ips Modul M2 - Individual-Dienstleistung, Version 3.5

datenschutz cert GmbH
29. Juli 2020

datenschutz cert

Inhaltsverzeichnis

1. Allgemeines

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 E-Health-Dienste, Online-Videosprechstunden, 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 herangezogen werden müssen. Auch sind Vorgaben der E-Privacy-Verordnung zu berücksichtigen. Schließlich müssen für ergänzende Dienstleistungen (z.B. für die von einigen E-Shops angebotene Möglichkeit des Kunden, sich über den Stand der Auslieferung eines bestellten Produkts zu informieren) ebenfalls die Bestimmungen des TMG berücksichtigt werden. Zudem können spezialgesetzliche Anforderungen für die jeweilige Dienstleistung vorrangig zu betrachten sein.

2. Materielle Rechtmäßigkeit

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 materiellrechtliche Voraussetzungen eingehalten werden.

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

2.1. Allgemeine Rechtmäßigkeit der Datenverarbeitung

2.1.1. Datenschutzrechtliche Grundlagen im Allgemeinen

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, Videosprechstunde, 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. Beispielsweise 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.

Ein anderes Beispiel stellt das Onlineangebot von Lebensmitteln dar. Hier hat das Bundesamt für Verbraucherschutz und Lebensmittelsicherheit verschiedene Voraussetzungen zusammengefasst, die für den Handel mit Lebensmitteln im Internet zu beachten sind. Dazu zählt insbesondere die Registrierung des Lebensmittelunternehmens.

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).

2.1.2. Fragen

- Welche personenbezogenen Daten werden verarbeitet? Sind diese Daten zur Gestaltung bzw. Erbringung des Dienstes erforderlich?
- Welche Nutzungsdaten werden verarbeitet? Sind diese Daten für die Erbringung des Dienstes erforderlich? Wann werden die Nutzungsdaten gelöscht?
- Werden Cookies gesetzt? Werden die Cookie-Daten zusätzlich zentral gespeichert? Für welche Zwecke und für welchen Zeitraum bleiben die Daten gespeichert?
- Werden in Cookies gespeicherte Daten ausgelesen? Welche Daten werden dabei für welche Zwecke erhoben?

2.1.3. 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

2.2. Optionale Anforderungen für die Prüfung von E-Commerce-Dienstleistungen (Online-Shops)

2.2.1. Rechtliche Grundlagen

Die Zulässigkeit der Verarbeitung mittels des Webportals von personenbezogenen Daten im Rahmen des elektronischen Kaufs richtet sich nach den Anforderungen der DSGVO; online-spezifisch sind weiterhin die Vorschriften des TMG bzw. der E-Privacy Verordnung einschlägig. Demnach dürfen beim Vertragsabschluss (elektronische Bestellung) die folgenden Daten verarbeitet werden:

- Daten, die den Kunden identifizieren (Name, Anschrift, elektronische Signatur), ggf. Kundennummer, soweit bereits eine Geschäftsbeziehung besteht,
- Daten über die bestellte Ware oder Dienstleistung (Bezeichnung, Artikelnummer, Konfektionsgröße usw.)
- Daten zur Lieferung (Lieferanschrift, gewünschtes Lieferdatum, bevorzugte Lieferungsform, gewünschte Verpackung),
- Daten zur Zahlungsabwicklung (abhängig vom Bezahlverfahren).
- Daten, die zum Verbindungsaufbau erforderlich sind (IP-Adressen und weitere durch die jeweiligen Protokolle definierte Angaben)

2.2.2. Fragen

- Welche Daten werden im Vorfeld des Vertragsabschlusses erhoben? Für welchen Zweck werden sie erhoben und sind sie für diesen Zweck erforderlich?
- Welche Daten werden beim Vertragsabschluss erhoben? Sind die Daten für den Vertragsabschluss erforderlich?
- Welche personenbezogenen Daten werden zusätzlich erhoben und gespeichert? Für welchen Zweck erfolgt die Erhebung?
- Werden die Zwecke bei der Erhebung festgelegt?

