Ergebnisses

Die Vergabestelle der datenschutz cert GmbH prüft den Audit-Report auf Schlüssigkeit. Kommt auch sie zu dem Ergebnis, dass das Webportal alle Anforderungen der ips-Kriterien mit einer Gesamtnote von mindestens 2 Punkten umsetzt, wird das Gütesiegel erteilt. Die Vergabestelle kann allerdings auch von der Ansicht der ips-Auditor*innen abweichen und das Gütesiegel nicht erteilen, was dann seitens der Vergabestelle zu begründen ist.

Die Vergabestelle kann das ips-Gütesiegel erteilen. Hierzu wird zum einen das ips-Logo auf der Homepage (mindestens auf der Startseite) implementiert und mit einem Link versehen, über den Interessierte per Klick zum online bereitgestellten Kurzgutachten gelangen können. Das Kurzgutachten ist auf dem Server der datenschutz cert GmbH abgelegt und innerhalb des geprüften Angebotes mit dem ips-Logo verlinkt. Das ips-Logo, die Kriterienkataloge sowie Marke und Hinweise auf ein gültiges ips-Gütesiegel dürfen nur mit Genehmigung der Vergabestelle und auf der Grundlage der Vergabe- und Nutzungsbedingungen verwendet werden.

Das Gütesiegel ist bei gleichbleibendem Webangebot für einen Zeitraum von zwei Jahren gültig und kann nach Ablauf der Gültigkeit durch eine erneute Prüfung mit positivem Abschluss erneuert werden.

3. Modul 1 - Informationsabruf

3.1. Anbieterkennzeichnung

3.1.1. Rechtliche Grundlagen

Zur Gewährleistung des Selbstbestimmungsrechts der Nutzer, die zunächst einmal nur als Besucher das Telemedienangebot aufsuchen („ansurfen“) ohne konkrete Absicht, mit dem Anbieter vertragliche Bindungen eingehen zu wollen, kommt den Informationsverpflichtungen auch schon bei diesem ersten Kontakt eine große Bedeutung zu: der Nutzer möchte wissen, mit wem er es auf Anbieterseite zu tun hat, welche juristische und auch natürliche Person hinter dem u.U. nicht durch bloßes Durchblättern der Seiten erkennbaren Anbieter tatsächlich steckt. Hinzuweisen ist in diesem Zusammenhang auf die Bestimmungen zur Nennung der verantwortlichen Stelle, konkretisiert durch die Vorgaben zur Anbieterkennzeichnung bzw. Impressumspflicht (§ 5 TMG), und auf die sonstigen Informationspflichten gemäß § 6 TMG. Die Informationspflichten gelten für Telemedien, die geschäftsmäßig angeboten werden. Geschäftsmäßig ist eine Datenverarbeitung dann, wenn sie auf eine gewisse Dauer und Wiederholung angelegt ist, wobei auf die Intensität des Datenumgangs, nicht auf eine Gewinnerzielungsabsicht abgestellt wird. Zusätzlich können Spezialgesetze besondere Informationspflichten auferlegen. Beispielweise legt die Dienstleistungs-Informationspflichtenverordnung (DL-InfoV) den Dienstleistern die Erbringung von Informationspflichten auf. Der Rundfunkstaatsvertrag (RStV) legt in § 55 Abs. 2 besondere Impressumspflichten im Online Journalismus fest. Unternehmer müssen gemäß §§ 36, 37 des Verbraucherstreitbeilegungsgesetzes (VSBG) besondere Informationspflichten beachten. Der Katalog ist nicht abschließend, daher hat der Gutachter zu prüfen, ob Spezialgesetze einschlägig sind und diese in die Prüfung mit einzubeziehen.

Des Weiteren kommt den Informationsverpflichtungen der DSGVO eine besondere Bedeutung zu, weil für die Nutzer häufig nicht ohne weiteres erkennbar ist, wer für die Verarbeitung personenbezogener Daten verantwortlich ist und welche Daten erhoben werden. Diesem Umstand tragen die Datenschutzvorschriften Rechnung.

Ggf. können gesonderte Regelungen bezüglich der Transparenz Anwendung, wenn es sich um Telekommunikationsrecht oder besonders sensible personenbezogene Daten handelt. Diese speziellen Anforderungen sind hier auch, insbesondere in den weiteren Modulen dieses Kriterienkataloges zu betrachten.

3.1.2. Fragen

Wird eine AK überhaupt gegeben?

Enthält die AK Namen und ladungsfähige Anschrift des Anbieters, bei jur. Personen die Angabe des Vertretungsberechtigten, ggf. Stammkapitalangaben oder Hinweise auf eine Liquidation?

Enthält die AK Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post? Wenn es sich um eine zulassungsgebundene Tätigkeit handelt, die Angaben zur zuständigen Aufsichtsbehörde?

Enthält die AK (soweit erforderlich) Registerangaben bzw. Angaben zum Beruf und zur Kammerzugehörigkeit bzw. Berufsbezeichnung?

Werden (soweit erforderlich) Angaben zu den besonderen berufsrechtlichen Regelungen oder wie für Heilberufe oder Architekten, die von der Führung eines Titels abhängig sind, gemacht?

Wird – soweit vorhanden – die Umsatzsteueridentifikationsnummer angegeben?

Wird ggf. auf eingeschaltete Hosting-Services und sonstiger Service-Provider hingewiesen, soweit keine Datenverarbeitung im Auftrag vorliegt?

Sind die Angaben leicht erkennbar, unmittelbar erreichbar und ständig verfügbar?

Ist die AK direkt von der Leitseite (Homepage) aus verfügbar (one klick away)?

Ist der direkte Zugriff auf die AK von allen Seiten aus möglich?

Merke: Seit 2016 ist zudem die Einrichtung einer Plattform für die Online-Streitbeilegung (sogenannte „OS-Plattform“) vorgesehen. Diese soll Verbrauchern und Unternehmern eine zentrale Anlaufstelle für die außergerichtliche Beilegung von Online-Streitigkeiten bieten. Nach Artikel 14 Abs. 1 der EU-Verordnung Nr. 524/2013 haben „in der Union niedergelassene Unternehmer, die Online-Kaufverträge oder Online-Dienstleistungsverträge eingehen, sowie in der Union niedergelassene Online-Marktplätze [...] auf ihren Websites einen Link zur OS-Plattform ein[zustellen]. Dieser Link muss für Verbraucher leicht zugänglich sein. In der Union niedergelassene Unternehmer, die Online-Kaufverträge oder Online-Dienstleistungsverträge eingehen, geben zudem ihre E-Mail-Adressen an.“

Zusätzliche Fragen:

- Ist eine Online-Streitbeilegung vorgesehen?

- Weist der Betreiber des Webportals auf die Teilnahme oder Nichtteilnahme an einer Online Streitbeilegung hin?

Merke für E-Health Dienstleistungen: Im Gesundheitsbereich herrschen besondere Aufklärungspflichten. Außerdem sollte der Barrierefreiheit für Menschen mit Behinderungen Rechnung getragen werden. Hinzuweisen ist ferner auf die ggf. notwendige Benennung einer zuständigen Aufsichtsbehörde (z.B. bei Apotheken, Arztpraxen) in der Anbieterkennzeichnung. Auch auf die Unterrichtung über die Datenverarbeitung ist für besondere personenbezogene Daten, zu denen Gesundheitsdatengehören, ist ein besonderes Augenmerk zu legen. Des Weiteren unterliegt Werbung für Arzneimitteln besonderen Anforderungen (z.B. das Gesetz über die Werbung auf dem Gebiet des Heilwesens (HWG) oder die MBO-Ä)

Zusätzliche Fragen:

- Enthält das Impressum alle erforderlichen Angaben, insbesondere im Falle der Aufsicht die zuständige Aufsichtsbehörde sowie ggf. ein Hinweis auf Berufsordnungen?

- Ist die Unterrichtung barrierefrei wahrnehmbar?

- Wird der Patient über eine Möglichkeit zur Einsichtnahme seiner Daten durch Dritte unterrichtet?

- Enthält das Internetportal Werbung für Heilmittel o.Ä., welche für jeden Nutzer zugänglich ist?

- Sind für den Anbieter die speziellen Regelungen der Berufsordnung anwendbar?

- Befindet sich die Werbung lediglich auf Seiten innerhalb eines geschlossenen Benutzerkreises mit medizinisch-fachlicher Ausrichtung und wird der Zugang durch Registrierung, Passwörter etc. sichergestellt?

- Sind Fotos oder Abbildungen enthalten, die medizinisches Personal in Arbeitskleidung zeigen?

- Wird damit geworben, dass Methoden oder Angebote des Anbieters bestimmte Krankheiten oder Symptome lindern oder beseitigen können?

- Kann der Nutzer beim Online-Kauf von Arzneimitteln zugleich einen Beipackzettel abrufen?

3.1.3. Bewertung

0 Punkte:

- eine AK liegt nicht vor bzw. enthält nicht alle gesetzlich vorgesehenen Inhalte
- eine AK liegt nicht vor
- die AK ist grob unvollständig, elementare Inhalte fehlen
- die AK enthält insbesondere keine Informationen zur Kontaktaufnahme (E-Mail-Adresse fehlt)
- die AK ist nur von einer Unterseite erreichbar bzw. der Link ist schwer auffindbar
- eine AK ist vorhanden, enthält jedoch nicht alle gesetzlichen Vorgaben
- die AK enthält falsche/unzutreffende Angaben
- eine Online-Streitbeilegungsmöglichkeit fehlt bei angebotenen Online-Kaufverträgen oder Online-Dienstleistungsverträgen

1 Punkt:

- die AK entspricht formal nicht vollständig den gesetzlichen Vorgaben
- die AK ist nur Teil einer Gesamtinformation (bspw. gemeinsam mit Datenschutzerklärung oder sonstiger Kundeninformation)
- die AK ist nur von der Homepage erreichbar (nicht von weiteren Unterseiten)

- eine Online-Streitbeilegungsmöglichkeit bei angebotenen Online-Kaufverträgen oder Online-Dienstleistungsverträgen ist vorhanden aber nicht leicht zugänglich
- die Unterrichtung ist nicht barrierefrei wahrnehmbar (sofern der Anbieter zur Barrierefreiheit verpflichtet ist
- es findet keine Unterscheidung der Werbung für Fachkreise und Laien statt, wenngleich die Werbung selbst sich in den Grenzen des Zulässigen hält
- Käufer können eine Bewertung zum Heilmittelprodukt in Foren abgeben, deren Inhalte nicht regelmäßig kontrolliert werden, sofern erforderlich

2 Punkte:

- die AK entspricht den gesetzlichen Vorgaben
- alle gesetzlich vorgeschriebenen Informationen sind in der AK enthalten
- die AK ist inhaltlich richtig
- die AK ist von allen Seiten des Angebots per „one-click-away" abrufbar

3 Punkte:

zusätzlich zu den gesetzlichen Vorgaben enthält die AK weitere Informationen

- die AK enthält mehr Informationen als gesetzlich vorgeschrieben, z.B. Links auf bzw. Kurzabdruck gesetzlicher Vorschriften
- sonstige weiterführende Links

3.2. Besondere Informationspflicht bei kommerzieller Kommunikation

3.2.1. Rechtliche Grundlagen

§ 6 TMG enthält zusätzliche Verpflichtungen zur Kennzeichnung von „kommerziellen Kommunikationen", also solchen Formen der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren, Dienstleistungen oder des Erscheinungsbildes eines Unternehmens oder einer sonstigen Organisation bzw. natürlichen Person dienen, die eine Tätigkeit, Gewerbe, Handwerk oder freien Beruf ausübt. Dem Nutzer soll auf den ersten Blick deutlich gemacht werden, dass und mit welchen kommerziellen Anbietern er es zu tun hat. Darüber hinaus ist unlautere oder irreführende Werbung ist demnach gemäß § 1 bzw. 3 UWG verboten. Davon erfasst werden grundsätzlich auch Aussagen von Dritten, z.B. in Foren oder Gästebüchern des Internetportals, für die der Betreiber verantwortlich bleibt.

