Verzeichnis von Verarbeitungstätigkeiten[1]: Hinweise zur Erstellung

Eine Ausarbeitung der

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Version 1.0

Stand der Bearbeitung: 02. August 2016

Autoren (alphabetisch)

Christoph Isele	Cerner Deutschland GmbH
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Kanzlei Spyra

[1] Gemäß Art. 30 Abs. 1,2 der europäischen Datenschutzgrundverordnung (DS-GVO).

Inhaltsverzeichnis

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Dieses Werk ist unter einer Creative Commons-Lizenz (4.0 Deutschland Lizenzvertrag) lizenziert.

D. h. Sie dürfen:

- Teilen: das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten
- Bearbeiten: das Material remixen, verändern und darauf aufbauen

und zwar für beliebige Zwecke, sogar kommerziell. Der Lizenzgeber kann diese Freiheiten nicht widerrufen solange Sie sich an die Lizenzbedingungen halten.

Die Nutzung ist unter den folgenden Bedingungen möglich:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Weitergabe unter gleichen Bedingungen: Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.
- Keine weiteren Einschränkungen Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.

Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

https://creativecommons.org/licenses/by-sa/4.0/deed.de

bzw. für den vollständigen Lizenztext

https://creativecommons.org/licenses/by-sa/4.0/legalcode

Einleitung

Ziel dieser Ausarbeitung ist es, bei der Erstellung des durch Art. 30 der europäischen Datenschutzgrundverordnung (DS-GVO) geforderten „Verzeichnis von Verarbeitungstätigkeiten“ Unterstützung zu leisten. Dazu werden zum einen die in Art. 30 genannten Anforderungen dargestellt, insbesondere die benötigten Felder eines entsprechenden Verzeichnisses dargestellt und eine Interpretationshilfe bzgl. einiger Begrifflichkeiten angeboten. Zum anderen werden auch Hinweise z.B. bzgl. der Interpretation dieser Anforderungen gegeben. Dabei unterscheidet das Dokument auch zwischen den Anforderungen, die an einen Verantwortlichen und einen Auftragsverarbeiter gestellt werden.

Diesen Überlegungen folgend, besteht das Dokument deshalb aus drei Abschnitten:

1) Hinweise, was bei einem Verzeichnis der Verarbeitungstätigkeiten zu beachten ist.
2) Mindestvorgaben bzgl. des Inhaltes des Verzeichnisses für den Verantwortlichen.
3) Angaben, was ein Auftragnehmer in seinem Verzeichnis mindestens (für jeden Auftraggeber) darstellen muss.

Es ist nicht die Auffassung der Autoren, dass bei den heutigen Möglichkeiten, welche die Methoden der modernen Informationstechnologie bieten, ein Tätigkeitsverzeichnis in Papierform oder als Word-Datei der beste Weg zur Abbildung der Anforderungen der DS-GVO ist. Vielmehr sollte idealerweise das Tätigkeitsverzeichnis mit anderen IT-Systemen verknüpft werden, so dass beispielsweise Kontaktdaten für das Tätigkeitsverzeichnis direkt aus dem digitalen Adressbuch des Unternehmens eingefügt oder konkrete Maßnahmen zur Darstellung der Sicherheit eines Verfahrens direkt aus dem IT-Sicherheitskonzept übernommen werden können.

Wichtig ist dabei jedoch, dass für das Tätigkeitsverzeichnis eine nachvollziehbare Historie vorhanden ist; denn nur so lässt sich der vom Gesetzgeber verfolgte Zweck, der Aufsichtsbehörde ein Werkzeug zur Überprüfung der Legitimität der Datenverarbeitung an die Hand zu geben, erfüllen.

Abschnitt I: Hinweise

1 „Übergangsregelung“

Die Übergangszeit zum Erfüllen der (vollständigen) Anforderungen der DS-GVO endet am 25. Mai 2018. Ab diesem Zeitpunkt müssen die Verarbeitungen beim Verantwortlichen den Anforderungen der DS-GVO genügen.

Mithin sollte die Zeitspanne des Inkrafttreten der DS-GVO (= 24 Mai 2016) bis zum Eintreten der direkten Wirksamkeit (= 25. Mai 2018) als Zeitraum zur Anpassung der eigenen Verarbeitungsprozesse und -Workflows an die Erfordernisse der DS-GVO interpretiert werden.

