

Classification of different categories of health data based on risk assessment and legitimation basis for data processing (Supplement to Deliverable ““Legal map” of the applicable legal framework conditions for research data processing”)

Vanessa Lettieri, Dennis-Kenji Kipker, Benedikt Buchner

Angaben zur Veröffentlichung / Publication details:

Lettieri, Vanessa, Dennis-Kenji Kipker, and Benedikt Buchner. 2023.
“Classification of different categories of health data based on risk assessment and legitimation basis for data processing (Supplement to Deliverable ““Legal map’ of the applicable legal framework conditions for research data processing”).”
Online-Ressource. Köln: NFDI4Health.
<https://doi.org/10.4126/FRL01-006449529>.

Nutzungsbedingungen / Terms of use:

CC BY 4.0

Dieses Dokument wird unter folgenden Bedingungen zur Verfügung gestellt: / This document is made available under these conditions:

CC-BY 4.0: Creative Commons: Namensnennung

Weitere Informationen finden Sie unter: / For more information see:

<https://creativecommons.org/licenses/by/4.0/deed.de>



Classification of different categories of health data based on risk assessment and legitimation basis for data processing (Supplement to Deliverable ””Legal map” of the applicable legal framework conditions for research data processing”)

Authors:

Lettieri, Vanessa¹; Kipker, Dennis-Kenji¹; Buchner, Benedikt¹
on behalf of the NFDI4Health Consortium

Acknowledgement:

Ahrens, Wolfgang²; Drepper, Johannes³; Fluck, Juliane⁵; Fröhlich, Holger⁴; Gehrke, Juliane³; Goek Ng, Hwei⁴; Haber, Anna C.⁶; Henke, Christian⁷; Holick, Marcel³; Intemann, Timm²; Kaulke, Knut³; Kirsten, Toralf; Kuntz, Alessandra S.⁷; Prasser, Fabian⁶; Sax, Ulrich⁷; Semler, Sebastian³;

¹ University of Bremen / University of Augsburg (since 01/08/2022)

² Leibniz Institute for Prevention Research and Epidemiology – BIPS

³ Technology, Methods, and Infrastructure for Networked Medical Research – TMF

⁴ Fraunhofer Institute for Algorithms & Scientific Computing – SCAI

⁵ Information Centre for Life Sciences – ZB MED

⁶ Berlin Institute of Health at Charité – Universitätsmedizin Berlin

⁷ Georg-August University Göttingen, University Medical Center (Institute for Medical Informatics)

DOI: 10.4126/FRL01-006449529

Version: V1_0

Publication date: 20.06.2023

Lizenz

Dieses Werk wurde unter der Lizenz „Creative Commons Namensnennung 4.0 International“ (CC BY 4.0) veröffentlicht. Den rechtsverbindlichen Lizenzvertrag finden Sie unter <https://creativecommons.org/licenses/by/4.0/legalcode>



This work was done as part of the NFDI4Health Consortium (www.nfdi4health.de). We gratefully acknowledge the financial support of the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – project number 442326535.

D6.6 - Klassifizierung verschiedener Kategorien von Gesundheitsdaten anhand von Risikobewertung und Legitimationsgrundlage für die Datenverarbeitung / Classification of different categories of health data based on risk assessment and legitimation basis for data processing

1. Zielsetzung und Hintergrund

Das europäische und das nationale Datenschutzrecht halten umfassende rechtliche Rahmenbedingungen für die wissenschaftliche Forschung bereit. Mit dem vorliegenden Deliverable D6.6 wird eine grafische und interaktive Guideline für Forschende zur Verfügung gestellt, um bei der Klassifikation von personenbezogenen Daten zu unterstützen und eine Leitlinie für die Verarbeitung auch von sensiblen personenbezogenen Daten im Forschungskontext an die Hand zu geben. Im Hinblick auf den Forschungsdatenschutz im Gesundheitssektor ergeben sich für den Forschenden verschiedene Probleme, die neben der Auslegung von Rechtsbegriffen wie dem „personenbezogenen Datum“ auch auf das komplexe rechtliche Gefüge zwischen europäischem Recht, Bundesrecht und Landesdatenschutzrecht zurückzuführen sind. Überdies ist zwischen zahlreichen allgemeinen und bereichsspezifischen Regularien zu unterscheiden. Um einen verständlichen Einstieg in diese komplexe Rechtsmaterie insbesondere für Fachfremde zu ermöglichen, bereitet Deliverable D6.6 diese unterschiedlichen juristischen Rahmenbedingungen in der Form einer schematischen Übersicht auf, die die datenschutzrechtlich wesentlichen Schritte bzw. Aufgaben einer Datenverarbeitung aufzeigt. Das interaktive Dokument soll auf diese Weise dazu beitragen, es Forschenden zu ermöglichen, den datenschutzbezogenen Rechtsrahmen ihrer Arbeit in Form einer **Checkliste mit Auswahlmöglichkeiten** zu ermitteln und zu beachten.

Inhaltlich ist das Dokument in Ergänzung zu Deliverable D6.2 („Legal map“ of the applicable legal framework conditions for research data processing) zu sehen und gibt dessen Ausführungen deshalb nur ausschnittsweise und bedarfsgerecht wieder. Vorgenanntes Dokument bereitet den datenschutzbezogenen Rechtsrahmen der Forschung umfassend auf, indem der Anwendungsbereich erläutert wird, die Verarbeitungsgrundsätze vorgestellt werden, eine Übersicht über die rechtlichen Rahmenbedingungen der Datenverarbeitung zu Forschungszwecken gegeben wird und abschließend der Forschungsdatenschutz im grenzüberschreitenden

Datenverkehr betrachtet wird. Soweit folglich Einzelfallfragen zu adressieren sind, wird insoweit auf D6.2 verwiesen. **Auch kann und will die in D6.6 gegebene Übersicht nicht die Beratung durch einen Datenschutzbeauftragten ersetzen, sondern dient nur als erster Anlaufpunkt, um eine Übersicht über die datenschutzrechtlich relevanten Forschungsprozesse zu erlangen.**

2. Guideline: Was muss ich bei der Verarbeitung personenbezogener Daten zu Forschungszwecken beachten?

Gliederung der Guideline:

- I. Findet eine Datenverarbeitung im Sinne der DS-GVO statt?
- II. Werden hierbei personenbezogene Daten verarbeitet?
- III. Werden die Daten pseudonymisiert oder anonymisiert verarbeitet?
- IV. Klassifizierung der Datenkategorien: Handelt es sich bei den verarbeiteten personenbezogenen Daten um einfache Daten oder besondere Kategorien personenbezogener Daten?
- V. Werden die Verarbeitungsgrundsätze für den Umgang mit personenbezogenen Daten nach der DS-GVO beachtet?
- VI. Welche Personen/Einrichtungen sind an der Datenverarbeitung beteiligt?
- VII. Erfolgt im Rahmen der Einbeziehung Dritter eine Datenübermittlung in Länder außerhalb der EU/des EWR ohne Angemessenheitsbeschluss?
- VIII. Welche Rechtsgrundlagen sind zur Legitimation der Verarbeitung der personenbezogenen Daten im Forschungskontext heranzuziehen?
- IX. Werden betroffene Personen gem. Art. 13 und 14 DS-GVO transparent über die Datenverarbeitung informiert?
- X. Werden die datenschutzrechtlichen Betroffenenrechte berücksichtigt und eingehalten?
- XI. Werden die technischen und organisatorischen Maßnahmen zur Datensicherheit angemessen umgesetzt?
- XII. Muss eine Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO durchgeführt werden?
- XIII. Ist im Rahmen der Datenverarbeitung eine Datenpanne erfolgt?
- XIV. Gibt es ein Konzept zur Speicherung und Aufbewahrung bzw. Löschung von Daten nach Ablauf ihrer Lebensdauer?

I. Findet eine Datenverarbeitung im Sinne der DS-GVO statt?

➤ Definition:

Der sachliche Anwendungsbereich der DS-GVO ist gem. Art. 2 eröffnet, wenn eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten erfolgt.

Eine Verarbeitung im Sinne der DS-GVO umfasst jede Handlung im Zusammenhang mit personenbezogenen Daten, namentlich verändern, speichern, übermitteln, erheben, löschen, verknüpfen. Der Begriff der Datenverarbeitung ist somit weit gefasst und es kommt nicht auf den Umfang oder die Dauer einer Datenverarbeitung an.

[Erläuterung in D6.2 Gliederungspunkt B.I.]

Ja

Nein

II. Werden hierbei personenbezogene Daten verarbeitet?

➤ Definition:

Personenbezogene Daten sind gem. Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, die sog. „betroffene Person“, beziehen. Zu unterscheiden ist somit zwischen der Datenverarbeitung basierend auf personenidentifizierenden Merkmalen und der Datenverarbeitung, die keine personenidentifizierenden Merkmale verwendet. Identifizierbar ist eine Person gem. Art. 4 Nr. 1 DS-GVO dann, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung (Namen, Kennnummer etc.) oder sonstigen besonderen Merkmalen, wozu auch physische, physiologische, genetische, psychische und soziale Merkmale gehören können, identifiziert werden kann. Insbesondere dann, wenn miteinander kombinierte Informationen den Rückschluss auf eine Einzelperson zulassen, kann von personenbezogenen Daten gesprochen werden.

[Erläuterung in D6.2 Gliederungspunkt B.II.]

Ja

Nein

III. Werden die Daten pseudonymisiert oder anonymisiert verarbeitet?



Die Prüfung, ob eine hinreichende Pseudonymisierung oder Anonymisierung vorliegt, sollte durch einen Datenschutzbeauftragten und ggf. unter Einbeziehung der Aufsichtsbehörden erfolgen.

➤ Definition:

Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken unterliegt gem. Art. 89 Abs. 1 S. 1 DS-GVO „geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person“. Der Grundsatz der Datenminimierung sowie die Wahrung der Rechte und Freiheiten betroffener Personen sollen durch technische und organisatorische Maßnahmen sichergestellt werden. Im Hinblick auf diese Maßnahmen nennt Art. 89 Abs. 1 S. 3 DS-GVO die Pseudonymisierung. Die Anonymisierung wird in dieser Vorschrift nicht explizit genannt, der Erwägungsgrund 26 der Verordnung legt dahingehend aber fest, dass die DS-GVO nicht für „anonyme Informationen“ gilt.

1. Pseudonymisierung

➤ Definition:

Die Pseudonymisierung von personenbezogenen Daten ist in Art. 4 Nr. 5 DS-GVO legaldefiniert als die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Dazu müssen die zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten einer identifizierten oder identifizierbaren natürlichen Person nicht zugewiesen werden. **Zu beachten ist, dass es sich bei pseudonymisierten Daten weiterhin um personenbezogene Daten handelt**, sodass der Anwendungsbereich des Datenschutzes nach wie vor vollständig eröffnet ist. Jedoch stellt die Pseudonymisierung eine technisch-organisatorische Maßnahme (TOM) dar, um Datensparsamkeit und Datensicherheit gem. Art. 32 DS-GVO zu realisieren.

[Erläuterung in D6.2 Gliederungspunkt B.III.1.]

Ja

Nein

2. Anonymisierung

➤ Definition:

Gem. Art. 2 Abs. 1 DS-GVO ist der Anwendungsbereich des Datenschutzrechts nur dann eröffnet, soweit eine Verarbeitung personenbezogener Daten erfolgt. Bei personenbezogenen Daten handelt es sich nach der Legaldefinition in Art. 4 Nr. 1 DS-GVO um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Allgemein versteht man unter Anonymisierung das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können. **Der Anonymisierungsvorgang als solcher ist dabei jedoch als eine Datenverarbeitung anzusehen und unterfällt deshalb dem Anwendungsbereich der DS-GVO, sodass er einer Rechtfertigung bedarf.**

[Erläuterung in D6.2 Gliederungspunkt B.III.1.]

Ja

Nein



Hinweis zur Anonymität von Datensätzen: Insbesondere dann, wenn **miteinander kombinierte Informationen** den Rückschluss auf eine Einzelperson zulassen, kann von einer „erhöhten Gefahr“ für die **Re-Identifizierung** einer betroffenen Person gesprochen werden. Dabei ist ein besonderes Augenmerk darauf gerichtet, das Erstellen umfassender Persönlichkeitsprofile durch systematische Zusammenführung von Daten nicht zu ermöglichen.