3.2.2. Fragen

Ist kommerzielle Kommunikation (Werbung, Verkauf) deutlich als solche erkennbar, sind ggf. Firmen- bzw. Produktlogos eingeblendet?

Ist bei kommerzieller Kommunikation die natürliche/jur. Person, in deren Auftrag sie erfolgt, klar identifizierbar?

Sind Preisnachlässe bzw. Zugaben oder Geschenke als solche erkennbar und sind die Bedingungen für ihre Inanspruchnahme zugänglich und verständlich?

Sind Preisausschreiben/ Gewinnspiele als solche erkennbar und die Teilnahmebedingungen zugänglich und als solche verständlich?

Können sich Dritte in Foren oder Gästebüchern über die angebotenen Produkte äußern? Werden diese Inhalte kontrolliert und ggf. entfernt?

3.2.3. Bewertung

0 Punkte: die gesetzlichen Vorgaben werden nicht eingehalten

- kommerzielle Kommunikation wird bewusst „getarnt“
- der Anbieter ist nicht zu identifizieren
- bei Zugaben, Geschenken bzw. Rabatten oder bei Preisausschreiben sind die Bedingungen für die Inanspruchnahme nicht abrufbar
- es wird nur ein „Strohanbieter“ angegeben

1 Punkt: die gesetzlichen Vorgaben werden nicht vollständig eingehalten

- die erforderlichen Angaben zu Teilnahme- bzw. Nutzungsbedingungen sind verklausuliert formuliert oder aus anderen Gründen schwer verständlich
- die erforderlichen Angaben sind nur schwer auffindbar

2 Punkte: die gesetzlichen Vorgaben werden eingehalten

- die kommerzielle Kommunikation wird als solche besonders gekennzeichnet
- der tatsächliche Anbieter wird genannt
- Teilnahme- und Nutzungsbedingungen sind leicht abrufbar
- die Teilnahme- und Nutzungsbedingungen sind verständlich

3 Punkte: die Unterrichtung erfolgt in vorbildlicher Weise

- es wird als Anbieter nicht nur die juristische Person, sondern auch der gesetzl. Vertreter benannt
- die Teilnahme- und Nutzungsbedingungen sind separat speicherbar oder druckbar

3.3. Datenschutzerklärung

3.3.1. Rechtliche Grundlagen

Sobald eine Datenverarbeitung stattfindet ist der Verantwortliche verpflichtet umfassenden Informations- und Mitteilungspflichten nachzukommen. Dazu gehören die Informationen über den Verantwortlichen sowie die Kontaktdaten des Datenschutzbeauftragten, die Art der Daten, die Datenverarbeitung, die Dauer der Speicherung, die Rechtsgrundlage, Übermittlung der Daten an Drittländer oder internationale Organisationen und die Rechte der Betroffenen Person. Dabei gilt ein besonderes Klarheits-

und Verständlichkeitsgebot. Die DSGVO schreibt eine umfassende unentgeltliche Unterrichtung des Nutzers zu Beginn der Erhebung über die Verarbeitung personenbezogener Daten vor. Gerade weil der Nutzer in diesem frühen Stadium häufig noch gar nicht damit rechnet und für den technischen Laien auch nicht ohne weiteres erkennbar ist, dass bereits mit Aufrufen der Seite(n) personenbezogene Daten erhoben werden (z.B. IP-Nr., Browsertyp, Uhrzeit und Dauer der Nutzung, Informationen über gesetzte Cookies etc.), ist es aus datenschutzrechtlicher Sicht umso wichtiger, dass der Nutzer darüber informiert wird, wer für die Datenverarbeitung verantwortlich ist und welche Daten erhoben werden. Diesem Umstand tragen die Vorschriften über die Unterrichtung Rechnung. Mit der Offenlegung der Verarbeitungsabsichten und der Konsequenzen der Erhebung und Speicherung personenbezogener Daten durch den Anbieter eines Dienstes soll erreicht werden, dass der Nutzer zu einem möglichst frühen Zeitpunkt Entscheidungsmöglichkeiten hinsichtlich des Weiteren Datenverarbeitungsprozesses erhält. Um dies zu gewährleisten müssen die Informationen transparent, leicht verständlich, übersichtlich, individuell und gezielt erfolgen. Die Unterrichtung hat in kindgerechter Sprache zu erfolgen, wenn sich die Datenverarbeitung an Kinder richtet. Besonders wichtig ist außerdem bei Einsatz automatisierter Entscheidungsfindung (Scoring) aussagekräftige Informationen über die verwendete Logik, die Tragweite und angestrebten Auswirkungen der Verarbeitung zu informieren. Die Informationen können auch gemäß Art. 12 Abs. 7 DSGVO in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigten Überblick über die beabsichtigte Verarbeitung zu vermitteln. In elektronischer Form dargestellte Bildsymbole müssen maschinell lesbar sein.

3.3.2. Fragen

Wird der Nutzer über die Identität des Verantwortlichen inklusive seiner Kontaktdaten (ggf. auch des Vertreters) unterrichtet?

Wird über die Kontaktdaten des Datenschutzbeauftragten informiert, sofern ein solcher bestellt wurde oder werden muss?

Erfolgt überhaupt eine Unterrichtung des Nutzers über das Ob und Wie der Erhebung, Verarbeitung und Nutzung personenbezogener Daten?

Ist die Unterrichtung über die Datenerhebung (soweit diese erfolgt) vollständig sowie inhaltlich und rechtlich korrekt?

Werden die Informationen dem Nutzer in leicht verständlicher Form präzise und transparent übermittelt?

Stehen die Informationen unentgeltlich zur Verfügung?

Wird über die Zwecke der Verarbeitung, die Kategorien personenbezogenen Daten und die Dauer der Speicherung informiert?

Sind, sofern aufgrund berechtigter Interessen Daten verarbeitet werden, diese Interessen genannt?

Informiert die Unterrichtung ggf. über die Empfänger der verarbeiteten Daten?

Informiert die Unterrichtung ggf., wenn gesetzlich oder vertraglich vorgeschrieben, über die Erforderlichkeit die Daten bereitzustellen?

Wird ggf. auf die Verarbeitung oder Übermittlung von Daten außerhalb des EWR (und die Maßnahme auf welche diese gestützt ist, bspw. EU Standardvertragsklauseln) hingewiesen?

Wird ggf. auf die Bildung von Nutzungsprofilen, die Nutzung automatisierter Entscheidungsfindung oder Profiling und das Widerspruchsrecht des Nutzers hingewiesen?

Wird ggf. auf Verfahren hingewiesen, die eine spätere Identifikation des Nutzers ermöglichen (z.B. Cookies, Web-Bugs)?

Erfolgt die Unterrichtung tatsächlich „vor" Beginn des Nutzungsvorgangs? Ist sie unmittelbar von der Homepage abrufbar?

Ist die Unterrichtung jederzeit (und von überall im Angebot) abrufbar?

Ist die Datenschutzerklärung für den durchschnittlichen Nutzer verständlich?

Ist sie auch für Kinder verständlich?

Erfolgt die allgemeine Unterrichtung in einer Datenschutzerklärung (Privacy Policy)?

Wird der Nutzer im Falle der Erstellung eines Benutzeraccounts darüber informiert, ob und wie eine Verknüpfung eines wählbaren Pseudonyms mit den ihn identifizierenden Daten erfolgt?

Werden dem Nutzer seine Rechte (bspw. auf Auskunft, Widerruf der Einwilligung, Beschwerde, Widerspruch, Benachrichtigung bei Verletzung, Berichtigung und Löschung) mitgeteilt?

Wird dem Nutzer sein Beschwerderecht bei einer Aufsichtsbehörde mitgeteilt?

Ist die Datenschutzerklärung aktuell?

3.3.3. Bewertung

o Punkte:

- die gesetzlichen Vorgaben werden nicht eingehalten
- es erfolgt überhaupt keine Unterrichtung
- es erfolgt nur ein pauschaler Hinweis, dass dem Datenschutz Rechnung getragen wird
- die Unterrichtung über die Datenverarbeitung stimmt mit den tatsächlichen Verhältnissen nicht überein
- die Unterrichtung ist grob unvollständig oder rechtlich fehlerhaft
- die Unterrichtung ist teilweise fehlerhaft
- die Informationen werden nicht unentgeltlich zur Verfügung gestellt
- die Datenschutzerklärung ist kompliziert und unverständlich geschrieben oder nicht auf der Sprache des Betroffenen verfügbar

- die Unterrichtung nennt die falsche Rechtsgrundlage für die Verarbeitung

1 Punkt:

- die gesetzlichen Vorgaben werden nicht vollständig eingehalten
- der Inhalt der Unterrichtung stimmt in unwesentlichen Punkten nicht mit der Geschäftspraxis überein
- die Unterrichtung erfolgt nicht separat, sondern gemeinsam mit allgemeinen Informationen über das Angebot oder im Rahmen von AGB
- die Unterrichtung nennt nicht den Verantwortlichen
- obwohl ein Datenschutzbeauftragter bestellt ist werden die Kontaktdaten nicht aufgeführt
- die Unterrichtung erfasst nicht alle Daten, die vom Anbieter erhoben bzw. verarbeitet werden
- es wird lediglich auf eine Übermittlung ins EWR Ausland hingewiesen, aber keine Grundlage wie das Privacy Shield erläutert
- die Unterrichtung ist nicht leicht verständlich
- die Unterrichtung erfasst nur einen Teil der erforderlichen Angaben
- die Unterrichtung ist erst dann einsehbar, wenn die Daten bereits erhoben worden sind
- die Unterrichtung informiert über alle Datenverarbeitungen aber nennt nicht die jeweiligen Widerspruchsmöglichkeiten
- die Unterrichtung wird nicht regelmäßig aktualisiert und angepasst
- die Unterrichtung ist kaum auffindbar

2 Punkte:

- die gesetzlichen Vorgaben werden eingehalten
- die Unterrichtung ist vollständig, es wird über alle erhobenen Daten informiert
- die Unterrichtung ist sowohl von der Homepage, als auch von den Unterseiten jederzeit über einen leicht auffindbaren Link abrufbar
- die Unterrichtung ist leicht verständlich und in einfacher Sprache formuliert, besonders wenn sie an Kinder gerichtet ist
- die Unterrichtung enthält keine rechtlichen Fehler
- die Unterrichtung ist aktuell
- die Unterrichtung enthält alle erforderlichen Angaben

3 Punkte:

- die gesetzlichen Vorgaben werden vorbildlich erfüllt
- auf die Unterrichtung wird gesondert hingewiesen

- die Unterrichtung ist ggf. separat speicherbar oder ausdruckbar
- die Unterrichtung wird in bestimmten Abständen erneuert, dies wird durch eine
- Versionsnummer mit Datum des aktuellen Stands dokumentiert
- die Unterrichtung enthält weitere Links zu datenschutzrechtlichen Vorschriften
- die Unterrichtung erfolgt in Kombination mit leicht verständlichen standardisierten Bildsymbolen

3.4. Information über Weitervermittlung

3.4.1. Rechtliche Grundlagen

Der Anbieter muss den Nutzer darüber informieren, wenn er ihn über einen Verweis auf seinen Seiten an einen anderen Diensteanbieter weitervermittelt. Eine solche Weitervermittlung findet immer dann statt, wenn der Nutzer bei Anklicken eines Links auf ein Angebot geleitet wird, für das ein anderer Anbieter i.S.d. TMG verantwortlich ist. Hintergrund ist, dem Nutzer eine höchstmögliche Transparenz zu gewährleisten. Wenn sich die Aufmachung der aufgerufenen Seiten nicht entscheidend verändert, merkt der durchschnittliche Nutzer oft nicht, dass er über mehrere Links auf dem Angebot eines anderen Anbieters gelandet ist. Wenn der Anbieter seiner gesetzlichen Pflicht nicht nachkommt, wird die Weitervermittlung für den Nutzer erst dadurch ersichtlich, dass sich die URL der aufgerufenen Seite geändert hat. Selbst dies muss dem durchschnittlichen Nutzer aber nicht ohne weiteres auffallen, wenn seine Aufmerksamkeit nur auf den Browserinhalt, nicht aber auf das Adressfenster gerichtet ist. Folge dieser unbemerkten Weiterleitung wäre, dass Nutzungsdaten in diesem Fall bei weiteren Anbietern erhoben und verarbeitet würden. Aus diesem Grund ist der Anbieter gesetzlich dazu verpflichtet, den Nutzer auf eine solche Weiterverweisung in geeigneter Form hinzuweisen.