2 Verantwortlichkeiten

Verantwortlich für die Erstellung bzw. das Vorhandensein des Verzeichnisses sowie der entsprechenden Aktualisierungen ist „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

In der Praxis dürfte deshalb diese Verantwortlichkeit der mit der Führung des Unternehmens / Organisation betrauten Person(en) wie z. B. Geschäftsführer, Vorstand etc. obliegen

3 Zielsetzung der Erstellung und Führen des Verzeichnisses

Entsprechend Erwägungsgrund 82 soll das in Art. 30 der europäischen Datenschutzgrundverordnung (DS-GVO) geforderte „Verzeichnis von Verarbeitungstätigkeiten“ u.a. dazu dienen, der Aufsichtsbehörde die Möglichkeit zu bieten, „die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse“ kontrollieren zu können. Dieses wiederum hat zur Konsequenz, dass in diesem Verzeichnis **alle** Verfahren geführt werden müssen, welche in der Zuständigkeit des Verantwortlichen bzw. im Aufgabenbereich des Auftragsverarbeiters liegen. Folglich sollte man in einem ersten Schritt alle Datenverarbeitungsprozesse identifizieren, diese entsprechend dokumentieren, um sie dann kompakt in einem den Anforderungen von Art. 30 entsprechenden Verzeichnis darzustellen.

4 Unterschiede zu den Regelungen im BDSG

Neben kleineren Abweichungen bzgl. des Inhaltes des Verzeichnisses gibt es im Vergleich zum BDSG in Art. 30 DS-GVO darüber hinaus einige Unterscheidungen bzgl. der Rahmenbedingungen. Die wesentlichen Unterschiede sollen im Nachfolgenden dargestellt werden:

1. Hinsichtlich der Auftragsdatenverarbeitung fordert(e) das BDSG einen schriftlichen Auftrag bzw. eine entsprechende „Regelung“ (vgl. § 11 Abs. 2 BDSG). Unabhängig vom Wortlaut wurden in der Praxis überwiegend ADV-Verträge abgeschlossen. Die europäische DS-GVO verlangt nunmehr explizit einen Vertrag. Die DS-GVO fordert in Art. 30, dass in dem Verzeichnis **alle** Verarbeitungstätigkeiten aufgeführt werden müssen, die im Verantwortlichkeits- bzw. dem Zuständigkeitsbereich des Verantwortlichen liegen. Das BDSG forderte hingegen in § 4 e, dass nur meldepflichtige, automatisierte Verfahren zu

dokumentieren sind. D. h. die Dokumentationsanforderungen der DS-GVO sind nun deutlich weiter gefasst als die Anforderungen des BDSG.

2. Das BDSG enthält in § 4d Abs. 5 S.2 Ausnahmetatbestände, wann ein Verfahrensverzeichnis nicht angelegt werden braucht. Diese Ausnahmetatbestände sind:
   - eine gesetzliche Verpflichtung (zur Verarbeitung) liegt vor
   - eine (wirksame) Einwilligung des Betroffenen in die Datenverarbeitung liegt vor
   - die Erhebung, Verarbeitung oder Nutzung ist für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich.

   Die DS-GVO kennt diese Ausnahmetatbestände nicht.
3. Die Anforderungen des BDSG – und damit auch das Führen eines Verfahrensverzeichnisses - sind von allen Unternehmen, für die das BDSG gilt, zu erfüllen. Art. 30 Abs. 5 DS-GVO befreit Unternehmen von der Pflicht zum Führen eines Tätigkeitsverzeichnisses unter folgenden Umständen:
   - Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, brauchen kein Verzeichnis führen, sofern
     - die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt
     - die Verarbeitung nicht nur gelegentlich erfolgt oder
     - die Verarbeitung nicht besondere Datenkategorien gemäß Artikel 9 Absatz 1 bzw.
     - die Verarbeitung nicht personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.
4. Das BDSG sieht grundsätzlich ein fehlendes Verfahrensverzeichnis nicht als bußgeldbewährte Ordnungswidrigkeit an. Vielmehr konnte nur eine fehlende Meldung entsprechend § 4d Abs. 1 BDSG sanktioniert werden. Da jedoch diese Meldepflicht entfiel, wenn die verantwortliche Stelle einen Datenschutzbeauftragten bestellte, war diese Sanktionsmöglichkeit für die meisten Unternehmen irrelevant, da die meisten Unternehmen einen Datenschutzbeauftragten bestellt haben.
   Im Gegensatz zum BDSG sieht jedoch Art. 83 Abs. 4 lit. a DS-GVO ein Bußgeld von bis zu 10.000.000 Euro bzw. von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (je nachdem, welcher der Beträge höher ist) vor, wenn kein den Anforderungen der DS-GVO entsprechendes Verzeichnis existiert!

5 Interpretation einzelner, relevanter Begrifflichkeiten

Bei der Interpretation der DS-GVO sollte man gerade in den ersten Jahren die Working Paper der Artikel-29-Datenschutzgrupppe beachten, da

1. der Datenschutz-Ausschuss sich letztlich aus denselben Mitgliedern wie die Artikel-29-Datenschutzgruppe zusammensetzt und
2. viele Bereiche der bisherigen Richtlinie 95/46/EG wortwörtlich oder dem Sinn entsprechend in die DS-GVO übernommen wurden, d.h. die Aussage der Artikel-29-Datenschutzgruppe zu den entsprechenden Abschnitten der RL 95/46/EG wird voraussichtlich der Interpretation des Datenschutz-Ausschusses zu den entsprechenden Bereichen der DS-GVO entsprechen.