In Anbetracht der sich laufend weiterentwickelnden technischen Möglichkeiten dürfte aber mittlerweile davon auszugehen sein, dass es keine absolute und unumstößliche Anonymität von Daten mehr geben kann. Diese Erkenntnis entspricht dem Ansatz des relativen Personenbezugs, dass vielmehr eine Risikoprognose vorzunehmen ist. Wird im Rahmen der Risikoprognose ermittelt, dass der Aufwand zur Re-Identifizierung dermaßen unverhältnismäßig ist, dass eine solche nach allgemeiner Lebenserfahrung und dem Stand von Wissenschaft und Technik nicht zu erwarten ist, ist ein Personenbezug nach dem relativen Ansatz abzulehnen. In die Risikoprognose einzubeziehen sind auch „das vorhandene oder erwerbbar Zusatzwissen des Verantwortlichen, aktuelle und künftige technische Möglichkeiten der Verarbeitung sowie der mögliche Aufwand und die verfügbare Zeit“. Zu beachten

ist jedoch zusätzlich, dass selbst wenn eine Anonymität der verarbeiteten Daten angenommen wird, dennoch datenschutzrechtliche Pflichten fortbestehen, da der Datenschutz auch vor einer möglichen **De-Anonymisierung** von Datenbeständen schützt. Daher müssen solche notwendigen Maßnahmen ergriffen werden, die dieses Risiko weitestgehend möglich reduzieren oder bestenfalls verhindern. Dies kann insbesondere durch technisch-organisatorische Maßnahmen und Prozesse des datenschutzrechtlichen Risikomanagements erfolgen.

Mit Blick auf das **Re-Identifizierungsrisiko von Forschungsdaten** gilt bei der Verarbeitung von Gesundheitsdaten eine Besonderheit: So ist zu beachten, dass je seltener ein Krankheitsbild und je kleiner eine Probandengruppe ist, umso weniger von anonymen Datensätzen ausgegangen werden kann, da sich gerade bei kleinen Personengruppen mit seltenen Erkrankungen das Re-Identifizierungsrisiko signifikant erhöhen dürfte.

Eine präzise Grenzziehung ist im Vorfeld einer konkreten rechtlichen Bewertung grundsätzlich schwierig, denn es muss auf den Verwendungszusammenhang der Daten im Einzelfall abgestellt werden. **Bevor sich eine Forschungseinrichtung deshalb auf die Anonymität eines Datensatzes beruft, ist dieser zuvor genauestens zu überprüfen und unter den rechtlichen Erwägungen im Einzelfall (Verwendung durch Personen/Stellen zu bestimmten Zwecken) zu bewerten.**

IV. **Klassifizierung der Datenkategorien: Handelt es sich bei den verarbeiteten personenbezogenen Daten um einfache Daten oder besondere Kategorien personenbezogener Daten?**



Besondere Kategorien personenbezogener Daten gem. Art. 9 DS-GVO sind in einem besonderen Maße schützenswert. Hier ist bei der Verarbeitung Vorsicht geboten und es gelten strengere gesetzliche Anforderungen, beispielsweise mit Blick auf die Erteilung einer datenschutzrechtlichen Einwilligung oder technisch-organisatorische Maßnahmen (TOM) zur Absicherung der Daten beispielsweise vor einem unbefugten Zugriff durch Dritte.

[Siehe zu den TOM im Einzelnen Prüfungspunkt IX dieser Handlungshilfe.]

Klassifikation – einfache personenbezogene Daten (Beispiele):

- Stammdaten (z.B. Namen, Anschriften, Kontaktangaben, Geburtsdatum)
- Zeiterfassungsdaten
- Zahlungsdaten
- Telekommunikationsdaten
- _____

Klassifikation – besondere Kategorien personenbezogener Daten (Beispiele):

➤ Definition:

Besondere Kategorien personenbezogener Daten haben einen höchstpersönlichen Charakter und können für betroffene Personen in vielen Fällen identitätsstiftend sein. Hierunter fallen Datenkategorien, die Ausdruck einer körperlichen, gesundheitlichen, seelischen, sozialen, familiären oder ökonomischen Notlage sein können. Dementsprechend besteht an

ihnen ein besonderes Vertraulichkeitsinteresse. Die unbefugte Offenlegung entsprechender Daten kann für die betroffene Person ein erhebliches Schadenspotenzial zur Folge haben.

Besondere Kategorien personenbezogener Daten können durchaus gleichzeitig mehreren Kategorien angehören. So handelt es sich z.B. bei genetischen Daten regelmäßig auch um Gesundheitsdaten.

Daten, aus denen die rassische und ethnische Herkunft hervorgeht

➤ Definition:

Informationen über die rassische Herkunft schließen Angaben über die Hautfarbe sowie sonstige markante äußere Merkmale mit ein, die auf die „biologische Abstammung“ abstellen. Teilweise kann im Ausnahmefall schon aus dem Namen einer Person, dem Geburts- oder Wohnort eine rassische oder ethnische Herkunft abgeleitet werden. Die Nationalität bzw. Staatsangehörigkeit wird hiervon nicht umfasst. Das Merkmal der ethnischen Herkunft stellt auf den kulturellen Aspekt, der eine Menschengruppe kennzeichnet, wie z.B. Sprache, Geschichte, Tradition, gemeinsame Werte und ein Zusammengehörigkeitsgefühl, ab. Hierunter fällt spezifisch nicht die Zugehörigkeit zu einer sozialen Schicht.

Daten, aus denen die politische Meinung hervorgeht

➤ Definition:

Politische Meinungen, religiöse und weltanschauliche Überzeugungen beziehen sich nicht nur auf die Unterstützung bestimmter Ansichten und Ideen, sondern erstrecken sich auch auf deren Ablehnung sowie Tätigkeiten. Dazu gehören z.B. die Zugehörigkeit zu einer politischen Partei oder einer weltanschaulichen Organisation, das Abonnement einer spezifisch ausgerichteten Zeitschrift, die Teilnahme an Offline- und Online-Petitionen, das Engagement bei einer Versammlung oder Demonstration, der Besuch einer entsprechenden Veranstaltung oder die Mitarbeit in politischen und ähnlichen Stiftungen oder Unterorganisationen.

Daten, aus denen die religiöse oder weltanschauliche Überzeugung hervorgeht

➤ Definition:

Unter religiösen oder anderen weltlichen und politischen Überzeugungen fallen z.B. Pazifismus, Sozialismus sowie Angaben über Anhänger von Naturreligionen und Sekten, Atheisten und Anthroposophen, genauso wie Angaben über Christen, Muslime, Buddhisten oder Mitgliedern weltanschaulicher Organisationen. Diese Anschauung kann auch durch Kleidung zum Ausdruck kommen. Dabei zielen die Überzeugungen eher auf Grundsätzliches ab, anders als hinsichtlich der politischen Meinungen, die sich auf aktuelle konkrete Fragestellungen, Ereignisse oder handelnde Personen beziehen können.

Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht

➤ Definition:

Unter der Gewerkschaftszugehörigkeit versteht man den Schutz der Koalitionsfreiheit. Das besondere Verarbeitungsverbot von Daten zur Zugehörigkeit in einer Gewerkschaft und einer gewerkschaftlichen Organisation richtet sich insbesondere gegen eine mögliche Dis-

kriminierung auf dem Arbeitsmarkt. Es spielt keine Rolle, ob die Gewerkschaft parteipolitisch oder insofern neutral ausgerichtet ist, wie groß die Gewerkschaft ist, ob es sich um eine Einheits- oder um eine in Konkurrenz stehende Beschäftigtenorganisation handelt.

□ Genetische Daten

➤ Definition:

Genetische Daten sind die ererbten oder erworbenen genetischen Merkmale eines Menschen, die aus der Analyse einer biologischen Probe des Betroffenen, insbesondere durch DNA- oder RNA-Analyse oder Analyse eines anderen Elements, durch die entsprechende Informationen erlangt werden können, gewonnen werden. Die Merkmale liefern eine eindeutige Information über die Physiologie oder Gesundheit des Menschen. Äußerlichkeiten, wie z.B. die Augen- oder die Haarfarbe, fallen nicht unter dieses Merkmal (siehe im Folgenden biometrische Daten).

□ Biometrische Daten

➤ Definition:

Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, welche die eindeutige Identifizierung dieses Menschen ermöglichen oder bestätigen, wie z.B. Gesichtsbilder oder daktyloskopische Daten (Fingerabdrücke).

□ Gesundheitsdaten

➤ Definition:

Gesundheitsdaten beziehen sich auf die körperliche oder geistige Gesundheit der betroffenen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, aus denen Informationen über deren Gesundheitszustand hervorgehen. Erfasst werden der bisherige, der derzeitige oder auch der künftige Gesundheitszustand.

Vom Begriff erfasst sind Beschreibungen über den Gesundheitszustand sowie über Differenzierungsfähige körperliche und seelische Merkmale, wie z.B. Gewicht, Größe, „Schönheitsfehler“, Befunddaten wie z.B. Röntgenbilder, Blutgruppe, Untersuchungsergebnisse, Ereignisse wie z.B. Operationen, Unfälle, Impfungen, Krankheiten, seien sie akut oder chronisch, körperlich oder seelisch, sichtbar oder unsichtbar, medizinische Bewertungen wie z.B. die Einstufung als Schwerbehinderter oder eine Krankschreibung für den Arbeitgeber, die Einnahme von Stoffen mit gesundheitlicher Wirkung wie z.B. von Alkohol, Drogen oder Medikamenten, der kurzfristige oder längerdauernde Aufenthalt in gesundheitsrelevanten Einrichtungen wie z.B. allgemeinen Krankenhäusern, Aids-, Krebs- oder Kurkliniken, Pflegeheimen, Arzt- oder Heilpraxen, psycho-sozialen Wohngruppen oder Maßregelvollzugsanstalten, Bestands-, Verkehrs- wie auch Inhaltsdaten des Telekommunikationsverkehrs zwischen Betroffenen und Gesundheitseinrichtungen wie auch Kommunikationsinhalte generell. Dazu gehören auch Nummern, Symbole oder Kennzeichen, die einer Person zugeteilt wurden, um diese für medizinische Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, einschließlich genetischer Daten und biologischer Proben, abgeleitet wurden, sowie Informationen über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand, unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem medizinischen Personal, einem Krankenhaus, einem medizinischen Gerät oder

einem In-Vitro-Diagnose-Test stammen. Die Zugehörigkeit zu einer bestimmten Krankenkasse oder Krankenversicherung oder der Umstand einer Beihilfeberechtigung ist kein Gesundheitsdatum.

Sozialdaten:

➤ Definition:

Sozialdaten sind personenbezogene Daten, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach den Sozialgesetzbüchern verarbeitet werden. Sozialdaten können zugleich auch Gesundheits- oder sonstige besondere Kategorien personenbezogener Daten sein, so etwa medizinische Diagnosen, behandelnde Ärzte oder Mütterchaften, aber z.B. auch eine spezifische Form des Versicherungsschutzes sowie die Teilnahme an einem strukturierten Behandlungsprogramm bei chronischen Erkrankungen. Zur Abgrenzung: Bei Krankenversicherungen vorliegende Angaben über Arbeitgeber, Einkommen oder Konfession sind für sich keine Gesundheitsdaten.

Daten zum Sexualleben oder der sexuellen Orientierung

➤ Definition:

Daten zum Sexualleben oder der sexuellen Orientierung umfassen Informationen über Hetero-, Bi- oder Homosexualität, sowie auch der Umstand einer Geschlechtsumwandlung, die Zugehörigkeit zu einem „dritten Geschlecht“ und, ob jemand nicht in einer Ehe, sondern in einer eingetragenen Lebenspartnerschaft lebt.

Daten über strafrechtliche Verurteilungen, Straftaten

[Erläuterung zu den rechtlichen Folgen der jeweiligen Einordnung mit Blick auf die Legitimation zur Datenverarbeitung inkl. weiterer Nachweise in D6.2 Gliederungspunkt D.]

V. Werden die Verarbeitungsgrundsätze für den Umgang mit personenbezogenen Daten nach der DS-GVO beachtet?

1. Verbotsprinzip mit Erlaubnisvorbehalt

➤ Definition:

Zentraler Grundsatz und Ausgangspunkt einer jeden datenschutzrechtlichen Betrachtung ist das so genannte „Verbotsprinzip mit Erlaubnisvorbehalt“: Demgemäß ist jede Verarbeitung personenbezogener Daten grundsätzlich untersagt – es sei denn, sie ist durch eine Rechtsgrundlage gedeckt. Hierbei kommen die datenschutzrechtliche Einwilligung und die gesetzlichen Erlaubnistatbestände in Betracht. **Im Ergebnis darf somit keine Verarbeitung personenbezogener Daten stattfinden, die nicht durch einen datenschutzrechtlichen Legitimationstatbestand gedeckt ist!**

[Erläuterung in D6.2 Gliederungspunkt C.I.]