3.4.2. Fragen

Wird eine Weitervermittlung zu einem anderen Anbieter überhaupt angezeigt?

In welcher Form wird die Weitervermittlung angezeigt?

Ist die Information auffällig und für den durchschnittlichen Nutzer verständlich?

Werden externe Werbe-Banner gekennzeichnet?

Welche Methoden werden zur Weitervermittlung verwendet (Web-Bugs, Skript-Dateien usw.)?

3.4.3. Bewertung

0 Punkte:

- die gesetzlichen Vorgaben werden nicht eingehalten

- es ist überhaupt nicht erkennbar, dass auf das Angebot eines dritten Anbieters verwiesen wird
- interne und externe Links werden nicht unterschieden (auch aus der Statusleiste des Browsers ist die Weitervermittlung nicht ersichtlich
- es erfolgt ein pauschaler Hinweis (möglicherweise auch nur in AGB), dass das Angebot Weitermittlungen enthält

1 Punkt:

- die gesetzlichen Vorgaben werden unzureichend erfüllt
- Links werden lediglich optisch hervorgehoben (Unterstrich bei mouse-over), ohne dass eine Trennung nach „intern“ und „extern“ deutlich gemacht wird
- der Anbieter, zu dem weiter verwiesen wird, wird nicht genannt oder
- der Server, an den weitervermittelt wird, wird nicht genannt

2 Punkte:

- die gesetzlichen Vorgaben werden vollständig eingehalten
- eine Weitervermittlung wird kenntlich gemacht
- durch einen Erläuterungstext
- in Form eines Pop-up-Fensters oder
- durch Anzeige eines Hinweises in der Statusleiste des Browsers
- die Information ist für den durchschnittlichen Nutzer so verständlich, dass die unterschiedlichen Verantwortlichkeiten verstanden werden können

3 Punkte:

- die gesetzlichen Vorgaben werden vorbildlich umgesetzt
- sobald der Mauszeiger über den Link fährt, öffnet sich eine QuickInfo (gelbes Fähnchen), welches auf die Weitervermittlung aufmerksam macht
- die QuickInfo nennt auch den Namen des Anbieters und den Server

3.5. Verantwortlichkeit für Inhalte

3.5.1. Rechtliche Grundlage

§ 7 TMG als zentrale Haftungsnorm des Multimediarechts stellt zunächst nur klar, dass sich aus dem Telemediengesetz keine Beschränkungen der Verantwortlichkeit für eigene Informationen ergeben. Grundsatz ist, dass der Inhalteanbieter für die eigenen Informationen nach den allgemeinen Gesetzen verantwortlich ist, es sei denn, aus den §§ 8 – 10 TMG ergibt sich etwas anderes. Unter „Information“ i.S.d. Vorschrift sind alle Angaben zu verstehen, die im Rahmen des jeweiligen Telemediums übermittelt oder gespeichert werden.

Ebenso grundsätzlich, wie der Diensteanbieter für eigene Inhalte verantwortlich ist, stellt § 7 Abs. 2 TMG klar, dass Diensteanbietern nicht eine allgemeine Verpflichtung

obliegt, die von ihnen übermittelten oder gespeicherten fremden Informationen zu überwachen und aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit bzw. rechtswidrige Inhalte hinweisen. Dieses Haftungsprivileg für fremde Inhalte entbindet die Anbieter jedoch nicht, speziellen Verpflichtungen zur Sperrung bestimmter Informationen (z.B. gerichtlichen oder verwaltungsbehördlichen Anordnungen), nachzukommen. Im Allgemeinen empfiehlt sich hier trotz des § 7 Abs. 2 TMG und der mittlerweile verbreiteten „Haftungsausschlüsse", in denen eine Distanzierung vom Inhalt externer Links zum Ausdruck gebracht wird, die im eigenen Web-Angebot präsentierten Inhalte in regelmäßigen Abständen auf etwaige rechtswidrige Inhalte zu überprüfen. Die zeitlichen Abstände solcher Überprüfungen sind dabei umso geringer, je öfter sich der Inhalt der Seiten ändert; soweit die Möglichkeit von Chat und anderen Foren gegeben ist, kann hier sogar eine tägliche Kontrolle erforderlich sein.

Soweit dem Nutzer Publikationsmöglichkeiten, beispielweise Blogs, Kommentierfelder oder Bewertungsportale, nur bei Bekanntgabe personenbezogener Daten entgeltlich oder unentgeltlich zur Verfügung gestellt werden, dürfen Bestandsdaten nur für die Begründung oder inhaltliche Ausgestaltung (bzw. Änderung) eines Vertragsverhältnisses erhoben werden – es sei denn, der Nutzer hat in die umfassendere Erhebung eingewilligt. Wenn diese Voraussetzung nicht vorliegt, dürfen personenbezogene Daten demnach nur in dem Umfang erhoben werden, in dem sie für den Publikationsdienst erforderlich sind. Dabei sind zwei Möglichkeiten zu unterscheiden:

Für den Fall, dass die zu veröffentlichenden gedanklichen Inhalte vor der Publikation redaktionell bearbeitet oder zumindest auf Einhaltung von Veröffentlichungsbedingungen überprüft werden, dürfte sich der erforderliche Datenumfang in der E-Mail-Adresse und einem Passwort erschöpfen: diese Daten reichen aus, um den Nutzer zumindest als Pseudonym zu identifizieren. Eine Ermittlung der wahren Identität ist hier aus keinem Grunde erforderlich. Wenn hingegen vor der Veröffentlichung keine weitere Überprüfung der Inhalte erfolgt, ist die Erbringung des Dienstes zwar auch nur mit den zuvor genannten Daten möglich, jedoch wäre es aus Anbietersicht zu rechtfertigen, wenn zusätzlich Bestandsdaten wie Name und Anschrift erhoben werden, damit die Möglichkeit besteht, Nutzer bei Veröffentlichung rechtswidrigen Inhalten zu identifizieren.

3.5.2. Fragen

Ist die Verantwortlichkeit für Inhalte vertraglich geregelt?

Werden die Verantwortlichkeitsregeln von §§ 7 ff. TMG beachtet?

Entsprechen die vertraglichen Regelungen auch der Zuordnung der Inhalte aus Empfängersicht (d.h. findet durch die vertraglichen Zuordnungen nicht eine „Umgehung" der Verantwortlichkeiten statt)?

Erfolgt eine Überwachung auf rechtswidrige (eigene) und fremde Inhalte?

3.5.3. Bewertung

o Punkte:

- das Bewusstsein für (verschiedene) Verantwortlichkeiten fehlt vollständig oder ist nicht geregelt
- das Bewusstsein für (verschiedene) Verantwortlichkeiten fehlt vollständig oder ist nicht geregelt verschiedene Diensteanbieter wirken bei der Diensteerbringung mit, die Verantwortlichkeiten sind jedoch nicht geklärt
- es gibt zwar schriftliche Vereinbarungen, diese entsprechen jedoch nicht den tatsächlich „aus Empfängersicht" zuordenbaren Inhalten
- das Angebot enthält rechtswidrige Inhalte

1 Punkt:

- die Verantwortlichkeiten sind zwar bekannt, Vorkehrungen zur Verhinderung von Verstößen werden aber nicht getroffen
- es gibt mündliche Absprachen über Verantwortlichkeiten, schriftliche Vereinbarungen bestehen nicht
- die Abgrenzung von Inhalten wird nicht überprüft

2 Punkte:

- das Bewusstsein für die Verantwortlichkeiten ist vorhanden und wird in der täglichen Praxis auch beachtet
- es gibt schriftliche Vereinbarungen über die Verteilung der Verantwortlichkeiten, diese werden auch regelmäßig überprüft
- die schriftlichen Vereinbarungen geben die tatsächlichen Verhältnisse wieder

3 Punkte:

- es herrscht eine hohe Sensibilität für die Verantwortlichkeit, dies wird dem Nutzer auch transparent gemacht
- fremde Inhalte, die durch technische Möglichkeiten als eigene erscheinen können (z.B. Chat, Foren etc.) werden in regelmäßigen Abständen überprüft
- auch Inhalte dritter Anbieter werden auf Rechtswidrigkeit überprüft und ggf. derartige Links gesperrt
- der Nutzer wird über die Verteilung der Verantwortlichkeiten gesondert informiert
- Nutzer können dem Anbieter rechtswidrige Inhalte mitteilen

3.6. Verarbeitung von Nutzungsdaten

3.6.1. Rechtliche Grundlage

Im Rahmen des reinen Info-Abrufs kommt i.d.R. noch keine rechtsgeschäftliche Bindung zwischen Nutzer und Anbieter zustande (von Seiten des Nutzers fehlt i.d.R. mangels Rechtsbindungswillen die erforderliche Willenserklärung). Aus diesem Grund dürfen Daten in diesem Stadium nur zur Ermöglichung der Diensterbringung erhoben werden, also nur für die technische Realisierung des Anzeigens der Angebots-Inhalte

im Browser des Nutzers, sowie der Interaktion zwischen Nutzer und Diensteanbieter. Gemäß Art 6 Abs. 1 lit. b DSGVO ist eine Verarbeitung von personenbezogenen Daten, ohne Einwilligung des Betroffenen zulässig, wenn es zur Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen erforderlich ist. Hierunter fällt auch die Verarbeitung der Bestandsdaten und Nutzungsdaten, die für die Verwendung des Telemediums notwendig sind. Zu diesen Nutzungsdaten zählen insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Während eines Seitenaufrufs erhobene Daten sind in der Regel Systemdaten (IP-Nr., Browsertyp), Nutzerkennungen, Standort der nachgefragten Ressource, Anfangs- und Endzeitpunkt der Nutzung, Hard- und Softwareumgebung, technischer Dienst, der genutzt werden soll (z.B. FTP) sowie Cookie-Informationen.

IP-Adressen

Während das Erheben von personenbezogenen Daten beim „Absurfen" eines Internet-Angebots bereits nur in eingeschränktem Umfang zulässig ist, bestehen hinsichtlich der Speicherung der so erhobenen Daten noch engere gesetzliche Grenzen. Nutzungsdaten dürfen über das Ende des Nutzungsvorgangs hinaus nur gespeichert werden, soweit diese für Zwecke der Abrechnung mit dem Nutzer im Zuge der Vertragserfüllung erforderlich sind. Wenn diese Voraussetzung vorliegt, handelt es sich bei den dann gespeicherten Daten um Abrechnungsdaten, die einem vertraglichen Zweck unterliegen können und dann ggf. länger zu speichern sind.

Bei der Mehrzahl der durch reinen Seitenabruf nutzbaren Inhalte erfolgt gegenüber dem Nutzer jedoch keine Abrechnung: die auf den Seiten verfügbaren Inhalte sind kostenlos aufruf-, bzw. speicherbar. Dies bedeutet wiederum für die Anbieter, dass sämtliche Nutzungsdaten unmittelbar nach Beendigung der Nutzung, also sobald der Nutzer das jeweilige Angebot verlässt (sei es durch Anklicken eines externen Links, durch Abbruch der Verbindung oder manuelle Eingabe einer neuen Adresse) zu löschen sind. Logfiles, also vom jeweiligen Web-Server automatisch erstellte Listen von IP-Nummern der Besucher, dürfen demnach nicht über den Nutzungszeitraum hinaus gespeichert werden. Lediglich zu revisionszwecken und zu Sicherheitszwecken (zum Schutz vor unbefugtem Zugriff, Störungen oder Angriffen) kann dies für einen Zeitraum von maximal sieben Tagen noch zulässig sein. Nach Ablauf dieser Zeit müssen IP-Adressen gelöscht oder anonymisiert werden.