5.1 Tätigkeit

Wie beim u.a. vom BDSG verwendeten Begriff „Verfahren“ ist auch beim in der DS-GVO verwendeten Begriff „Tätigkeit“ unklar, wie eng oder weit dieser Begriff zu interpretieren ist. Wird nämlich der Begriff „Tätigkeit“ zu eng gewählt / definiert, muss wirklich jede Datenverarbeitungstätigkeit bei dem Verantwortlichen dokumentiert werden, was allein durch den Umfang die Nutzbarkeit des Verzeichnisses zur Kontrolle des Verantwortlichen / Auftragsverarbeiters durch die Aufsichtsbehörden ad absurdum führt. Ein zu weites Verständnis des Begriffs „Tätigkeit“ kann jedoch wiederum auch schnell dazu führen, dass wesentliche Tätigkeiten undokumentiert bleiben und man sich damit dem schon vorstehend erwähnten Bußgeldtatbestand wegen unzureichender Führung des Verzeichnisses aussetzt.

Um diesem Konflikt so gut wie möglich Rechnung zu tragen, sehen es die Verfasser als notwendig an, eine sinnvolle Bündelung von „Tätigkeiten“ durchzuführen. Diesbezüglich dürfte es dem auch in der DS-GVO erhaltenen „Zweckbindungsgebot“ folgend sinnvoll sein, die entsprechenden Tätigkeiten zusammenzufassen, die einem einheitlichen Verarbeitungszweck dienen.

5.2 Verantwortlicher

Eine Definition zum „Verantwortlichen“ findet sich in Art. 4 Abs. 7 DS-GVO. Verantwortlicher ist demnach die natürliche oder juristische

- Person,
- Behörde,
- Einrichtung oder
- andere Stelle,

die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Wesentliches Kennzeichen und damit auch taugliches Abgrenzungskriterium eines Verantwortlichen zu einem Auftragsverarbeiter ist damit (wie bisher) die (alleinige) Entscheidungsbefugnis über die Mittel und Zwecke der Datenverarbeitung.

5.3 Zweck

Der Zweck bzw. die Zwecke der Verarbeitung personenbezogener Daten werden grundsätzlich vom Verantwortlichen festgelegt. Dabei gilt es jedoch zu beachten, dass ein Verantwortlicher nicht vollständig frei die entsprechenden Zwecke festgelegen darf. Vielmehr darf er nur solche Zwecke wählen, die Grundlage der Zulässigkeit der Verarbeitung sind[2]. Daraus folgt zwangsläufig auch, dass ein unzulässiger Zweck wie beispielsweise eine unverhältnismäßige Datenverarbeitung nicht die Verarbeitungsbefugnisse des Verantwortlichen erweitern kann[2].

5.4 Verletzung des Schutzes personenbezogener Daten

Art. 4 Abs. 12 DS-GVO enthält die Definition zur „Verletzung des Schutzes personenbezogener Daten“. Demzufolge liegt eine solche vor, wenn es zu einer Verletzung der Sicherheit, die

- zur Vernichtung,
- zum Verlust oder
- zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder
- zur unbefugten Offenlegung von beziehungsweise

[2] Damman U. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage 2014, Rn.113.

- zum unbefugten Zugang zu

personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, kommt.

Eine „Verletzung des Schutzes personenbezogener Daten“ ist damit in mannigfaltigen Fällen denkbar. Zunächst natürlich immer in den Fällen, in denen „Unbefugte“ auf für sie nicht bestimmte Daten zugreifen können. Dieses dürfte somit für alle Fälle gelten, in denen sich bspw. Hacker unberechtigt Zugang zu den Systemen verschaffen. Darüber hinaus dürften aber sogar schon die Fälle von der Regelung erfasst sein, in denen Mitarbeiter durch ein unzulängliches Rollen- und Berechtigungskonzept (unbefugt) Zugriff auf Daten erhalten, auf die sie eigentlich keinen Zugriff haben dürften.

Aufgrund der weitreichenden Definition von Art. 4 Abs. 12 DS-GVO dürfte ferner eine solche Verletzung auch schon dann vorliegen, wenn Befugte im Rahmen der Datenverarbeitung Daten verändern, vernichten, usw., obwohl eine rechtliche Grundlage wie z. B. ein Vertrag mit dem Betroffenen oder auch ein Gesetz eine Aufbewahrungspflicht der Originaldaten beim Verantwortlichen verlangen.