Ja

Nein

2. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

➤ Definition:

Aus dem Transparenzgrundsatz folgt, dass der betroffenen Person alle Informationen zur Verfügung zu stellen sind, die für eine Einschätzung und Beurteilung der konkreten Verarbeitung ihrer personenbezogenen Daten erforderlich sind. Der Transparenzgrundsatz verlangt von der verantwortlichen Stelle zum einen die transparente Ausgestaltung einer Einwilligungserklärung und zum anderen den transparenten Umgang mit personenbezogenen Daten. Infolgedessen muss die betroffene Person zum Zeitpunkt der Datenerhebung über die konkrete Datenverarbeitung informiert werden. Anforderungen an die Informationspflicht („Datenschutzerklärung“) finden sich in den Art. 12, 13 und 14 DS-GVO.

[Erläuterung der informierten Einwilligung in D6.2 Gliederungspunkt D.I.4.]

Ja

Nein

3. Bestimmtheit und Zweckbindung

➤ Definition:

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer Weise verarbeitet werden, die mit diesen Zwecken unvereinbar ist. Dies bestimmt Art. 5 Abs. 1 lit. b DS-GVO mit dem sog. „Zweckbindungsgrundsatz“. Aufgrund des regelmäßig gemeinnützigen Charakters der wissenschaftlichen Forschung sieht die DS-GVO jedoch Privilegien für die Forschung vor, indem eine Fiktion der Vereinbarkeit mit den ursprünglichen Zwecken für wissenschaftliche Forschungszwecke ermöglicht wird. So wird gesetzlich bestimmt, dass eine Weiterverarbeitung für wissenschaftliche Forschungszwecke nicht als unvereinbar mit den ursprünglichen Zwecken gilt. Eine Weiterverarbeitung muss dabei jedoch den geeigneten Garantien des Art. 89 Abs. 1 DS-GVO unterliegen. Wo der Forschung somit einerseits Privilegien eingeräumt werden, gehen mit diesen Privilegien andererseits auch erhöhte datenschutzrechtliche Anforderungen einher. **Folgende Fragen stellen sich deshalb in diesem Zusammenhang:**

Welchem Zweck dient die Datenverarbeitung?

Kann der Forschungszweck genau definiert werden?¹

Welche Daten werden zur Erreichung des Zwecks konkret benötigt (Stichwort: Datenminimierung)?

[Erläuterung in D6.2 Gliederungspunkt C.III.]

4. Datenminimierung

➤ Definition:

Der Grundsatz der Datenminimierung bestimmt, dass sich die Datenerhebung auf das für die Verarbeitung erforderliche Maß beschränken sollte. Dies ist dann der Fall, wenn die Aufgabe des Verantwortlichen ohne die Datenverarbeitung nicht, nicht rechtzeitig, nicht

¹ Falls nein, sind für diesen Fall die Besonderheiten des sog. „Broad Consent“ zu berücksichtigen. Demgemäß können betroffene Personen ihre Einwilligung lediglich für bestimmte Bereiche wissenschaftlicher Forschung erteilen, wenn dies unter Einhaltung der anerkannten ethischen Standards wissenschaftlicher Forschung geschieht. Siehe dazu D6.2 D.III.3.

vollständig oder nur mit einem unverhältnismäßigen Aufwand erfüllt werden könnte. Entscheidende Frage ist somit – und dies gilt auch im Kontext der wissenschaftlichen Forschung – ob im Einzelfall eine ebenso effektive Alternative zur Datenverarbeitung mit geringerer Eingriffstiefe vorhanden ist. **Wurde der Grundsatz der Datenminimierung beachtet?**

[Erläuterung in D6.2 Gliederungspunkt C.IV.]

- Ja
- Nein

5. Speicherbegrenzung

➤ Definition:

Personenbezogene Daten müssen grundsätzlich in einer Form gespeichert werden, die eine Identifizierung der betroffenen Person nur so lange ermöglicht, wie dies zur Erreichung der Verarbeitungszwecke erforderlich ist, Art. 5 Abs. 1 lit. e DS-GVO. Für die Datenverarbeitung zu Zwecken der wissenschaftlichen Forschung ist auch hier wieder eine Privilegierung vorgesehen: Personenbezogene Daten dürfen demnach, sofern sie ausschließlich für wissenschaftliche Forschungszwecke verarbeitet werden, länger gespeichert werden, soweit geeigneten Garantien gem. Art. 89 Abs. 1 DS-GVO getroffen werden. **Wurde der Grundsatz der Speicherbegrenzung beachtet?**

[Erläuterung in D6.2 Gliederungspunkt C.V.]

- Ja
- Nein

6. Datensicherheit

➤ Definition:

Ausgehend vom Grundsatz der Datensicherheit müssen personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen (sog. TOM) so verarbeitet werden, dass eine angemessene technische Sicherheit (Datensicherheit) der personenbezogenen Daten gewährleistet ist (Art. 32 DS-GVO). Hierbei orientiert sich das Gesetz am unbestimmten Rechtsbegriff „Stand der Technik“. Einbezogen werden müssen dabei die Art und Anzahl verarbeiteter Daten, das wissenschaftliche Verfahren und auch die eventuell auftretende veränderte Bedrohungslage in der Datensicherheit. Zur Datensicherheit gehört im Sinne der klassischen Ziele der IT-Sicherheit: der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Beschädigung. **Wurde der Grundsatz der Datensicherheit beachtet?**

[Erläuterung in D6.2 Gliederungspunkt C.VI.]

- Ja
- Nein

VI. Welche Personen/Einrichtungen sind an der Datenverarbeitung beteiligt?

➤ Definition:

Sind andere Personen oder Einrichtungen an einer Datenverarbeitung beteiligt oder werden personenbezogene Daten an andere Einrichtungen übermittelt, kann dies datenschutzrechtlich eine Auftragsverarbeitung gem. Art. 28 DS-GVO oder eine Datenübermittlung dar-

stellen, die einer Legitimationsgrundlage bedarf. Die erhöhten datenschutzrechtlichen Anforderungen bei der Einbeziehung Dritter folgen aus der mit der Offenlegung gegenüber einem weiteren Personenkreis verbundenen Gefährdungslage für die Daten.