- Findet eine Koppelung der Erbringung des Dienstes an die Angabe nicht erforderlicher Daten statt?
- Welche Daten werden beim Vertragsabschluss bzw. im Rahmen des Vertragsverhältnisses gespeichert? Sind die Daten für den Abschluss und die Abwicklung des Vertrags erforderlich?
- Welche personenbezogenen Daten werden zusätzlich gespeichert?
- Für welchen Zeitraum bleiben die Daten gespeichert?
- Werden Bestands- und Nutzungsdaten für andere Zwecke als zur Erbringung des Dienstes genutzt? Für welche Zwecke?
- Werden Nutzungsprofile erstellt? Welche Daten gehen in die Nutzungsprofile ein? Wie werden die Daten individuell zugeordnet? Für welche Zwecke werden die Nutzungsprofile erstellt? Wie werden die ggf. verwendeten Pseudonyme gebildet?
- Werden Kundenprofile erstellt? Welche Daten gehen in die Kundenprofile ein? Wie werden die Daten individuell zugeordnet? Werden die Kundenprofile mit den Nutzungsprofilen zusammengeführt?
- Werden Daten für Werbezwecke genutzt? Um welche Daten handelt es sich dabei?
- Werden die zum Abschluss bzw. zur Abwicklung des Vertragsverhältnisses auch für andere Zwecke genutzt? Um welche Zwecke handelt es sich?
- Sofern Lebensmittel zum Online-Kauf angeboten werden: Hat der Anbieter eine entsprechende Registrierung nach den Lebensmittelvorschriften nachgewiesen?

2.2.3. Bewertung

0 Punkte: Die Datenverarbeitung überschreitet den gesetzlichen Rahmen erheblich

- beim Kaufvertrag werden zwangsweise Daten erhoben, die für die Abwicklung des Kaufs nicht erforderlich sind (z.B. Angaben zum Beruf, Geburtsdatum, Geschlecht),
- 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
- sofern Lebensmittel zum Online-Kauf angeboten werden: Der Anbieter hat keine entsprechende Registrierung nach den Lebensmittelvorschriften nachgewiesen

1 Punkt: Die Erhebung überschreitet den gesetzlichen Rahmen geringfügig

- eine Prüfung entgegenstehender berechtigter Interessen des Betroffenen ist nicht vollständig
- es werden geringfügig mehr Daten erhoben, als für die Vertragsabwicklung 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

Im Rahmen der Übermittlung personenbezogener Daten in E-Shops sind im Wesentlichen zwei Varianten zu betrachten, zum einen die Übermittlung zur Vertragsabwicklung (etwa an Lieferanten der bestellten Ware oder an das Kreditkartenunternehmen), daneben die Übermittlung zu Werbezwecken. Sie sind nur zulässig, wenn die Voraussetzungen des Art. 6 DSGVO erfüllt sind.

2.2.4. Fragen zur Übermittlung:

- Werden Bestandsdaten übermittelt? An wen und für welchen Zweck?
- Werden Nutzungsdaten übermittelt? An wen und für welchen Zweck?
- Werden Daten des Kunden zur Abwicklung des Vertragsverhältnisses übermittelt? An wen und für welchen Zweck?
- Werden Daten des Kunden zur Bonitätsprüfung übermittelt? Welche Daten werden dabei an wen übermittelt?
- Werden Daten für Werbezwecke übermittelt? Um welche Daten handelt es sich dabei und wer ist der Empfänger?
- Welche sonstigen personenbezogenen Daten werden übermittelt? An wen und für welchen Zweck?
- Für welchen Zeitraum bleiben die Daten gespeichert?

2.2.5. Bewertung

0 Punkte: Es werden Daten trotz gesetzlichen Verbots übermittelt

1 Punkt: Die Übermittlung überschreitet den gesetzlichen Rahmen geringfügig

- eine Prüfung entgegenstehender berechtigter Interessen des Betroffenen unterbleibt; hiervon ist stets dann auszugehen, wenn der Betroffene nicht über die Übermittlung unterrichtet wurde

2 Punkte: Die Übermittlung erfolgt in dem gesetzlich zulässigen Rahmen

- Widerspruchsrechte und Einwilligungsvorbehalte werden beachtet
- entgegenstehende überwiegende schutzwürdige Interessen des Betroffenen werden geprüft und berücksichtigt
- die Übermittlung beschränkt sich auf die bei Erhebung festgelegten Zwecke

3 Punkte: Die Übermittlungspraxis ist vorbildlich

- es werden besondere Vorkehrungen getroffen, um den Umfang der Übermittlung zu minimieren

- alle mit Zweckänderungen verbundenen Übermittlungen, insbesondere für Werbezwecke erfolgen stets auf Basis der Einwilligung

2.3. Optionale Anforderungen für die Prüfung von 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.

2.3.1. Rechtliche Grundlagen im E-Health-Bereich am Beispiel des Verkaufs von Arzneimitteln und der Verarbeitung zu Forschungszwecken

Durch die Art. 20ff. 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 Ausnahmetatbeständen - 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.

2.3.2. 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?