5.5 Stand der Technik

Die DS-GVO erwähnt in manchen ihrer Regelungen (z. B. in Artt. 25 und 32) den Begriff „Stand der Technik“, ohne jedoch diesen Begriff weiter zu definieren. Weil neben diesem Begriff in der Praxis weitere Begriffe wie „allgemein anerkannte Regeln der Technik“, und „Stand der Wissenschaft und Technik“ oftmals unzutreffend synonym verwendet werden, ist es aus Sicht der Verfasser angezeigt, im Nachfolgenden kurz die jeweiligen Begrifflichkeiten zu erläutern. Dieses insbesondere deshalb, weil diese Begrifflichkeiten sich doch mehr oder weniger unterscheiden und daher u.U. auch andere rechtliche Implikationen mit sich bringen können.

- Allgemein anerkannte Regeln der Technik: Auch wenn dieser Begriff des Öfteren in der Literatur, Rechtsprechung etc. verwendet wird, erfuhr er nie eine Legaldefinition. Vielmehr wird zur Begriffsbestimmung häufig auf die Rechtsprechung zu den „allgemein anerkannten Regeln der Baukunst“, der u.a. in § 319 Abs. 2 StGB verwendet wird, zurückgegriffen. Demnach ist eine Regel (der Baukunst) dann allgemein anerkannt, wenn sie die ganz vorherrschende Ansicht der (technischen) Fachleute darstellt und darüber hinaus in der Praxis erprobt und bewährt ist.
- Stand der Technik: Auch wenn dieser Begriff nun den Einzug in die DS-GVO gefunden hat, wird dieser Begriff zumeist in umwelt- und technikrechtlichen Gesetzen und Verordnungen verwendet, wie z.B. in § 3 Abs. 6 Bundes-Immissionsschutzgesetz (BImSchG). Die Definition im BImSchG wurde bei der Überarbeitung dieses Gesetzes im Jahre 2001 an geltende europäischen Vorgaben angepasst, sodass diese Definition (abgesehen von den umweltspezifischen Aspekten) auch maßgeblich für die Auslegung der DS-GVO angesehen werden kann. So heißt es hier:

    > „Stand der Technik im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Begrenzung von Emissionen in Luft, Wasser und Boden, zur Gewährleistung der Anlagensicherheit, zur Gewährleistung einer umweltverträglichen Abfallentsorgung oder sonst zur Vermeidung oder Verminderung von Auswirkungen auf die Umwelt zur Erreichung eines allgemein

hohen Schutzniveaus für die Umwelt insgesamt gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere die in der Anlage aufgeführten Kriterien zu berücksichtigen."

Diese genannten 13 Kriterien sind:

1. Einsatz abfallarmer Technologie,
2. Einsatz weniger gefährlicher Stoffe,
3. Förderung der Rückgewinnung und Wiederverwertung der bei den einzelnen Verfahren erzeugten und verwendeten Stoffe und gegebenenfalls der Abfälle,
4. vergleichbare Verfahren, Vorrichtungen und Betriebsmethoden, die mit Erfolg im Betrieb erprobt wurden,
5. Fortschritte in der Technologie und in den wissenschaftlichen Erkenntnissen,
6. Art, Auswirkungen und Menge der jeweiligen Emissionen,
7. Zeitpunkte der Inbetriebnahme der neuen oder der bestehenden Anlagen,
8. für die Einführung einer besseren verfügbaren Technik erforderliche Zeit,
9. Verbrauch an Rohstoffen und Art der bei den einzelnen Verfahren verwendeten Rohstoffe (einschließlich Wasser) sowie Energieeffizienz,
10. Notwendigkeit, die Gesamtwirkung der Emissionen und die Gefahren für den Menschen und die Umwelt so weit wie möglich zu vermeiden oder zu verringern,
11. Notwendigkeit, Unfällen vorzubeugen und deren Folgen für den Menschen und die Umwelt zu verringern,
12. Informationen, die von internationalen Organisationen veröffentlicht werden,
13. Informationen, die in BVT-Merkblättern enthalten sind.

Wenngleich natürlich nicht alles aus dem Gesetz 1:1 auf die Regelungen zur Gewährleistung der Anforderungen der DS-GVO übertragen werden kann, bietet das Gesetz eine recht gute Darlegung, was im Sinne des europäischen Gesetzgebers unter Stand der Technik zu verstehen ist.

Auch in der Begründung zum IT-Sicherheitsgesetz[3] findet sich eine Definition zum Stand der Technik, die das in § 3 Abs. 6 BImSchG genannte Prinzip auf die IT adaptiert hat. So heißt es hier:

„Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden."

- Stand der Wissenschaft und Technik: Dieser Begriff umfasst die neuesten technischen und wissenschaftlichen Erkenntnisse. Mithin bedingt dieser Begriff eine intensive Auseinandersetzung / Beachtung der Ergebnisse der aktuellen, wissenschaftlichen Forschung.

[3] Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). S. 14,15. Online, zitiert am 2016-07-12; Verfügbar unter https://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile.