ACHTUNG: Das Rechtsverhältnis ist für diesen Fall durch einen Datenschutzbeauftragten zu prüfen und entsprechende Verträge sind auf den Weg zu bringen. Eine Auftragsverarbeitung ohne entsprechende vertragliche Grundlage im Vorfeld ist unzulässig! Zu beachten ist ebenfalls, dass auch eine Datenübermittlung innerhalb eines Unternehmens/einer Einrichtung ggf. einer vertraglichen Grundlage bedarf.

Folgende Fragen sind im Kontext der wissenschaftlichen Forschung zu berücksichtigen:

1. Wie ist das Rechtsverhältnis zu den an der Datenverarbeitung beteiligten Personen ausgestaltet?

Verarbeiten die Personen/Einrichtungen die personenbezogenen Daten als „verlängerter Arm“ weisungsgebunden und ohne eigene Entscheidungsbefugnis? (→ „Auftragsverarbeiter“, Art. 28 DS-GVO)

Werden die personenbezogenen Daten mit weiteren Stellen gemeinsam genutzt? (→ Gemeinsame Verantwortlichkeit, Art. 26 DS-GVO)

Sind die datenverarbeitenden Stellen ggf. eigenständige, voneinander unabhängige Verantwortliche?

2. Handelt es sich um Beschäftigte / Studierende / Forschende?

Ja

Nein

a. Sind diese Personen auf das Datengeheimnis verpflichtet worden?

Ja

Nein

b. Wurde die Einrichtung (z.B. Universität, (Hoch-)schule über die Datenverarbeitung informiert bzw. besteht ein Forschungsauftrag?

Ja

Nein

c. Haben Abstimmungen mit dem Datenschutzbeauftragten der Forschungseinrichtung stattgefunden?

Ja

Nein

VII. Erfolgt im Rahmen der Einbeziehung Dritter eine Datenübermittlung in Länder außerhalb der EU/des EWR ohne Angemessenheitsbeschluss?

➤ Definition:

Drittstaaten im Sinne der DS-GVO sind solche Länder, die nicht zum europäischen datenschutzrechtlichen Binnenraum gehören und für die auch kein Angemessenheitsbeschluss der EU-Kommission vorliegt. Infolge der damit verbundenen erhöhten Gefährdungslage für den Datenschutz fordert das europäische Datenschutzrecht deshalb, dass das fehlende Schutzniveau auf alternativem Wege herzustellen ist, beispielsweise durch Standarddatenschutzklauseln (SCC). Beispiele für eine solche Drittstaaten-Übermittlung im Forschungskontext können die Einbeziehung von ausländischen Forschungseinrichtungen in einem Konsortium oder die Verwendung ausländischer Cloud-Services sein.



Aufgrund der mit der Auslandsdatenübermittlung erhöhten rechtlichen wie technisch-organisatorischen Komplexität sollte zwingend der Datenschutzbeauftragte einbezogen werden – das ist auch dann der Fall, wenn außereuropäische Cloud-Anbieter zu Verarbeitung von personenbezogenen Daten genutzt werden, die ihre Rechenzentren in der EU belegen haben (z.B. Microsoft 365).

[Erläuterung mit vertieften Hinweisen zum „zweistufigen Vorgehen“ in D6.2 Gliederungspunkt E.]

Ja

Nein

VIII. Welche Rechtsgrundlagen sind zur Legitimation der Verarbeitung der personenbezogenen Daten im Forschungskontext heranzuziehen?

Hinweis: An dieser Stelle ist zur Legitimation der Datenverarbeitung entscheidend, ob „allgemeine“ personenbezogene Daten gem. Art 6. DS-GVO oder besondere personenbezogene Daten („sensible“ Daten) gem. Art 9 DS-GVO vorliegen (siehe vorangehenden Prüfungspunkt Nr. IV). Jeweils zur Legitimation zur Verfügung stehen die datenschutzrechtliche Einwilligung und gesetzliche Erlaubnistatbestände, die jeweils gleichrangig sind.



Insbesondere die korrekte Bestimmung der richtigen Legitimationsgrundlage einer Verarbeitung von personenbezogenen Daten und des Vorliegens ihrer tatbestandlichen Voraussetzungen sollte durch einen Datenschutzbeauftragten überprüft werden.

Im Folgenden werden die Voraussetzungen einer wirksamen datenschutzrechtlichen Einwilligung nach Art. 6 und Art. 9 DS-GVO aufgelistet.

[Detaillierte Erläuterung der Legitimationsmöglichkeiten zur Datenverarbeitung basierend auf Einwilligung und allgemeinen/bereichsspezifischen gesetzlichen Erlaubnistatbeständen in D6.2 Gliederungspunkt D.]

1. Auf welcher Rechtsgrundlage werden „einfache“ Kategorien personenbezogener Daten verarbeitet?

- Auf Grundlage einer Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO (untenstehend weitere Konkretisierung)
- Auf Grundlage eines gesetzlichen Erlaubnistatbestands
- **Datenschutzrechtliche Anforderungen an die Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO:**

➤ Hinweis:

Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben sowie in leicht zugänglicher Form und in einer klaren und einfachen Sprache abzufassen. Die Einwilligung muss nachgewiesen werden können!

- Hat die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben?
- Wurde die Einwilligung freiwillig vor dem Beginn der Datenverarbeitung erklärt?
- Ist die Einwilligung bestimmt erfolgt?
- Ist die Einwilligung informiert erfolgt?
- Wurde die betroffene Person über die Widerrufbarkeit der Einwilligung informiert und besteht die Möglichkeit die Einwilligung zu widerrufen?
- Wurde für die Einwilligung seitens der Aufsichtsbehörde o.Ä. ein Verfallsdatum festgelegt?

2. Auf welcher Grundlage werden besondere Kategorien personenbezogene Daten verarbeitet?

- Auf Grundlage eine Einwilligung gem. Art. 9 Abs. 2 lit. a DS-GVO (untenstehend weitere Konkretisierung)
- Auf Grundlage eines gesetzlichen Erlaubnistatbestands
- **Datenschutzrechtliche Anforderungen an die Einwilligung gem. Art. 9 Abs. 2 lit. a DS-GVO:**

➤ Definition:

Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben sowie in leicht zugänglicher Form und in einer klaren und einfachen Sprache abzufassen. Die Einwilligung muss nachgewiesen werden können!