Ein Nutzen personenbezogener Daten liegt vor, wenn die Daten konkret mit dem jeweiligen Personenbezug verwendet werden, entscheidend ist die Kenntnisnahme des Informationsgehalts der Daten: die rein statistische, meist automatisierte Auswertung von Web-Zugriffen stellt keine Nutzung i.S.d. Datenschutzvorschriften dar. Eine Nutzung der beim Info-Abruf erhobenen Nutzungsdaten ist, außer der Betroffene hat der Nutzung über die gesetzlich zulässigen Zwecke hinaus eingewilligt, nur zur Bildung pseudonymisierter Nutzungsprofile zulässig. Nutzungsprofile dürfen nur aus den Nutzungsdaten erstellt werden, die im gesetzlich zulässigen Rahmen erhoben wurden, also denjenigen Daten, die bei der Erbringung des Dienstes ohnehin angefallen sind. Soweit der Nutzer im Rahmen der allgemeinen Unterrichtung über die Datenverarbeitung nicht auf sein Widerspruchsrecht hingewiesen wurde, ist nicht nur

die Unterrichtung unvollständig, auch die Bildung von Nutzungsprofilen ist mit diesem Versäumnis unzulässig.

Cookies

Das Setzen von Cookies ist zunächst an §§ 25, 26 TTDSG zu messen. Ist danach eine Einwilligung notwendig, sind an diese enge Voraussetzungen geknüpft.

Das Datenschutzrecht gestattet gemäß Art. 6 Abs. 1 lit. a DSGVO die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, soweit eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Wirksame Einwilligungen müssen stets die Anforderungen des Art. 7 DSGVO erfüllen, also insb. auf einer tatsächlich freiwilligen Entscheidung des Betroffenen beruhen. Die Verarbeitung und Nutzung von Bestands- und Nutzungsdaten des Telemediums außerhalb des primären Erhebungszwecks bedarf stets der Einwilligung. Eine Einwilligung kann schriftlich, elektronisch aber auch mündlich erfolgen, muss jedoch durch den Verantwortlichen protokolliert werden. Der Nutzer muss die Einwilligung durch eine aktive Handlung, beispielweise durch Klicken einer leeren Checkbox, erteilen. Dagegen liegt keine wirksame Einwilligung vor, sofern die Checkbox bereits vorab angekreuzt sind (Urteil vom 1. Oktober 2019, Az. C-673/17 – Planet49 GmbH).

In jedem Fall muss dabei sichergestellt sein, dass der Betroffene, dessen Daten erhoben, verarbeitet oder genutzt werden sollen, tatsächlich Urheber der Einwilligung ist. Weiterhin muss der Inhalt der elektronischen Einwilligung für den Nutzer jederzeit abrufbar sein. Er soll in die Lage versetzt werden, den Inhalt einer von ihm abgegebenen Einwilligung auch dann zu erfahren, wenn ihm nur bekannt ist, welchem Diensteanbieter gegenüber er sie abgegeben hat. Da der Diensteanbieter die Einwilligung protokollieren muss, hat er dem Nutzer im Übrigen Auskunft über die Tatsache und den Inhalt der Einwilligung zu erteilen, etwa wenn der Nutzer sich nicht mehr mit Sicherheit daran erinnern kann, ob er eine Einwilligung erteilt hat. Jederzeit abrufbar ist eine Einwilligung dann, wenn der Nutzer auf sie rund um die Uhr über das Internet zugreifen kann.

Insbesondere für die Einwilligung zur Nutzung von Cookies oder Trackings Pixeln hat sich der Einsatz von sogenannten Cookie-Bannern etabliert. Dabei stehen eine konkludente und eine ausdrückliche Einwilligung zur Verfügung. Eine konkludente Einwilligung über ein Cookie-Banner bei der die reine Weiternutzung der Webseite als Einwilligung gewertet wird, ist nicht zulässig, wenn der Webseitenbetreiber die Einwilligung nicht nachweisen kann. Wird beispielsweise ein Cookie-Banner lediglich angezeigt und die Einwilligung einfach wegen „Weitersurfens“ unterstellt (Urteil vom 1. Oktober 2019, Az. C-673/17 – Planet49 GmbH) liegt keine wirksame Einwilligung vor. Umfasst ein Cookie-Banner einen Button zum Bestätigen der Einwilligung des Nutzers stellt dies, sofern protokolliert und nachweisbar eine wirksame Einwilligung dar. Die Datenverarbeitung darf erst nach Abgabe Einwilligung beginnen, der Webseitenbetreiber muss also durch technische und organisatorische Maßnahmen sicherstellen, dass auf der Einstiegseite vorher keine Verarbeitung, z.B. Tracking, durchgeführt wird.

Werden Cookies eingesetzt, um gezielt Werbung auf den besuchten Webseiten einzublenden, sind auch Vorgaben der Aufsichtsbehörden zum sogenannten Behavioral Targeting als Auslegung heranzuziehen.

Webtracking / Reichweitenmessung

Für die Bewertung an dieser Stelle zu berücksichtigen ist der Einsatz von Webtracking-Verfahren (auch sogenannte Reichweitenmessung), mit denen das Nutzerverhalten ausgewertet wird (z.B. Google Analytics, etracker, Matomo etc.).

Die Messung des Webpublikums und Nutzungsanalyse kann durch den Betreiber selbst durchgeführt werden. In diesem Fall kann die Datenverarbeitung nach Ansicht der Datenschutzaufsichtsbehörden noch auf ein berechtigtes Interesse des Anbieters zur Optimierung der Webseitendarstellung i.S.d. Art. 6 Abs. 1 lit. f DSGVO gestützt werden.[1] Dem Nutzer muss in diesem Fall eine Widerspruchsmöglichkeit gewährt werden.

Eine Einwilligung i.S.d. Art. Art. 6 Abs. 1 lit. a DSGVO hingegen ist erforderlich, wenn die Datenverarbeitung nicht unbedingt erforderlich ist um die Webseite zur Verfügung zu stellen. Eine Einwilligung des Nutzers ist daher erforderlich, wenn das Nutzerverhalten ausgewertet wird, die Einbindung eines Dritten die Weiterleitung oder die Verkettung von Daten über das Nutzerverhalten ermöglicht.[2]

Wird zur Durchführung der Messung des Webpublikums und Nutzungsanalyse das Tool eines Dritten eingesetzt, ist eine vertragliche Grundlage für die Datenverarbeitung durch diesen Dritten erforderlich. Dies kann eine Auftragsverarbeitung i.S.d. Artikel 28 DSGVO sein, dann muss ein Vertrag zur Auftragsverarbeitung zwischen dem Anbieter und diesem Dritten vorliegen. Ist der Dritte nicht weisungsgebunden und bestimmt die Datenverarbeitung im Zusammenhang mit dem Tracking teilweise selbst, ist die gemeinsame Verantwortlichkeit zwischen dem Anbieter und dem Dritten in einem Vertrag entsprechend der Anforderungen des Artikel 26 DSGVO zu vereinbaren.

Nach unserem Verständnis sind daher folgende Möglichkeiten zulässig:

- die vorübergehende, eigene Speicherung und Auswertung der Nutzungsdaten (auch IP-Adressen der Nutzer) für einen kurzen Zeitraum (7 Tage) zum Zweck der Sicherstellung der Systemsicherheit gemäß § 100 Abs. 1 TKG und/oder zur eigenen statistischen Auswertung der Zugriffe, sofern ein Hinweis auf das Widerrufsrecht der betroffenen Person erfolgt.
- die Inanspruchnahme eines Dienstleisters als Auftragsverarbeiter zum Zweck der vorgenannten Auswertung auf Grundlage durch eine lokale Implementierung einer Analysesoftware. Der Dienstleister verfolgt kein eigenes Interesse an der Auswertung, eine Weitergabe der Daten an den Dritten oder eine Nutzungsprofilbildung erfolgt nicht. Die Zusammenführung mit Daten von anderen Webseiten ist ausgeschlossen und der Auftraggeber hat jederzeitige Einflussmöglichkeit auf die Nutzungsdaten. Der Nutzer kann jederzeit seinen Widerspruch ausüben und die Verarbeitung der Nutzungsdaten für statistische Analysen wird nach Ausübung eines Widerspruchs sofort beendet. Die Analyse dient nur dem Interesse das Webangebot zu optimieren und die Darstel-

---

1 Vgl. DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand März 2019, S. 12

2 Vgl. EuGH, Urteil vom 1. Oktober 2019 (Az. C-673/17 – Planet49 GmbH; Stellungnahme des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg, Zum Einsatz von Cookies und Cookie-Bannern – was gilt es bei Einwilligungen zu tun (EuGH-Urteil „Planet49“)? Vom 9. Oktober 2019, online abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/zum-einsatz-von-cookies-und-cookie-bannern-was-gilt-es-bei-einwilligungen-zu-tun-eugh-urteil-planet49/ (abrufbar Januar 2023).

lung an die Endgeräte anzupassen. Der Anbieter hat eine Interessenabwägung anhand der „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“ der DSK vorgenommen, welche kein überwiegendes Interesse des Nutzers ergeben hat.

- die Inanspruchnahme eines Dienstleisters als Auftragsverarbeiter oder im Rahmen einer gemeinsamen Verantwortlichkeit zum Zweck der vorgenannten Auswertung auf Grundlage einer wirksamen Einwilligung des Nutzers unter Hinweis auf dessen Widerrufsrecht, sofern die Auswertung nicht unbedingt erforderlich ist um die Webseite zur Verfügung zu stellen.

Bei der Bewertung ist der Sinn und Zweck der DSGVO und des Datenschutzrechts in den Vordergrund zu stellen. Dabei soll auch die aktuelle Auslegung der Datenschutzaufsichtsbehörden zur Reichsweitenmessung und zur Auslegung der E-Privacy Verordnung Berücksichtigung finden.

Beispiel: Ein Anbieter setzt Matomo zur Reichweitenmessung ein. Er hat eine Interessenabwägung vorgenommen, welche zu Gunsten seines berechtigten Interesses ausgefallen ist. Es findet keine Übermittlung von Daten an Matomo statt, Matomo wird auf den eigenen Rechnern gehostet. Die Daten werden anonymisiert, die Verarbeitung wird transparent in der Datenschutzerklärung erklärt und dem Nutzer wird eine Widerspruchsmöglichkeit gegeben. Hier kann der Einsatz mit 2 Punkten bewertet werden.

Wird ein Tracking über den Zweck der eigenen Besuchermessung hinaus eingesetzt, etwa für Zwecke der Werbung, Marktforschung oder bedarfsgerechten Gestaltung der Telemedien, muss die Verarbeitung auf einer Einwilligung des Nutzers beruhen.

Hierzu können Nutzungsprofile unter einem Pseudonym erstellt werden, also einem Kennzeichen, welches zwar zur Bestimmung des Betroffenen herangezogen werden kann, ihn aber nicht unmittelbar identifiziert. Dies gilt jedoch nur, wenn der Nutzer in diese spezielle Art der Nutzung wirksam eingewilligt hat und auf sein Widerrufsrecht im Rahmen der allgemeinen Unterrichtung über die Datenverarbeitung hingewiesen wird (sog. opt in – Lösung).

Rechtskonforme Einbindung von Social Networks

Eine Darstellung des Anbieters in sozialen Netzwerken, wie meta, instagram, twitter etc. ist in der Regel nicht Gegenstand einer ips-Zertifizierung. Der Anbieter kann allerdings auf seinen Webseiten sogenannte Social Plugins oder Verlinkungen zu seinem Profil auf einem Sozialen Netzwerk einbinden (z.B. den „Gefällt-mir-Button“ / „I-Like“). Soweit hierbei personenbezogene Daten erfasst werden oder eine individuelle Profilbildung möglich wäre, ist dies datenschutzrechtlich äußerst kritisch zu sehen und führt grundsätzlich zu einem Ausschluss der Zertifizierungsfähigkeit dieses Webangebotes.