2.3.3. 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)

2.4. Optional: Sonstige materiellrechtliche Voraussetzungen

2.4.1. Rechtliche Grundlagen

Aufgrund der Vielfältigkeit möglicher Online-Dienstleistungen bestehen grundsätzlich auch je nach konkretem Angebot weitere unterschiedlichste rechtliche Anforderungen im Hinblick auf eine zulässige Datenverarbeitung. Soweit das Angebot z.B. die Verarbeitung von Sozialdaten ermöglicht, müssen die §§ 67 ff. SGB X beachtet werden, Angaben, die der ärztlichen Schweigepflicht unterliegen, dürfen nicht – bzw. nur unter engen Voraussetzungen – durch Dritte im Rahmen der Auftragsverarbeitung verarbeitet werden, besonders sensible Daten bedürfen der Datenschutzfolgeabschätzung, spezielle technische Verfahren bedürfen weiterer rechtlicher Überprüfung usw. Sämtliche Möglichkeiten, mit denen über das Internet im Rahmen von Online-Dienstleistungen personenbezogene Daten ausgetauscht werden, deren zulässige Verarbeitung sich nach weiteren rechtlichen Vorgaben innerhalb und außerhalb der DSGVO richtet, können an dieser Stelle nicht aufgezählt werden. Die nachfolgenden Fragen sollen daher nur darauf hinweisen, dass der Gutachter ggfls. weitere Rechtsvorschriften heranziehen und prüfen muss. Ist eine Online-Dienstleistung bereits vom Anwendungsfall anderer ips-Module zu spezifischen Online-Angeboten (z.B. E-Commerce) erfasst, ist es mit guter Begründung auch vertretbar, auf die Ergebnisse des dortigen ips-Modules zu verweisen.

2.4.2. Fragen

- Handelt es sich bei dem geprüften Web-Angebot um eine Individual-Dienstleistung?
- Muss der Nutzer zur Inanspruchnahme der Individual-Dienstleistung personenbezogene Daten angeben, die über vertragstypische Bestandsdaten hinausgehen?
- Müssen innerhalb des Web-Angebotes Angaben über die rassische oder ethnische Herkunft, politische Meinungen (personenbezogen!), religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben gemacht werden?
- Hat die erforderliche Datenschutzfolgeabschätzung stattgefunden?
- Wird die Individual-Dienstleistung durch besondere Berufsgruppen erbracht, die Zeugnisverweigerungsrechte haben (Ärzte, Betreuer, Rechtsanwälte, Steuerberater etc.)?
- Werden Daten, die besonderen Vertraulichkeitsvorschriften unterliegen, im Rahmen von Auftragsverarbeitung durch Dritte verarbeitet?
- Werden in diesem Zusammenhang erforderliche Verschlüsselungen beachtet? (Bsp.: Daten, die der ärztlichen Schweigepflicht unterliegen, dürfen i.d.R. nicht im Wege der Auftragsverarbeitung verarbeitet werden bzw. nur, wenn diese verschlüsselt werden und für Dritte nicht einsehbar sind.)
- Sind beim Einsatz Dritter (Auftragsverarbeitung) besondere Zulässigkeitsvorschriften der Landesdatenschutzgesetze zu beachten?
- Werden besondere technische Verfahren zur Datenverarbeitung eingesetzt?

- Wird die Beachtung zusätzlicher spezieller materiellrechtlicher Anforderungen beim Einsatz solcher besonderen technischen Verfahren sichergestellt (Bsp: automatisierte Abrufverfahren?

2.4.3. Bewertung

0 Punkte: die rechtlich einschlägigen Vorgaben zum Datenschutz und zur IT-Sicherheit werden nicht beachtet

1 Punkt: die anwendbaren Rechtsvorschriften werden geringfügig unterschritten

2 Punkte: die anwendbaren Rechtsvorschriften werden eingehalten

3 Punkte: Datenschutz oder Datensicherheit werden in besonderem Maße eingehalten und gehen über die gesetzlichen Anforderungen hinaus

3. Online-Einwilligungen

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 oder Videosprechstunden) unterliegen sie zumeist sehr eng gefassten und einzelfallbezogenen Erlaubnistatbeständen. In der Regel kommt daher der Einwilligung des Betroffenen eine besondere Bedeutung zu. Weitere Einwilligungser-

fordernisse können spezialgesetzlich geregelt sein, z.B. in Landesgesetzen (z.B. Landeskrankenhausgesetze, Verordnungen etc. für **Videosprechstunden und 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.

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?

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. Datenvermeidbarkeit und Datensparsamkeit

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-Commerce Dienstleistungen: etwa wie beim DASIT-Modell in Bezug auf das Vertragsabschlussverhalten, bei dem durch eine Funktionstrennung von Shop, Zahlungsprovider und Lieferanten den jeweiligen Stellen nur wenige Informationen zur Verfügung stehen.

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.

4.2. 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?

4.3. Bewertung

o 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