- Hat die betroffene Person in die Verarbeitung der genannten sensiblen personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt?
- Wurde die Einwilligung freiwillig vor dem Beginn der Datenverarbeitung erklärt?

- Ist die Einwilligung bestimmt erfolgt?
- Ist die Einwilligung informiert erfolgt?
- Wurde die betroffene Person über die Widerrufbarkeit der Einwilligung informiert und besteht die Möglichkeit die Einwilligung zu widerrufen?
- Wurde für die Einwilligung seitens der Aufsichtsbehörde o.Ä. ein Verfallsdatum festgelegt?
- Bedarf es neben der Einwilligung auch der Schweigepflichtentbindung? **[Erläuterung in D6.2 Gliederungspunkt D.I.9.]**

IX. Werden betroffene Personen gem. Art. 13 und 14 DS-GVO transparent über die Datenverarbeitung informiert?

1. Enthält die Datenschutzzinformation alle wesentlichen Angaben? Checkliste:

- Rechtsgrundlage der Datenverarbeitung:** Tatbestände aus der DS-GVO bzw. aus dem nationalen Recht (Einwilligung oder gesetzlicher Erlaubnistatbestand) **[Erläuterung in D6.2 Gliederungspunkt D.]**
- Art, Umfang und Dauer der Datenverarbeitung:** Welche Daten werden auf welche Weise durch welche Stelle für wie lange verarbeitet? Finden Datenübermittlungen an Dritte statt? Existiert ein fester Lösungszeitpunkt bzw. gibt es Anhaltspunkte zur Bestimmung der Speicherdauer?
- Zweck der Datenverarbeitung:** Was wird mit der Datenverarbeitung bezweckt? Ist die Datenverarbeitung zur Erreichung dieses Zwecks tatsächlich erforderlich? Wird der benannte Zweck eingehalten bzw. findet eine Durchbrechung der Zweckbindung statt?
- Betroffenenrechte:** Für jede Datenverarbeitung sind Informationen zu erteilen, welche jeweiligen Rechte den betroffenen Personen zur Verfügung stehen. Für den Fall der datenschutzrechtlichen Einwilligung ist auf die Möglichkeit des Widerrufs hinzuweisen (siehe zu den Betroffenenrechten im Folgenden Prüfungspunkt X.).
- Kontakt Daten des Verantwortlichen:** Nennung des Ansprechpartners für Datenschutzfragen, ggf. Kontakt des Datenschutzbeauftragten, falls ein solcher bestellt wurde.
- Datenübermittlung in das Nicht-EU-Ausland:** Bestehen gültige Datenschutzabkommen bzw. werden anderweitige Garantien vorgesehen, um einen angemessenen, dem europäischen Niveau entsprechenden Maßstab auch im Ausland zu gewährleisten?

2. Wird/wurde die Datenschutzinformation vor Beginn der Datenverarbeitung ausgehändigt oder haben betroffene Personen die Möglichkeit, die Datenschutzinformation auf einer Webseite einzusehen?

Ja

Nein

X. Werden die datenschutzrechtlichen Betroffenenrechte berücksichtigt und eingehalten?

➤ Definition:

Durch Art. 15 bis Art. 22 DS-GVO werden betroffenen Personen die sog. „Betroffenen“-Rechte eingeräumt, die diese gegenüber dem für die Verarbeitung der Daten Verantwortlichen geltend machen können.



Die verantwortliche Stelle muss begründete Betroffenenanfragen nach Art. 12 Abs. 3 DS-GVO grds. unverzüglich (innerhalb eines Monats) umsetzen.

Gem. Art. 89 Abs. 2 DS-GVO können Ausnahmen von einzelnen untenstehenden Rechten getroffen werden, wenn diese die Verwirklichung der spezifischen Forschungszwecke unmöglich machen oder ernsthaft beeinträchtigen. Ob eine solche Ausnahme vorliegt, ist jedoch durch einen Datenschutzbeauftragten für den konkreten Einzelfall zu prüfen!

Folgende Rechte können von der durch die Datenverarbeitung betroffenen Person ggü. der verantwortlichen Stelle eingefordert werden – dementsprechend sollten angemessene Vorkehrungen im Vorfeld der Datenverarbeitung getroffen werden, um diese Rechte erfüllen zu können. Checkliste:

Auskunft

➤ Definition:

Wenn die betroffene Person von ihrem Auskunftsrecht gem. Art. 15 DS-GVO Gebrauch macht, muss die Verantwortliche Stelle Auskunft darüber geben, ob und wenn ja in welchem Umfang welche personenbezogenen Daten verarbeitet werden. Das Auskunftsrecht bezieht sich dabei sowohl auf die Metadaten, die über die betroffene Person gespeichert sind, als auch auf die eigentlichen Inhaltsdaten.



Von diesem Recht kann für die wissenschaftliche Forschung gem. Art. 89 Abs. 2 DS-GVO eine Ausnahme vorgesehen werden. Dies ist durch einen Datenschutzbeauftragten zu prüfen.

Berichtigung

➤ Definition:

Mit dem Recht auf Berichtigung gem. Art. 16 DS-GVO erhält die betroffene Person das Recht auf Korrektur unrichtiger Daten oder Vervollständigung oder Ergänzung von unvollständigen Daten. Hierdurch wird dem Recht auf informationelle Selbstbestimmung in besonderem Maße Rechnung getragen.



Von diesem Recht kann für die wissenschaftliche Forschung gem. Art. 89 Abs. 2 DS-GVO eine Ausnahme vorgesehen werden. Dies ist durch einen Datenschutzbeauftragten zu prüfen.

Einschränkung (Sperrung)

➤ Definition:

Die betroffene Person kann von dem Verantwortlichen verlangen, dass die Verarbeitung eingeschränkt wird, wenn eine der vier Voraussetzungen des Art. 18 Abs. 1 DS-GVO gegeben sind.



Von diesem Recht kann für die wissenschaftliche Forschung gem. Art. 89 Abs. 2 DS-GVO eine Ausnahme vorgesehen werden. Dies ist durch einen Datenschutzbeauftragten zu prüfen.

Löschung

➤ Definition:

Die betroffene Person kann verlangen, dass die sie betreffenden personenbezogenen Daten gelöscht werden, sofern eine der Voraussetzungen des Art. 17 Abs. 1 DS-GVO vorliegen. Löschung der Daten meint die absolute technische Unkenntlichmachung der Datensätze.