Zertifizierungsfähig sind hingegen folgende Umsetzungen:

Wenn der "Gefällt mir" Button bzw. das Logo als einfache Verlinkung eingebunden wird, führt dies dazu, dass eine Datenverarbeitung erst dann in Gang gesetzt wird, wenn der Nutzer den Link aktiv anklickt. Bei der Verlinkung sollte ein Logo verwendet

werden, welches nicht beim Sozialen Netzwerk liegt, um eine systematische Auswertung im Ansatz zu verhindern.

Ferner ist es technisch realisierbar, Webseitenbesucher individuell vor der Einbindung eines Social Plugins um Erlaubnis zu fragen - entweder bei erstmaligem Aufruf der Startseite oder konkret vor jeder Nutzung des Buttons. Erteilt der Nutzer seine Einwilligung nicht, kann er zwar die Webseite besuchen, das Social Plugin bleibt allerdings deaktiviert.

Aufsichtsbehörden haben sich zu den konkreten Einbindungsmöglichkeiten von Social Plugins geäußert. So geht der Landesbeauftragte für den Datenschutz in Baden-Württemberg (LfDI BW) unter Ziffer 4.6 seines 30. Tätigkeitsberichts auf den sogenannten Zwei-Klick-Button ein. Dem Tätigkeitsbericht ist zu entnehmen, dass der LfDI BW diese Lösung "vorübergehend toleriert". Durch den Zwei-Klick-Button soll verhindert werden, dass bereits der Aufruf einer Internetseite mit integriertem Social Plugin zu einer Datenübertragung an den Betreiber der Social Media Plattform führt. Alternativ dazu besteht die sogenannte Sharif-Lösung von Heise, die nur noch einen Klick benötigt.

Zwar sind auch diese Lösungen nicht unumstritten, stellen derzeit jedoch praktikable Lösungen dar, mit welchen die Webseitenbetreiber versuchen können, etwaige Datenschutzverstöße von Social Media Diensten zu kompensieren.

Von einer direkten Einbindung des "Gefällt mir" Buttons als Social Plugin ist hingegen abzuraten.

Beispiel: Ein Anbieter setzt ein Plugin von meta ein. Er setzt dabei die Anforderungen des Landesbeauftragten für den Datenschutz in Baden-Württemberg bzw. die sogenannte „Heise-Lösung“ um. Hier kann der Einsatz noch mit 2 Punkten bewertet werden.

3.6.2. Fragen

Welche Nutzungsdaten werden vom wem erhoben und gespeichert und an wen übermittelt?

Werden Nutzungsprofile (NP) erstellt? Welche Daten gehen in die NP ein? Wie werden die Daten individuell zugeordnet? Für welche Zwecke werden die NP erstellt? Wie werden die ggf. verwendeten Pseudonyme gebildet?

Hat der Nutzer ein Widerspruchsrecht gegen die Verwendung seiner Daten?

Wird die IP-Adresse des Nutzers erfasst und wenn ja von wem und wofür?

Beschränkt sich die Erhebung der Nutzungsdaten auf diejenigen Daten, die für die Erbringung bzw. Abrechnung des jeweiligen Dienstes erforderlich sind?

Werden die Daten grds. nur für den Zweck verarbeitet, für den sie erhoben wurden?

Werden Cookies gesetzt? Welche? Wie wird der Nutzer darüber informiert? Kann er widersprechen?

Werden Tracking Pixel eingesetzt? Welche? Wie wird der Nutzer darüber informiert? Kann er widersprechen?

Werden in Cookies oder Trackings Pixeln gespeicherte Daten ausgelesen? Welche Daten werden dabei für welche Zwecke erhoben?

Bei Einsatz von Webtracking-Tools oder Social Plugins: werden die aktuellen Vorgaben der Datenschutzaufsichtsbehörden umgesetzt?

3.6.3. Bewertung

0 Punkte:

- die Datenverarbeitung überschreitet den gesetzlichen Rahmen erheblich
- Bestands-, Nutzungs- oder Abrechnungsdaten werden unzulässig erhoben, verarbeitet oder genutzt, es werden Daten erhoben, die zur Nutzung nicht erforderlich sind
- NP werden unter voller Identität des Nutzers (soweit hierzu personenbezogene Daten erhoben wurden) erstellt
- der Nutzer wird auf sein ggf. bestehendes Widerspruchsrecht nicht hingewiesen
- der Nutzer kann den Dienst ohne Zustimmung zur Verwendung seiner Daten in NP nicht in Anspruch nehmen
- Nutzungsdaten (IP-Adressen) werden ohne Zeitbegrenzung gespeichert
- es werden Methoden des Webtrackings eingesetzt, mit denen - auf Veranlassung, aber ohne Einflussmöglichkeit des Anbieters - Nutzungsdaten unter Einschluss der IP-Adresse an einen Auftragnehmer durch dessen Tools (Skripte, übergreifender Cookie-Zugriff etc.) gelangen und dieser kann die Nutzungsdaten für eigene Zwecke auswerten
- die personenbezogenen Daten werden – entgegen gesetzlicher Vorgaben - ohne Einwilligung des Betroffenen für die Bildung von Nutzungsprofilen über die Grenzen der Webseite oder Werbezwecke verwendet
- die erhobenen Daten sind zwar für die Erbringung des Dienstes erforderlich, werden aber zusätzlich noch für andere Zwecke verwendet, eine Information des Nutzers findet nicht statt, eine Einwilligung erfolgt nicht
- bei Einsatz von Webtracking-Tools werden die aktuellen Vorgaben der Datenschutzaufsichtsbehörden nicht umgesetzt
- trotz Einwilligungserfordernis beginnt das Tracking bereits vor Abgabe der Einwilligung
- beim Einsatz von Social Plugins werden die aktuellen Vorgaben der Datenschutzaufsichtsbehörden nicht umgesetzt.
- NP werden zwar pseudonym erstellt, können aber technisch einfach mit dem Träger des Pseudonyms zusammengeführt werden

1 Punkt:

- die Datenverarbeitung überschreitet den gesetzlichen Rahmen geringfügig

- die erhobenen Daten sind nicht sämtlich für die Erbringung des Dienstes erforderlich, werden aber nicht an Dritte weitergegeben
- zusätzliche Daten werden zwar abgefragt, der Dienst wird aber auch ohne die Angabe dieser Daten erbracht
- Nutzungsdaten werden erst nach einem längeren Auswertungszeitraum (z.B. eine Woche) gelöscht
- Die vom Anbieter durchgeführte Interessenabwägung für den Einsatz eines Webtracking Tools fällt zu Gunsten des Verantwortlichen aus, obwohl die Umsetzung eine andauernde Wiedererkennung oder eine Weitergabe von Daten an Dritte ermöglicht.
- NP und die zugrundeliegenden „Träger-identifizierenden" Nutzungsdaten werden getrennt verarbeitet und können nicht zusammengeführt werden

2 Punkte:

- es werden nicht mehr personenbezogene Daten erhoben als gesetzlich zulässig
- die Verarbeitung von Nutzungsdaten beschränkt sich auf den gesetzlich zulässigen Umfang
- Nutzungsdaten werden spätestens sieben Tage nach Beendigung des Nutzungsvorgangs gelöscht, pseudonymisiert oder anonymisiert
- der Nutzer wird auf sein Widerspruchsrecht hingewiesen
- Für Verarbeitung von Nutzungsdaten zur Bildung von NP basiert auf einer wirksamen Einwilligung des Nutzers unter Hinweis auf dessen Recht auf Widerruf.
- der Nutzer kann den Dienst auch ohne Zustimmung in die Verarbeitung seiner Daten für NP in Anspruch nehmen
- bei Einsatz von Webtracking-Tools werden die aktuellen Vorgaben der Datenschutzaufsichtsbehörden umgesetzt.
- Der Anbieter hat für Reichweitenmessungen auf der Grundlage eines berechtigten Interesses des Verantwortlichen eine Interessenwägung anhand der Vorgaben der Aufsichtsbehörden durchgeführt, welche zu Gunsten des Verantwortlichen ausfällt
- soziale Netzwerke sind per Logo verlinkt, ohne dass hierüber personenbezogene Daten erfasst oder an das Netzwerk übermittelt werden.
- bei der Einbindung von Social Plugins wird die 2-Klick-Lösung umgesetzt.

3 Punkte:

- es werden weniger personenbezogene Daten erhoben, als gesetzlich zulässig
- die Inanspruchnahme wird anonym ermöglicht; technisch erforderliche Nutzungsdaten mit direktem oder indirektem Personenbezug werden nicht gespeichert

- auf Tools zur Reichweitenmessung wird verzichtet, es werden keine NP erstellt
- NP werden mit der Erstellung anonymisiert, eine spätere Verknüpfung mit dem Nutzer ist nicht mehr möglich
- es werden keine Nutzungsdaten an dritte Diensteanbieter übermittelt

3.7. Datensparsamkeit im Hinblick auf Nutzungsdaten

3.7.1. Rechtliche Grundlage

Das Gebot zur Datenvermeidung ergibt sich aus Art. 5 DSGVO. Danach haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Bereits bei der Systemgestaltung ist durch gezielte Auswahl der Software und ihrer Konfiguration das Ziel der Datenvermeidung in der Weise zu realisieren, dass beim bloßen Informationsabruf, also dem „Besuch" des Internet-Angebots möglichst wenige Datenspuren hinterlassen werden.

3.7.2. Fragen

Ist bei der Gestaltung und Auswahl des Systems das Ziel beachtet worden, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen?

Werden personenbezogene Nutzungsdaten frühestmöglich anonymisiert bzw. pseudonymisiert?

Ist der Web-Server so konfiguriert, dass eine Vollprotokollierung der Nutzungsdaten unterbleibt?

Ist der Web-Server so konfiguriert, dass die zunächst vollständig protokollierten Daten kurzfristig anonymisiert bzw. pseudonymisiert werden?

Wird die Nutzung von der Angabe umfassender (für die Nutzung nicht benötigter) Daten abhängig gemacht?

Hat der Nutzer die Wahl, ob er personenbezogene Daten mitteilt?

Kann das Medium anonym in Anspruch genommen werden?

Ist die Nutzung des Mediums unter Pseudonym möglich?

3.7.3. Bewertung

0 Punkte:

- Datensparsamkeit ist in keinem Stadium berücksichtigt
- weder bei der Wahl der Software, noch bei der Gestaltung des Dienstes ist Datensparsamkeit berücksichtigt worden
- die Nutzung ist nicht anonym oder unter Pseudonym möglich

1 Punkt:

- die gesetzlichen Vorgaben sind nur marginal umgesetzt worden
- die Nutzung wäre mit geringem technischem und finanziellem Aufwand anonym oder unter Pseudonym möglich

2 Punkte:

- die gesetzlichen Vorgaben sind angemessen umgesetzt worden
- auf das Erfordernis der Datensparsamkeit ist durch Wahl von Software oder Konfiguration des Dienstes geachtet worden
- die Nutzungsdaten werden direkt im Anschluss an die Nutzung anonymisiert

3 Punkte:

- soweit technisch und finanziell möglich, sind Maßnahmen zur Datensparsamkeit umgesetzt
- die Nutzung des Dienstes ist vollständig anonym möglich
- es sind weitere, besondere Maßnahmen zur Datensparsamkeit getroffen

4. Modul 2 – Individual-Dienstleistung

In dieser Komponente des Kriterienkatalogs werden die besonderen datenschutzrechtlichen Anforderungen beschrieben, die mit den jeweils angebotenen Online-Dienstleistungen zusammenhängen. Erfasst werden zudem Dienste, deren Angebot durch den Nutzer selbst personalisierbar ist. Dabei müssen sowohl das allgemeine Datenschutzrecht als auch internetspezifische Aspekte betrachtet werden. Aufgrund der Vielfalt an Möglichkeiten in der Ausgestaltung von Individualdienstleistungen bietet dieses Modul verschiedene Unterkategorien an, anhand derer die speziellen Anforderungen für Dienstleistungen im Bereich E-Health-Dienste, Presseportale, Bürgerportaldienste, Registrierungsvorgänge, Anmeldungen an Online-Accounts oder Online-Einwilligungsfunktionen geprüft werden können. All diese Dienstleistungen haben gemeinsam, dass für die dabei verarbeiteten personenbezogenen Daten die Bestimmungen der DSGVO und der Anpassungsbestimmungen in den EU-Mitgliedstaaten anhand der Öffnungsklauseln zum Tragen kommen. Dieses Modul ist allgemein ausgerichtet und betrachtet die Zulässigkeit der Datenverarbeitung im Rahmen der Online-Dienstleistung. Dies kann die Zusendung eines E-Mail-Newsletters sein oder auch die Registrierung an einem geschlossenen Nutzeraccount etc. Im Hinblick auf die Kommunikation über das Internet ist die Sicherung der Authentizität der Vertragspartner, der Integrität der Inhalte und die Gewährleistung der Vertraulichkeit von besonderer Bedeutung. Für die Internet-spezifischen Aspekte kommt das Telemediengesetz (TMG) zur Anwendung, wobei ergänzend die Bestimmungen der DSGVO zum technisch-organisatorischen Datenschutz oder auch spezifische Vorgaben des TTDSG herangezogen werden müssen. Zudem können spezialgesetzliche, datenschutzrechtliche Anforderungen für die jeweilige Dienstleistung vorrangig zu betrachten sein.