5.6 Pseudonymisierung

Die Legaldefinition der „Pseudonymisierung“ bzw. von „pseudonyme Daten“ findet sich in Art. 4 Abs. 5 DS-GVO. Hiernach sind Daten dann als pseudonyme anzusehen, wenn sie

a) „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person“ zuordenbar und
b) diese zusätzlichen Informationen gesondert aufbewahrt werden und
c) technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Gemäß Erwägungsgrund 26 sollen, um festzustellen, ob eine natürliche Person identifizierbar ist, „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren“, Erwägungsgrund 26 führt diesbezüglich weiter aus, dass bei der Feststellung, „ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden“, alle „objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden“ sollen. Dabei ist die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen, d. h. bei Entwicklungen, die Einfluss auf die Re-Identifizierung nehmen können, wie beispielsweise höhere Rechenleistungen, ist zu überprüfen, ob die Daten noch als pseudonym anzusehen sind oder als re-identifizierbar bewertet werden müssen.

Erwägungsgrund 28 führt aus, dass die ausdrückliche Einführung der "Pseudonymisierung" in der DS-GVO nicht bedeutet, dass keine weiteren Datenschutzmaßnahmen getroffen werden müssen. Die Pseudonymisierung ist deshalb für sich gesehen eine Maßnahme um die „Risiken für die betroffenen Personen zu senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen“.

Dabei bedingt eine Pseudonymisierung nicht notwendigerweise die Nutzung eines sog. „Daten-Treuhänders“. Erwägungsgrund 29 betont vielmehr, dass Pseudonymisierungsmaßnahmen auch bei demselben Verantwortlichen durchaus möglich sind. Daraus folgt wiederum, dass die vorhandenen Daten, einem entsprechend „legalen“ Zweck vorausgesetzt, pseudonymisiert z. B. für allgemeine Analysen genutzt werden können, sofern dabei die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Umsetzung der Anforderungen der DS-GVO getroffen wurden. Insbesondere muss der Verantwortliche dabei sicherstellen, dass die „zusätzlichen Informationen, mit denen die pseudonymen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden“.

Aufgrund der Tatsache, dass es sich bei der Pseudonymisierung auch um eine Verarbeitungshandlung handelt, muss auch bei einer Pseudonymisierung aufgrund der Risikogeneigtheit dieser Verarbeitung, eine Datenschutzfolgenabschätzung erfolgen. So stellt Erwägungsgrund 75 klar heraus, dass auch die „unbefugte Aufhebung der Pseudonymisierung“ zu den Risiken für die Rechte und Freiheiten natürlicher Personen gehört und somit in einer Datenschutzfolgenabschätzung evaluiert werden muss.

Darüber hinaus gehört gemäß Erwägungsgrund 85 schon das Risiko der unbefugten Aufhebung der Pseudonymisierung auch zu den Gründen, die zu einer Meldung gemäß Artt. 33, 34 DS-GVO führen können.

6 Anforderungen an das Verzeichnis

Den Regelungen des Art. 30 DS-GVO folgend, werden folgende Anforderungen an ein Verzeichnis von Verarbeitungstätigkeiten gestellt:

1. Es existiert genau ein Verzeichnis, in dem alle Verarbeitungstätigkeiten für jeden Verantwortlichen (Art. 30 Abs. 1 DS-GVO) bzw. Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO) aufgeführt sind.
2. Das Verzeichnet bildet alle (Mindest-) Inhalte, die in Art. 30 Abs. 1 DS-GVO für den Verantwortlichen bzw. in Art. 30 Abs. 2 DS-GVO für den Auftragsverarbeiter verbindlich festgelegt sind, ab.
3. Das Verzeichnis ist grundsätzlich schriftlich zu führen. Eine elektronische Form ist jedoch auch zulässig (Art. 30 Abs. 3 DS-GVO).
4. Auf Anfrage muss der Verantwortliche bzw. der Auftragsverarbeiter der Aufsichtsbehörde das Verzeichnis zur Verfügung stellen (Art. 30 Abs. 4 DS-GVO).

Da nur ein Verzeichnis existieren soll, ist es offensichtlich, dass die „Stammdaten“ von Verantwortlichen und Auftragnehmer (also Anschrift und entsprechende Kontaktdaten) nur einmal aufgeführt werden müssen.

In diesem Zusammenhang sei insbesondere auf die Forderung von Art. 30 Abs. 2 lit. a hingewiesen, in der festgelegt wird, dass der Auftragnehmer zur jeweiligen Tätigkeit insbesondere auch die Kontaktdaten des Verantwortlichen angeben muss. Diese Forderung lässt sich ferner auch aus Erwägungsgrund 82 herleiten. Denn nur wenn die entsprechenden Informationen vorhanden sind, ist eine Aufsichtsbehörde in der Lage, eine ordnungsgemäße Auftragsvergabe und –abwicklung zu überprüfen.