Widerspruch

➤ Definition:

Werden personenbezogene Daten auf Grundlage eines berechtigten Interesses gem. Art. 6 Abs. 1 lit. f DS-GVO (Interessenabwägungsklausel) durch einen Verantwortlichen verarbeitet, hat die betroffene Person das Recht, der Datenverarbeitung gem. Art. 21 DS-GVO zu widersprechen.



Von diesem Recht kann für die wissenschaftliche Forschung gem. Art. 89 Abs. 2 DS-GVO eine Ausnahme vorgesehen werden. Dies ist durch einen Datenschutzbeauftragten zu prüfen.

Übertragung (Datenportabilität)

➤ Definition:

Das Recht auf Datenübertragbarkeit/Datenportabilität ermöglicht es betroffenen Personen gem. Art. 20 DS-GVO, die von ihnen bereitgestellten Daten in einem bestimmten (auch maschinenlesbaren) Format zu erhalten und die Möglichkeit, die personenbezogenen Daten unmittelbar an einen anderen Verantwortlichen übermitteln zu lassen.

XI. Werden die technischen und organisatorischen Maßnahmen zur Datensicherheit angemessen umgesetzt?

➤ Definition:

Art. 32 DS-GVO regelt die Sicherheit der Verarbeitung von personenbezogenen Daten und behandelt die entsprechenden rechtlichen Festsetzungen. Die Datensicherheit ist dabei kein absoluter juristischer Begriff, sondern orientiert sich an der jeweiligen Bedrohungslage, der Art der verarbeiteten Daten und der jeweiligen Methoden einer Datenverarbeitung. Dies wird durch die Formulierung „unter Berücksichtigung des Stands der Technik“ wiedergegeben. Beispielhaft werden in Art. 32 DS-GVO überdies verschiedene technische und organisatorische Maßnahmen (TOM) aufgezählt. Zu berücksichtigen sind neben dem Stand der Technik laut Gesetz die Implementierungskosten, die Art, der Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit der Risiken für die Datenschutzrechte der betroffenen Personen.

[Erläuterung in D6.2 Gliederungspunkt C.VI.]

Fragenkatalog zur Datensicherheit (nicht abschließend):

Werden geeignete technische und organisatorische Maßnahmen (TOM) ergriffen, die die Sicherheit der verarbeiteten personenbezogenen Daten gewährleisten?

I. **Wie werden die Daten verarbeitet? Welche Software oder Dienstleister unterstützen dabei?**

II. **Wurde mit diesen Dienstleistern ein Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO geschlossen?**

Ja

Nein

III. **Ist die Software zur Datenverarbeitung auf dem aktuellsten Stand?**

Ja

Nein

IV. **Erfolgt eine Datensicherung? Wenn ja, wie?**

Ja, _____

Nein

V. **Bestehen Backup und Notfall-Konzepte zur Sicherstellung der Verfügbarkeit der Daten?**

Ja

Nein

VI. Sind Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und Endgeräten vorhanden?

- Ja, _____
- Nein

VII. Wurden Zutrittskontrollmaßnahmen zu Serverräumen/Büroräumen/Laboren getroffen?

- Ja
- Nein

VIII. Existieren Zugangs- und Zugriffsberechtigungen und Passwortparameter?

- Ja, _____
- Nein

IX. Wurden Maßnahmen zur sicheren Datenübertragung getroffen?

- Ja, _____
- Nein

X. Werden sonstige Maßnahmen zur Datensicherheit getroffen, die ebenfalls in die Risikobewertung einfließen können?

- Ja, _____
- Nein

XII. Muss eine Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO durchgeführt werden?

➤ Definition:

Nach Art. 35 Abs. 1 DS-GVO hat der Verantwortliche für einen Verarbeitungsvorgang eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Form der Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge hat. Hierzu hat die Datenschutzaufsicht gem. Art. 35 Abs. 4 DS-GVO entsprechende „Positivlisten“ besonders risikoträchtiger Datenverarbeitungsvorgänge erstellt.²

Folgende Fragen sind zur Feststellung einer Datenschutzfolgenabschätzung zu stellen: Erfolgt eine

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen? (Art. 35 Abs. 3 lit. a DS-GVO)

² <https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/Datenschutz-Folgenabschaetzungen.html>.

- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gem. Art. 9 Abs. 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10? (Art. 35 Abs. 3 lit. b DS-GVO)
- oder eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche? (Art. 35 Abs. 3 lit. c DS-GVO)

XIII. Ist im Rahmen der Datenverarbeitung eine Datenpanne erfolgt?

➤ Definition:

Eine Verletzung des Schutzes personenbezogener Daten, auch Datenpanne genannt, ist ein Vorfall, bei dem unberechtigte Personen Zugriff auf (personenbezogene) Daten erhalten.

- Ja
- Nein

Falls ja: Prüfung, ob eine Meldung an die Aufsichtsbehörde und betroffene Person gem. Art. 33 DS-GVO erforderlich ist.

➤ Definition:

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gem. Art. 55 DS-GVO zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.



Die Prüfung und Einschätzung, ob eine Verletzung des Schutzes personenbezogener Daten zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt und meldepflichtig ist, sollte durch einen Datenschutzbeauftragten vorgenommen werden.

- Ja, die Verletzung des Schutzes personenbezogener Daten führt zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

➔ **Achtung: Fristwahrung beachten!**

- Nein, die Verletzung des Schutzes personenbezogener Daten führt nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

XIV. Gibt es ein Konzept zur Speicherung und Aufbewahrung bzw. Löschung von Daten nach Ablauf ihrer Lebensdauer?

➤ Definition:

Personenbezogene Daten dürfen grundsätzlich nur so lange verarbeitet werden, wie diese für die festgelegten Zwecke der Datenverarbeitung erforderlich sind. Wenn der

*Zweck ihrer Verarbeitung entfällt, sind die Daten regelmäßig zu löschen. Es obliegt somit dem datenschutzrechtlich Verantwortlichen, die Löschfristen umzusetzen und ggf. bemessen an seinen Verarbeitungszwecken vorab zu bestimmen. Für die wissenschaftliche Forschung bestehen Ausnahmen und personenbezogene Daten dürfen unter Umständen länger gespeichert sowie weiterverarbeitet werden. **Diese Ausnahmen sollten zusammen mit dem Datenschutzbeauftragten erörtert werden.***

[Erläuterung in D6.2 Gliederungspunkt C. und D.]

- Ja
- Nein