4.1. Allgemeine Rechtmäßigkeit der Datenverarbeitung

Hier wird bewertet, inwieweit im Rahmen der individuellen Dienstleistung die gesetzlichen Vorgaben sowohl im Hinblick auf online-spezifische Rechtsvorschriften, als auch darüber hinaus im Hinblick auf weitere datenschutz-relevanten, materiellrechtliche Voraussetzungen eingehalten werden.

Verstöße gegen die gesetzlichen Vorgaben führen zur Abwertung und verhindern eine positive datenschutzrechtliche Bewertung.

4.1.1.1. Rechtliche Grundlagen

Für Individualdienstleistungen gelten grundsätzlich die Normen der DSGVO für die Verarbeitung von personenbezogenen Daten.

Merke: Hier sind nur die einschlägigen Unterkategorien für die jeweilige Dienstleistung zu betrachten. Dazu muss bestimmt werden welche individuelle Dienstleistung erbracht wird und die entsprechenden optionalen Anforderungen für die jeweilige Kategorie geprüft werden. Die Anforderungen der auf gelisteten Kategorien E-Commerce, E-Health oder Online-Einwilligung sind nicht abschließend.

Die Bandbreite der sonstigen in Frage kommenden rechtlichen Vorgaben ist dabei durchaus groß und kann in diesem Rahmen nicht abschließend genannt werden. Bei-

spielsweise kann die Individual-Dienstleistung die Verarbeitung besonders geschützter Daten (Sozialdaten, besonders vertrauenswürdige Daten i.S.d. § 203 StGB) beinhalten, so dass der Gutachter im Rahmen der Auditierung auch Gesetze heranziehen muss, die nachfolgend nicht explizit aufgeführt sind.

In jedem Fall ist der Prüfung dieser sonstigen materiellrechtlichen Voraussetzungen besonderes Gewicht zuzumessen – gerade aus dem Grund, da nicht alle möglicherweise im konkreten Fall in Betracht kommenden Vorschriften genannt werden (können).

4.1.2. Fragen

- Welche personenbezogenen Daten werden verarbeitet?
- Sind diese Daten zur Gestaltung bzw. Erbringung des Dienstes erforderlich?
- Welche Daten werden dabei für welche Zwecke erhoben?

4.1.3. Bewertung

0 Punkte: Die Datenverarbeitung überschreitet den gesetzlichen Rahmen erheblich

- es werden zwangsweise Daten erhoben, die für die Abwicklung der Dienstleistung nicht erforderlich sind
- Daten werden ohne gesetzliche Erlaubnis und ohne wirksame Einwilligung des Betroffenen für andere Zwecke genutzt
- Nutzungsprofile werden mit Daten über den Träger des Pseudonyms zusammengeführt

1 Punkt: Die Erhebung überschreitet den gesetzlichen Rahmen geringfügig

- eine Prüfung entgegenstehender berechtigter Interessen des Betroffenen ist erforderlich, wird aber nicht oder nicht korrekt durchgeführt
- es werden geringfügig mehr Daten erhoben, als für die Abwicklung der Dienstleistung erforderlich ist

2 Punkte: Die Erhebung entspricht dem gesetzlichen Rahmen

- entgegenstehende überwiegende schutzwürdige Interessen des Betroffenen werden geprüft und ggf. berücksichtigt
- die Datenverarbeitung hält sich insgesamt in den gesetzlich gezogenen Grenzen
- Nutzungsdaten werden nach Beendigung des Nutzungsvorgangs gelöscht, pseudonymisiert oder anonymisiert
- Widerspruchsrechte und Einwilligungsvorbehalte werden beachtet

3 Punkte: Es werden besondere Maßnahmen getroffen, um den Umfang der erhobenen Daten zu minimieren

- die mit Zweckänderungen verbundenen Nutzungen, insbesondere für Werbezwecke erfolgen stets auf Basis der Einwilligung

4.2. Zusätzliche Anforderungen für die E-Health-Dienstleistungen

In diesen Teil des Moduls können fallen z.B.:

- Digitale bzw. elektronische Gesundheitsakten
- Arzt-, Heilberufs-, Apotheken-, Medizinratgeber-, Telemedizin- oder Patientenportale
- Portale für den Versand von Arzneimitteln
- Gesundheitsforen
- Digitale Gesundheitsnetzwerke

Merke: Wie bereits zuvor angesprochen, bestehen aufgrund des vielfältigen Leistungsspektrums unterschiedliche rechtliche Anforderungen im Hinblick auf eine zulässige Datenerhebung und -verarbeitung. Aufgrund der großen Bandbreite der in Frage kommenden rechtlichen Vorgaben ist eine abschließende Benennung der einschlägigen Normen nicht möglich. Für den E-Health-Bereich kommen etwa Vorgaben zum Patientendatenschutz, zur ärztlichen Schweigepflicht oder zum Sozialdatenschutz in Betracht. Verstöße gegen die gesetzlichen Bestimmungen führen zur Abwertung und verhindern eine positive datenschutzrechtliche Bewertung. Zunächst sollte immer die Organisationsform oder Trägerschaft des Anbieters geklärt werden, da je nach Organisation unterschiedliche Gesetze zur Anwendung gelangen (z.B. als private juristische Person, öffentlich-rechtlicher Träger oder Religionsgemeinschaft). Ggf. ist auch nach dem jeweiligen Berufsstand zu fragen (z.B. Regelungen zum Arzneimittelvertrieb für Apotheker). Sämtliche Möglichkeiten, mit denen über das Internet personenbezogene Daten ausgetauscht werden, können an dieser Stelle nicht aufgezählt werden. Die nachfolgenden Punkte sollen daher nur darauf hinweisen, dass der Gutachter ggf. weitere Rechtsvorschriften heranziehen und prüfen muss.

Hervorzuheben ist, dass eine Prüfung nach diesen Anforderungen keine ggf. notwendige Prüfung nach dem Medizinproduktegesetz darstellen kann. Es wird also mit der ips-Prüfmethode keine Konformität zum Medizinproduktegesetz bewertet oder bescheinigt.

Beispiel: Verkaufs von Arzneimitteln und der Verarbeitung zu Forschungszwecken

Durch die Art. 2off. des Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung (GMD) ist öffentlichen Apotheken der Versand und der elektronische Handel von apothekenpflichtigen Arzneimitteln mit Endverbrauchern erlaubt. Für den Versand von Arzneimitteln, die auf dem elektronischen Wege bestellt werden können, gelten die Bestimmungen des Apothekengesetzes i.V.m. dem Arzneimittelgesetz i.V.m. der Apothekenbetriebsordnung.

Weitere Reglementierungen ergeben sich für Apotheker aus den entsprechenden Landesberufsordnungen.

Bei der Erhebung und Verarbeitung von Gesundheitsdaten durch nichtöffentliche Stellen über Webportale, die zu Forschungszwecken genutzt werden, handelt es sich um besondere personenbezogene Daten. In diesen Fällen ist ggf. Art. 89 DSGVO zu beachten. Grundsätzlich ist danach eine Erhebung und Verarbeitung nur mit Einwilligung des Betroffenen zulässig, es sei denn, sie ist - neben anderen Ausnahmetatbe-

ständen - zur Durchführung wissenschaftlicher Forschung erforderlich, wobei zum einen das Forschungsinteresse das Interesse des Betroffenen erheblich überwiegen muss und eine anderweitige Zweckerreichung nur mit unverhältnismäßigem Aufwand erreicht werden könnte. Auch zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik oder Behandlung ist die Verarbeitung zulässig, soweit sie durch Geheimhaltungsträger (Ärzte bzw. entsprechend Verpflichtete) vorgenommen wird. Daten, die für Forschungszwecke erhoben wurden, dürfen nicht zu anderen Zwecken genutzt werden. Es gilt insofern ein Zweckänderungsverbot. Ferner sind Daten so früh wie möglich zu anonymisieren. Unter Umständen reicht auch ein Pseudonymisieren aus.

4.2.1. Fragen

- Handelt es sich bei dem Portal um ein Angebot, welches den Gesetzen zum Vertrieb von Heil- und Arzneimitteln unterliegt (z.B. Online-Versandapotheke)?
- Ist eine Erlaubnis der Aufsichtsbehörde eingeholt worden? Wird darauf möglicherweise im Angebot hingewiesen?
- Welche Einrichtungen (Server, EDV, Provider) werden für den Versandhandel eingesetzt? Sind diese zuverlässig oder liegt z.B. eine Zertifizierung nach ISO 9001 vor?
- Wie lange dauert der Versand?
- Werden rezeptpflichtige Medikamente verkauft?
- Wie wird die Übergabe des Rezeptes an den Anbieter sichergestellt?
- Werden Produkte angemessen beschrieben?
- Wird die Packungsbeilage online zum Abruf bereitgehalten?
- Wird eine Beratung angeboten?
- Werden Proben, Zugaben oder anderweitige Zuwendungen in Verbindung mit dem Warenkauf angeboten?
- Wann und wie erfolgt die Auslieferung?
- Werden Gesundheitsdaten für Forschungszwecke genutzt und wenn ja, welche?
- Werden die besonderen Zulässigkeitsvoraussetzungen eingehalten, die erforderliche Interessenabwägung vorgenommen und das Ergebnis dokumentiert?
- Besteht die Gefahr, dass Daten, die zu Forschungszwecken erhoben wurden, auch für andere Zwecke genutzt werden?
- Werden die Daten anonymisiert oder pseudonymisiert?
- Ist eine Zusammenführung von Bestandsdaten mit Forschungsdaten möglich?
- Wird der Betroffene umfassend über den Verwendungszweck und ggf. die Datenweitergabe informiert?
- Sollen die Daten veröffentlicht werden?
- Wird – soweit erforderlich - eine Einwilligung eingeholt?
- Wird ein Widerspruch beachtet?
- Erhält der Betroffene Zugang zu seinen Daten?