6.1 Rechenschaftspflicht („Accountability“)

Der Gesetzgeber sieht das Verzeichnis aus Art. 30 DS-GVO als „dynamisch“ an. Dieses hat mithin zur Konsequenz, dass jede identifizierte bzw. definierte Tätigkeit in regelmäßigen Abständen darauf hin zu überprüfen ist, ob die Prozesse auch genauso ablaufen, wie ursprünglich festgestellt und dokumentiert. Dieses wiederum hat zur Konsequenz, dass, wenn sich Verarbeitungstätigkeiten z.B. auf Grund geänderter Anforderungen ändern, diese Änderung auch in der Dokumentation / dem Verzeichnis dargestellt werden muss.

Diese Notwendigkeit wird nochmals durch die in Art. 5 Abs. 2 DS-GVO definierte „Rechenschaftspflicht“ unterstrichen. Nach dieser Pflicht muss der Verantwortliche (jederzeit) nachweisen können, dass die Datenverarbeitung (zu jeder Zeit) rechtskonform erfolgt(e). Diese gesetzliche Anforderung hat mithin zur Konsequenz, dass ein Verzeichnis von Verarbeitungstätigkeiten eine Historie enthalten muss, die entsprechend gepflegt wird, um damit die Einhaltung der Vorgaben der DS-GVO auch für den zurückliegenden Zeitraum nachweisen kann.

Die Artikel-29-Datenschutzgruppe erstellte zum Thema Rechenschaftspflicht im Jahre 2010 ein „Working Paper[4]“, welches das Thema aus ihrer Sichtweise behandelt. Die von der Artikel-29-Datenschutzgruppe in diesem Paper vertretenen Sichtweisen, dürften durchaus weiterhin ihre

[4] Working Paper 173 „Stellungnahme zum Grundsatz der Rechenschaftspflicht“ (2010-07-13). . Online, zitiert am 2016-07-17; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_de.pdf.

Relevanz behalten haben und für die Zukunft (die Geltung der DS-GVO) höchstwahrscheinlich ihre Geltung behalten. (Siehe auch einführende Worte zu Kapitel 5.)

7 Weitergehende Dokumentation

Art. 5 DS-GVO beinhaltet weitere Anforderungen, die u.a. auch die Dokumentationspflicht betrifft. Dieses bedeutet, dass der Verantwortliche weitaus mehr „Dinge“ dokumentieren muss, als in Art. 30 DS-GVO bzgl. der Dokumentation in einem Verzeichnis der Verarbeitungstätigkeiten vorgeschrieben ist. Diese dokumentierten Informationen muss er wie vorstehend beschrieben u.a. aufgrund seiner Rechenschaftspflicht (jederzeit) nachweisen bzw. vorweisen können.

Nach Ansicht der Autoren erscheint es deshalb sinnvoll, einige der (übrigen) von der DS-GVO vorgesehenen Dokumentationspflichten bzw. zu dokumentierenden Informationen mit in das Verzeichnis der Verarbeitungstätigkeiten aufzunehmen. Dieses hat den großen Vorteil, dass die Unterlagen / Informationen, welche die Aufsichtsbehörden zur Überprüfung benötigen, alle an derselben Stelle zu finden sind.

Diesbezüglich sei (informatorisch) auch auf das Working Paper 173 „Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht“ der Artikel-29-Datenschutzgruppe verwiesen. Dieses Dokument enthält u.a. eine beispielhafte Aufzählung von Maßnahmen zur Gewährleistung der „Accountability“. Die dort aufgeführten Beispiele dürften ferner einen guten Eindruck vermitteln, wie sich die Aufsichtsbehörden einen Nachweis hinsichtlich der Rechenschaftspflicht vorstellen.

Weil sich der Gesetzgeber zum Ziel gesetzt hat, mit dem Verzeichnis jederzeit eine Überprüfung zu ermöglichen, ist es angezeigt, dass im Verzeichnis alle relevanten Ansprechpartner benannt werden. Diesbezüglich sieht die DS-GVO jedoch zwingend nur den oder die Verantwortlichen sowie dessen Vertreter und - sofern vorhanden - den Datenschutzbeauftragten vor.

Nach Erfahrungen der Verfasser erleichtert es jedoch die Arbeit einer Aufsichtsbehörde und vermindert die Nachfragen bei einer ggfs. stattfindenden Überprüfung, wenn zusätzlich zu den explizit gesetzlich geforderten Angaben zumindest die für die entsprechenden Verarbeitungstätigkeiten relevanten Personen wie z. B. die IT-Verantwortlichen (IT-Leiter), (falls bestellt) der Informationssicherheitsbeauftragte sowie der entsprechende Verfahrensverantwortliche im Verzeichnis mit aufgeführt werden.