4.2.2. Bewertung

0 Punkte:

- Der gesetzliche Rahmen wird nicht eingehalten
- eine notwendige Erlaubnis der Aufsichtsbehörde für den Online-Versandhandel von Arzneimitteln liegt nicht vor
- rezeptpflichtige Medikamente sind frei bestellbar
- Medikamente werden nicht oder nicht ausreichend beschrieben
- Medikamente werden von einem virtuellen Arzt („Cyber-Doc“) nach einer Online-Diagnose verordnet
- es werden nach der geltenden Landesberufsordnung in unzulässiger Weise Proben, Geschenke oder anderweitige Zuwendungen angeboten
- Versand- oder Wareninformationen zu Heilmitteln oder Arzneimitteln fehlen
- es wird keine Beratung zum Kauf von Medikamenten angeboten
- personenbezogene Daten werden über den Forschungszweck hinausgehend genutzt oder dafür an Dritte übermittelt
- auf ein Widerspruchsrecht wird nicht hingewiesen
- eine notwendige Einwilligung wird nicht eingeholt
- Daten werden unbefugt an Dritte weitergeleitet
- eine Interessenabwägung hat nicht stattgefunden
- Gesundheitsdaten können leicht mit den Bestandsdaten des Nutzers/Patienten zusammengeführt werden

1 Punkt:

- Der gesetzliche Rahmen wird nur geringfügig überschritten
- eine notwendige Erlaubnis der Aufsichtsbehörde liegt vor
- Medikamente werden anhand von Stichworten oder in knappen Ausführungen beschrieben
- gesetzliche Vorgaben zum Versand, zur Werbung oder Abgabe von Geschenken etc. werden nicht vollständig beachtet
- Versandfunktionen und Wareninformationen zu Heilmitteln oder Arzneimitteln sind wenig verständlich
- der Bestellvorgang wird ohne eine Warenkorbfunktion abgewickelt, dem Nutzer wird nicht Gelegenheit gegeben, den Stand seines Bestellvorganges einzusehen
- der Versand dauert länger als 2 Tage
- die Versandkosten sind unangemessen oder werden missverständlich oder gar nicht dargestellt
- der Transport oder die Verpackung der Medikamente ist unsicher. Die ausgelieferte Verpackung lässt auf den Inhalt bzw. den Medikamententyp schließen
- eine Beratung ist schwer zugänglich, die Fachkompetenz zweifelhaft
- eine Interessenabwägung der Datenverarbeitung zu Forschungszwecken ist nicht oder nur schwer nachvollziehbar

- die Information des Betroffenen über die Datenverarbeitung zu Forschungszwecken ist nicht angemessen
- Widerspruchsrechte zur Datenverarbeitung zu Forschungszwecken können nur schwerfällig durchgesetzt werden
- Daten zu Forschungszwecken werden erst zu einem späteren Zeitpunkt anonymisiert oder pseudonymisiert

2 Punkte:

- Die Verarbeitung entspricht dem gesetzlichen Rahmen
- für die Bestellung rezeptpflichtiger Medikamente muss der Nutzer zunächst eine ärztliche Verschreibung an den Anbieter übermitteln
- anhand einer Warenkorbfunktion kann der Nutzer den Bestellstatus während der Sitzung abfragen
- der Versand erfolgt zügig, i.d.R. innerhalb von 1-2 Werktagen
- die Versandkosten sind angemessen
- die Auslieferung erfolgt gesichert anhand einer neutralen Verpackung
- daten für Forschungszwecke werden zum frühestmöglichen Zeitpunkt pseudonymisiert oder anonymisiert
- die Zusammenführung von Bestandsdaten und Gesundheitsdaten für Forschungszwecke ist nur unter erschwerten Voraussetzungen im Einzelfall möglich und notwendig
- der Nutzer wird leicht verständlich über die Verwendung seiner Daten für Forschungszwecke informiert
- eine notwendige Einwilligung für Forschungszwecke wird eingeholt

3 Punkte:

- es werden zusätzliche, über das gesetzlich vorgeschriebene Maß hinausgehende Maßnahmen getroffen
- der Kunde erhält in jedem Fall Beratung, bevor er das Produkt bestellen kann
- Packungsbeilagen sind zugleich online abrufbar oder Medikament, Anwendung und Wirkung werden detailliert beschrieben
- Server, EDV oder Provider, mit denen der Arzneimittelversand abgewickelt wird, sind auf dem neusten technischen Stand
- es liegt z.B. eine Zertifizierung nach ISO 9001 vor
- der Nutzer wird mehrfach und umfassend über die Verwendung seiner Daten zu Forschungszwecken informiert
- die Daten zu Forschungszwecken werden unmittelbar nach Erhebung anonymisiert
- der Nutzer erhält online Zugang zu seinen Daten zu Forschungszwecken und kann diese verwalten (Berechtigungskonzepte können vom Nutzer erstellt und modifiziert werden)

4.3. Online-Einwilligungen

4.3.1. Rechtliche Grundlagen

Das Datenschutzrecht gestattet gemäß Art. 6 Abs 1 lit. a DSGVO die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, soweit eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Wirksame Einwilligungen müssen stets die Anforderungen des Art. 7 DSGVO erfüllen, also insbesondere auf einer tatsächlich freiwilligen Entscheidung des Betroffenen beruhen. Die Verarbeitung und Nutzung von Bestands- und Nutzungsdaten des Telemediums außerhalb des primären Erhebungszwecks bedarf stets der Einwilligung, während die zweckfremde Verarbeitung und Nutzung von Daten nach der DSGVO unter Umständen (insbesondere, wenn es sich um Zwecke der Direktwerbung handelt) zulässig ist, wenn der Betroffene nicht widerspricht. Eine Einwilligung kann schriftlich, elektronisch aber auch mündlich erfolgen, muss jedoch durch den Verantwortlichen protokolliert werden. Der Verantwortliche hat gemäß Art. 7 Abs. 3 den Nutzer vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen.

Merke für die Verarbeitung besonderer Kategorien personenbezogener Daten: gemäß Art. 9 Abs. 1 DSGVO bedarf es bei der Verarbeitung von Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, sowie genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person bedürfen zur Verarbeitung immer einer Einwilligung oder eines anderen Erlaubnistatbestandes aus Art. 9 Abs. 2 DSGVO durch den Betroffenen. Die Verarbeitung solcher besonderen Kategorien von Daten kann nicht auf die allgemeinen Erlaubnistatbestände aus Art. 6 DSGVO gestützt werden.

Sofern die Erhebung und Verarbeitung von besonderen personenbezogenen Daten nicht einem Vertragszweck unterfallen (z.B. Behandlungsvertrag im Falle von E-Health Dienstleistungen) unterliegen sie zumeist sehr eng gefassten und einzelfallbezogenen Erlaubnistatbeständen. In der Regel kommt daher der Einwilligung des Betroffenen eine besondere Bedeutung zu. Weitere Einwilligungserfordernisse können spezialgesetzlich geregelt sein, z.B. in Landesgesetzen (z.B. Landeskrankenhausgesetze, Verordnungen etc. für **E-Health Dienstleistungen**).

Merke für die Einwilligung durch Kinder gem. Art. 8 DSGVO: Die Einwilligung eines Kindes ist rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Ansonsten muss die Zustimmung der Eltern (oder eines anderen Trägers der elterlichen Verantwortung) erteilt werden. Der Verantwortliche muss sich unter Berücksichtigung der verfügbaren Mittel über die Erteilung dieser Zustimmung vergewissern. Dieser Sonderreglung unterliegen ausschließlich Angebote, die einem Kind direkt gemacht werden.

4.3.2. Fragen

- Werden Bestands- oder Nutzungsdaten auf Grund einer Einwilligung erhoben, gespeichert oder genutzt? Was ist Gegenstand dieser Einwilligungen?
- Liegt eine Verarbeitung von besonderen Kategorien personenbezogener Daten vor für die eine Einwilligung zwingend notwendig ist?
- Ist der Inhalt der Einwilligungserklärung in einfacher, klarer Sprache verständlich formuliert?
- Ist klar ersichtlich zu welchen Zwecken die Einwilligung gegeben wird (Bestimmtheit)?
- Ist die Einwilligungserklärung besonders hervorgehoben, soweit sie zusammen mit anderen Erklärungen abgegeben wird?
- Ist die Einwilligung tatsächlich freiwillig und frei von Zwängen; insbesondere wird die Nutzung des Dienstes nicht von der Einwilligung in die Nutzung der Daten für andere Zwecke abhängig gemacht, soweit ihm kein anderer Zugang möglich ist?
- Ist die Einwilligung jederzeit widerrufbar?
- Wird der Nutzer über seine Möglichkeit des Widerrufs mit Wirkung für die Zukunft unterrichtet?
- In welcher Form erfolgt die Einwilligung zur Erhebung, Verarbeitung und Nutzung bei Daten?
- Erfolgen Einwilligungserklärungen unter Einhaltung der elektronischen Form (§ 126a BGB)?
- Wie wird ggf. die Abweichung von der Schriftform bzw. elektronischen Form begründet? Welche zusätzlichen Maßnahmen werden ergriffen, um die Warn- und Beweisfunktion der Einwilligungserklärung zu gewährleisten?
- Werden Bestands- oder Nutzungsdaten auf Grund einer elektronischen Einwilligung erhoben, gespeichert oder genutzt?
- Erfolgt die elektronische Einwilligung durch bewusste und eindeutige Handlung des Nutzers?
- Wird bei elektronischer Einwilligung ohne gesicherte Authentifizierung des Nutzers auf einem anderen Kommunikationskanal eine Bestätigung an den Nutzer gesendet (confirmed opt in) oder eine zusätzliche Bekräftigung durch den Nutzer abgefordert (double opt in)?
- Wird die elektronische Einwilligung protokolliert?
- Ist der Inhalt der elektronischen Einwilligung jederzeit abrufbar?

- Wird bei Angeboten, die sich direkt an Kinder die Zustimmung der Eltern eingeholt, sofern das Kind das 16. Lebensjahr noch nicht vollendet hat?

4.3.3. Bewertung

0 Punkte: Von den gesetzlichen Vorgaben zur Einwilligung wird erheblich abgewichen

- die Einwilligung wird von einer unzulässigen Zustimmung zur Nutzung der Daten für andere Zwecke abhängig gemacht

- die Einwilligung erfolgt ohne Wahlfreiheit oder die Erbringung der Dienstleistung wird von einer Einwilligung abhängig gemacht (Kopplungsverbot)
- die Einwilligung des Nutzers wird unterstellt, wenn er nicht widerspricht
- trotz gesetzl. Erfordernisses wird keine Einwilligung eingeholt
- bei Kindern unter 16 Jahren wird die Zustimmung der Eltern nicht eingeholt

1 Punkt: Von den gesetzlichen Vorgaben zur Einwilligung wird geringfügig abgewichen

- die Einwilligungserklärung ist unklar formuliert
- der Verantwortliche kann nicht nachweisen, dass der Betroffene bei der Einwilligung ausreichend informiert war
- auf das Widerrufsrecht wird nicht hingewiesen

2 Punkte: Die Einwilligung erfüllt die gesetzlichen Anforderungen und ist widerrufbar

- die Einwilligung erfolgt durch bewusste Handlung des Nutzers
- die Einwilligung wird protokolliert und kann über einen Link vom Nutzer jederzeit abgerufen werden
- auf die Möglichkeit des jederzeitigen Widerrufs wird hingewiesen, der Hinweis ist leicht auffindbar und für den durchschnittlichen Nutzer verständlich
- die Einwilligung ist jederzeit widerrufbar
- der Widerruf kann schriftlich, elektronisch oder mündlich erfolgen

3 Punkte: Bei Einwilligungen werden besondere, über die gesetzlichen Anforderungen hinausgehende Datenschutzaspekte berücksichtigt

- die Einwilligung erfolgt in einem gesicherten Verfahren (Schriftform oder qualifizierte elektronische Signatur gem. § 126a BGB)
- auch für Fälle, in denen ohne Einwilligung Daten verarbeitet werden dürfen, etwa auf Grundlage legitimer Interessen des Verantwortlichen gem. Art. 6 Abs. 1 lit. f DSGVO (z.B. Nutzung von Daten für Zwecke der Direktwerbung), wird eine Einwilligung eingeholt

4.4. Datensparsamkeit bei Online-Formularen

4.4.1. Rechtliche Grundlagen

Das Gebot zur Datenvermeidung ergibt sich aus Art. 5 DSGVO. Danach haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Bezogen auf Individual Dienstleistungen ist die Datenvermeidung bei der Systemgestaltung durch die Auswahl solcher Software und ihre Konfiguration in der Weise zu realisieren, dass Angaben der Nutzer möglichst wenige Datenspuren hinterlassen. Dies kann etwa durch Pseudonymisierung oder Anonymisierung der Daten erfolgen.