8 Mapping der technischen und organisatorischen Maßnahmen (TOM): DS-GVO vs. BDSG

Wesentlich für eine ordnungsgemäße Datenverarbeitung ist, dass die erforderlichen technischen und organisatorischen Schutzmaßnahmen getroffen wurden. Dabei müssen entsprechend Art. 32 DS-GVO diese Schutzmaßnahmen unter Berücksichtigung

- des Stands der Technik
- der Implementierungskosten
- der Art der Verarbeitung
- dem Umfang der Verarbeitung
- dem Zweck der Verarbeitung
- der Eintrittswahrscheinlichkeit des Risikos für die Rechte und Freiheiten natürlicher Personen

- der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

getroffen werden. D. h. um zu bestimmen, welche spezifischen Schutzmaßnahmen zu treffen sind, ist immer eine Abwägung der Erfordernisse vorzunehmen. Ändern sich die jeweils zu berücksichtigenden Umstände (z.B. eine Änderung der Eintrittswahrscheinlichkeit auf Grund neuer technischer Möglichkeiten), ist eine neue Bewertung und ggfs. die Aktualisierung / Anpassung der Schutzmaßnahmen erforderlich.

Im Nachfolgenden erfolgt zu Visualisierungszwecken eine Gegenüberstellung der von Art. 32 DS-GVO geforderten Maßnahmen mit den Maßnahmen bzw. Kontrollen aus dem Anlage zu § 9 BDSG. Damit soll der Leser in die Lage versetzt werden zu prüfen, wie bzw. wo die von der DS-GVO geforderten Maßnahmen möglicherweise schon heute, im Rahmen der Kontrollen der Anlage zu § 9 BDSG berücksichtigt wurden.

Art. 32 DS-GVO	**Anlage zu § 9 BDSG**
Art. 32 Abs. 1 lit.lit. A Pseudonymisierung personenbezogener Daten	-/-
Art. 32 Abs. 1 lit.lit. a Verschlüsselung personenbezogener Daten	-/-
Art. 32 Abs. 1 lit.lit. b: … Vertraulichkeit, … im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	Zutrittskontrolle Zugangskontrolle Zugriffskontrolle Weitergabekontrolle Auftragskontrolle Zweckbindung
Art. 32 Abs. 1 lit.lit. b: … Integrität, … im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	Eingabekontrolle Auftragskontrolle
Art. 32 Abs. 1 lit. b: … Verfügbarkeit … im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	Verfügbarkeitskontrolle
Art. 32 Abs. 1 lit. b: … Belastbarkeit … im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	-/-
Art. 32 Abs. 1 lit. c: Beschreibung des Verfahrens zur Gewährleistung den Zugang zu den personenbezogenen Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	-/-
Art. 32 Abs. 1 lit. d: Beschreibung der Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	-/-

Im Whitepaper „Datenschutz-Folgenabschätzung - Ein Werkzeug für einen besseren Datenschutz“ werden den u.a. auch in der DS-GVO enthaltenen Schutzzielen entsprechende Maßnahmen

zugeordnet. Dies erleichtert die Zuordnung der eigenen Maßnahmen zu den Schutzzielen der DS-GVO, wobei die nachfolgend dargestellte Tabelle aus dem Whitepaper die Zuordnung in Kurzfassung darstellt[5]:

Schutzziel	Komponente	Maßnahmen
Sicherstellung von Verfügbarkeit	Daten, Systeme, Prozesse	Redundanz, Schutz, Reparaturstrategie
Sicherstellung von Integrität	Daten	Hash-Wert-Vergleich
	Systeme	Einschränkung von Schreibrechten, regelmäßige Integritätsprüfungen
	Prozesse	Festlegung von Referenzwerten (min/max), Steuerung der Regulation
Sicherstellung von Vertraulichkeit	Daten, Systeme	Verschlüsselung
	Prozesse	Rechte- und Rollenkonzepte
Sicherstellung von Nichtverkettbarkeit durch Zweckbestimmung	Daten	Nutzung anonymer Daten, Pseudonymisierung, attributbasierte Credentials
	Systeme	Trennung (Isolierung) von Datenbeständen, Systemen und Prozessen
	Prozesse	Identity Management, Anonymitätsinfrastrukturen, Audits
Sicherstellung von Transparenz durch Prüffähigkeit	Daten	Dokumentation, Protokollierung
	Systeme	Systemdokumentation, Protokollierung von Konfigurationsänderungen
	Prozesse	Dokumentation von Verfahren, Protokollierung
Sicherstellung von Intervenierbarkeit durch Ankerpunkte	Daten	Zugriff auf Daten für den Betroffenen (Auskunft, Berichtigung, Sperrung, Löschung)
	Prozesse	Helpdesk/einheitlicher Ansprechpartner für Änderungen/Löschungen, Change Management

9 Literatur

9.1 Artikel-29-Datenschutzgruppe

Alle Working Paper sind auf der Homepage der Artikel-29-Datenschutzgruppe unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm zu finden

- Working Paper 48 „Stellungnahme zur Verarbeitung personenbezogener Daten von Beschäftigten“ (2001-09-13)

[5] Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt (2016) White Paper Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz. Tabelle 1, S.27,28. Online, zitiert am 2016-07-12; Verfügbar unter https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/aktuelles/aktuelles_047.php