Merke für E-Health Dienstleistungen: In die Überlegungen zur Datenvermeidung einbezogen werden muss ferner die Speicherdauer medizinischer Daten. Die hier gesetzlich vorgeschriebenen Aufbewahrungspflichten von zehn Jahren bzw. – bei Röntgenaufnahmen von Personen unter 18 Jahren bis zu deren 28. Lebensjahr - sind einzuhalten. Gleichwohl muss geprüft werden, ob eine Sperrung oder Pseudonymisierung der Daten auch zu einem früheren Zeitpunkt ermöglicht wird.

4.4.2. Fragen

- Ist bei der Gestaltung und Auswahl des Systems das Ziel beachtet worden, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen?
- Werden personenbezogene Daten frühestmöglich anonymisiert bzw. pseudonymisiert?
- Kann eine Inanspruchnahme der Leistung auch anonym bzw. unter einem Pseudonym erfolgen?
- Nach welcher Zeit erfolgt eine Sperrung der Daten?

4.4.3. Bewertung

0 Punkte: Maßnahmen zur Datenvermeidung und Datensparsamkeit werden nicht getroffen

- weder bei der Wahl der Software, noch bei der Gestaltung der Datenverarbeitungsverfahren ist Datenvermeidung bzw. Datensparsamkeit berücksichtigt worden
- Daten bleiben auf Dauer personenbezogen gespeichert, obwohl dies nicht erforderlich ist
- es werden mehr Daten erhoben als für die Erbringung des Dienstes erforderlich

1 Punkt: Datenvermeidung und Datensparsamkeit wurden zwar bei der Systemgestaltung berücksichtigt, sind jedoch verbesserungsbedürftig

- Daten werden auf Grund der Systemgestaltung personenbezogen gespeichert, obwohl datenschutzfreundliche Systemalternativen verfügbar sind
- die Daten werden zwar anonymisiert bzw. pseudonymisiert, jedoch nicht zu einem möglichst frühen Zeitpunkt

2 Punkte: Es werden angemessene Maßnahmen zur Datenvermeidung und –Sparsamkeit getroffen

- datenschutzfreundliche Systemalternativen wurden geprüft und soweit wirtschaftlich vertretbar realisiert
- die personenbezogenen Daten werden frühestmöglich pseudonymisiert;
- die unter Pseudonym gespeicherten Daten werden gegen eine Zuordnung zum Träger des Pseudonyms angemessen gesichert
- die personenbezogenen Daten werden frühestmöglich anonymisiert bzw. gelöscht

3 Punkte: Datenvermeidung und Datensparsamkeit werden vorbildlich realisiert

- es werden besondere Maßnahmen zur Datenvermeidung getroffen, die ggf. auch eine anonyme bzw. pseudonyme Erbringung der Dienstleistung ermöglichen
- sämtliche medizinische Befunddaten sind pseudonymisiert (z.B. durch Barcodes oder Laborlistennummern) und können nur von Nutzer mit den Identifikationsdaten zusammengeführt werden
- die Maßnahmen werden laufend dem Stand der Technik angepasst

5. Modul 3 - Datenschutzmanagement

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?

5.1. Bestellung eines betrieblichen / behördlichen Datenschutzbeauftragten

5.1.1. 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).

5.1.2. 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?

5.1.3. 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

5.2. Verzeichnis von Verfahrenstätigkeiten

5.2.1. 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.

5.2.2. 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?

5.2.3. 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

5.3. Datenschutzfolgeabschätzung

5.3.1. 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.

5.3.2. 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?

5.3.3. 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

5.4. Datenschutzpolitik & Sensibilisierung

5.4.1. Rechtliche Grundlagen

Unter dem Punkt „Datenschutzpolitik & Sensibilisierung" sind vorliegend die sonstigen gesetzlichen Anforderungen zusammengefasst, deren Einhaltung die „Datenschutzkultur" 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 Bedeutung sind in diesem Zusammenhang systematische Regelungen zum Umgang mit personenbezogenen Daten (Datenschutzpolitik bzw. Privacy Policy). Sie richten sich zum einen an 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).

5.4.2. Fragen

- 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?

5.4.3. 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

5.5. Auftragsverarbeitung

5.5.1. 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 nachgewiesene, gültige Zertifizierung gemäß ISO/IEC 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.

5.5.2. 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?

5.5.3. 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/IEC 27001)

5.6. Technische und organisatorische Maßnahmen

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.

Ggf. sind spezielle organisatorische Sicherheitsmaßnahmen nach § 19 TTDSG einschlägig.

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/IEC 27001, IT-Grundschutz eines Rechenzentrums, in denen die Webserver untergebracht sind), dann kann auf die nachweisbaren Ergebnisse auch verwiesen werden.

5.7. Privacy by design / default (Art. 25 DSGVO)

5.7.1. Rechtliche Grundlagen

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 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.

5.7.2. Fragen

- Welche Maßnahmen heben sich im Sinne des Datenschutzes besonders hervor?
- Wurden z.B. in anderen Modulen oder in anderen Fragen dieses Moduls Maßnahmen mit „3“ als besonders vorbildlich bewertet?

5.7.3. Bewertung

0 Punkte

- In anderen Modulen oder in anderen Fragen wurde mindestens 1 Aspekt mit „0“ bewertet

1 Punkt

- In anderen Modulen oder in anderen Fragen wurde mindestens 1 Aspekt mit „1“ bewertet

2 Punkte

- Technikgestaltung und / oder datenschutzfreundliche Voreinstellungen können hinsichtlich der Online-Dienste und Datenverarbeitungen bejaht und nachgewiesen werden

3 Punkte

- In anderen Modulen oder in anderen Fragen wurde mindestens 1 Aspekt mit „3“ bewertet

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

5.8.1. Rechtliche Grundlagen

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.

5.8.2. 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?

5.8.3. 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

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

5.9.1. Rechtliche Grundlagen

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.

5.9.2. 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?

5.9.3. 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

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

5.10.1. Rechtliche Grundlagen

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.

5.10.2. 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?

5.10.3. 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

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

5.11.1. Rechtliche Grundlagen

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

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.

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

5.11.2. 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?

5.11.3. 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

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

5.12.1. Rechtliche Grundlagen

Der Verantwortliche muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der getroffenen technischen und organisatorischen Maßnahmen ein-

richten. 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.

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 (i.d.R. nach OWASP Top 10) 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.

5.12.2. 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?

5.12.3. 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

5.13. Spezialfall: TOM im E-Health Bereich

Merker: 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 des Modules Datenschutzmanagement). Sie sollen daher zusammenfassend aufgeführt und bewertet werden.

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.

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.

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

0 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

5.14. 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.

5.14.1. 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.

Ggf. sind Ausprägungen des BDSG und der Landesdatenschutzgesetze sowie weiterer Spezialgesetze zu beachten.

5.14.2. 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?

5.14.3. 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

5.15. 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.

5.15.1. 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?

5.15.2. 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.

5.16. Weitere spezielle Betroffenenrechte

5.16.1. Rechtliche Grundlagen

Ggf. sind Betroffenenrechte der §§ 22ff. TTDSG einschlägig.

Soweit es sich bei den veröffentlichten Beiträgen um eigenständige geistige Schöpfungen wie Rezensionen oder ähnliche Beiträge handelt, gilt für diese grundsätzlich der Schutz des UrhG. Abzugrenzen hiervon sind bloße Kommunikationsbeiträge wie sie in Chats, Messageboards und sonstigen Foren öffentlicher Kommunikation erscheinen. Unterscheidungsmerkmal, ob ein veröffentlichter Beitrag ein Werk i.S.d. §§ 1 und 2 UrhG darstellt, ist die geistige Schöpfungstiefe. Das Urhebergesetz schützt den Urheber in seinen geistigen und persönlichen Beziehungen zum Werk (Urheberpersönlichkeitsrecht) und in der Nutzung des Werkes (Verwertungsrechte) in körperlicher und unkörperlicher Form. Das Urheberrecht selbst ist zu Lebzeiten des Urhebers nicht übertragbar. Der Urheber kann lediglich anderen Personen das Recht einräumen, sein Werk auf einzelne oder alle Nutzungsarten zu nutzen (Nutzungsrechte). Die Nutzungsrechte können räumlich, zeitlich oder inhaltlich beschränkt eingeräumt werden und ausschließlich (exklusiv) oder nicht ausschließlich (einfaches Nutzungsrecht) begründet werden. Die wichtigsten Rechte, die ein Urheber einem Nutzer übertragen kann, sind das Vervielfältigungsrecht (§ 16 UrhG), das Verbreitungsrecht (§ 17 UrhG), das Vorführungsrecht (§ 19 Abs. 4 UrhG) und das Senderecht (§ 20 UrhG). Diese Rechte betreffen die Herausgabe eines Werkes unmittelbar und beziehen sich auf im Wesentlichen körperliche, also materielle, Verbreitungs- und Kopierverfahren. Bei Telemedien, die dem Nutzer die Publikation von Werken i.S.d. UrhG (eben die o.g. Rezensionen u.ä.) kostenlos anbieten, hat sich unter Anbietern mittlerweile etabliert, sich sämtliche Verwertungsrechte abtreten zu lassen:

Bsp: Sie gewähren xyz eine zeitlich und örtlich unbeschränkte und ausschließliche Lizenz zur weiteren Verwendung Ihrer Rezension für jegliche Zwecke online wie offline. Wir bemühen uns, Sie stets als Autor zu benennen.

Diese für den durchschnittlichen Nutzer meist kaum wahrgenommene Abtretung seiner Rechte ist i.d.R. an die Nutzung der Publikationsmöglichkeit gekoppelt, d.h. eine Nutzung ist ohne Abtretung der Rechte in vielen Fällen gar nicht möglich. Wenngleich diese Koppelung nicht primär ein speziell datenschutzrechtliches Kriterium ist, fallen doch mit der Übertragung dieser Rechte zusätzliche Daten an, auf deren Erhebung der Nutzer entweder Einfluss (3 Punkte) oder keinen Einfluss (0 Punkte) hat.

5.16.2. Fragen

Wird der Nutzer überhaupt auf seine urheberrechtlichen Rechte hingewiesen?

Muss der Nutzer seine urheberrechtlichen Nutzungsrechte übertragen, um den Dienst bzw. das Telemedium in Anspruch nehmen zu können?

Erfolgt die Übertragung dieser Rechte durch bewusste Handlung des Nutzers oder „versteckt" im Rahmen von Nutzungsbedingungen?

Wird die Übertragung dieser Rechte protokolliert?

Hat der Nutzer nach der Publikation noch irgendwelchen Einfluss auf seinen Beitrag (Dauer der Publikation, Möglichkeit, diese zu löschen), wird er auf sein Rückrufsrecht, § 42 UrhG, hingewiesen?

Hat der Nutzer Einfluss auf Art und Umfang der zur Veröffentlichung gespeicherten personenbezogenen Daten? Kann er bestimmen, ob die Daten nur unter Pseudonym gespeichert werden?

5.16.3. Bewertung

0 Punkte:

- der Nutzer hat auf die Art der Datenerhebung und die Übertragung seiner Verwertungsrechte keinen Einfluss
- Beiträge werden nur dann publiziert, wenn der Nutzer einzelne oder sämtliche Verwertungsrechte auf den Anbieter überträgt (Übertragung einer kostenlosen „Generallizenz")

1 Punkt:

- der Nutzer hat geringen Einfluss auf die Art der Datenerhebung
- die Veröffentlichung der Beiträge ist an die Übertragung der Verwertungsrechte gekoppelt, der Nutzer kann aber bestimmen, dass seine Daten hierzu nur unter Pseudonym gespeichert werden

2 Punkte:

- der Nutzer kann über die Übertragung seiner Rechte selbst bestimmen

- der Nutzer kann mit bewusster Einwilligung wählen, ob er die Verwertungsrechte überträgt

3 Punkte:

- der Nutzer muss keine Rechte übertragen, personenbezogene Daten werden nicht erhoben
- der Beitrag wird ohne Bedingungen publiziert
- der Nutzer hat auch nach der Veröffentlichung noch Einfluss auf die Dauer: per E-Mail kann der Beitrag entfernt werden.