- Working Paper 55 " Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten" (2002-05-29)
- Working Paper 91 „Arbeitspapier über genetische Daten" (2004-03-17)
- Working Paper 1321 „Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)" (2007-02-15)
- Working Paper 136 „Stellungnahme zum Begriff ‚personenbezogene Daten' " (2007-06-20)
- Working Paper 160 „Stellungnahme zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen) (2009-02-11)
- Working Paper 169 „Stellungnahme zu den Begriffen ‚für die Verarbeitung Verantwortlicher' und ‚Auftragsverarbeiter' „ (2009-02-16)
- Working Paper 173 „Stellungnahme zum Grundsatz der Rechenschaftspflicht" (2010-07-13)
- Working Paper 187 „Stellungnahme zur Definition von Einwilligung" (2011-07-13)
- Working Paper 203 „Opinion on purpose limitation „ (2013-04-02)
- Working Paper 211 „Stellungnahme zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung" (2014-02-27)
- Working Paper 213 „Stellungnahme über die Meldung von Verletzungen des Schutzes personenbezogener Daten" (2014-03-25)
- Working Paper 216 „Stellungnahme zu Anonymisierungstechniken" (2014-04-10)
- Working Paper 217 „Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (2014-04-09)

9.2 Datenschutz Folgenabschätzung / Risikoabschätzung

- Drackert S. (2014) Die Risiken der Verarbeitung personenbezogener Daten- Eine Untersuchung zu den Grundlagen des Datenschutzrechts. Duncker & Humblot GmbH. ISBN '978-3-428-1 4730-4
- Eman KE, Dankar KF, Vaillancourt, R, Roffey, T, Lysyk M. (2009) Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records. Can J Hosp Pharm 62(4):307–319
- Forum Privatheit (2016) White Paper Datenschutz-Folgenabschätzung - Ein Werkzeug für einen besseren Datenschutz. Online, zitiert am 2016-04-21; Verfügbar unter https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf

9.3 De-Identifikation

- DIN EN ISO 25237 „Pseudonymisierung" (2015-10, Entwurf)
- Statistische Bundesamt
    - „Handbuch zur Anonymisierung wirtschaftsstatistischer Mikrodaten" (2005-09), Bestellnummer: 1030804059004 https://www.destatis.de/DE/Publikationen/StatistikWissenschaft/Band4_AnonymisierungMikrodaten.html
    - „Verfahren zur Anonymisierung von Einzeldaten (2010-09), Bestellnummer: 1030816-10900-1, ISBN: 978-3-8246-0901-7 https://www.destatis.de/DE/Publikationen/StatistikWissenschaft/Band16_AnonymisierungEinzeldaten.html
- Integrating the Healthcare Enterprise (IHE) International: De-Identification Handbook, basierend auf HIPAA (2014-06)
    - Wiki: http://wiki.ihe.net/index.php/Healthcare_De-Identification_Handbook

  - Benutzerhandbuch: http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_De-Identification_Rev1.1_2014-06-06.pdf
  - http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_De-Identification-Mapping_Rev1.1_2014-06-06.xlsx
- Digital Imaging and Communications in Medicine (DICOM)
  - Supplement 142: Clinical Trial De-identification Profiles (2011-01-25)
  - Correction Proposal 1295: De-identification method code meaning too long (2013-02-22)
  - Correction Proposal 1298: Update description of Detector ID de-identification (2013-03-16)
  - Correction Proposal 1300: Include PPS End Date & Time in Composite IODs and de-identification (2011-08-22)
  - Correction Proposal 1339: Add various new dates, times, serial numbers and UIDs for de-identification (2013-09-30)
- Health Insurance Portability and Accountability Act (HIPAA)
  - De-Identification FAQ http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf
  - Anleitung zur De-Identifikation (Stand 2012) http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html
- National Institute of Standards and Technology (NIST): „De-Identification of Personal Information“ (NISTIR 8053) http://dx.doi.org/10.6028/NIST.IR.8053 bzw. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

Abschnitt II: Verzeichnis von Verarbeitungstätigkeiten: Verantwortlicher

1 Stammdaten

1.1 Namen und die Kontaktdaten des Verantwortlichen[6]

Name / Bezeichnung der datenverarbeitenden Stelle[7]	
Straße Hausnummer[8]	
PLZ / Ort	
Telefon	
Telefax[9]	
E-Mail-Adresse9	
Internet-Adresse[5]	

Angaben zur geschäftlichen Korrespondenz

Rechtsform der Gesellschaft	
Handelsregisternummer9	
Umsatzsteueridentifikationsnummer9	
Wirtschafts-Identifikationsnummer9	

1.2 Persönliche Nennung der verantwortlichen Personen

1.2.1 Geschäftsführung[10]

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[5]	
E-Mail-Adresse[5]	
Internet-Adresse[5]	

[6] Hinweis: siehe hierzu auch Working Paper 169 „Stellungnahme 1/2010 zu den Begriffen ‚für die Verarbeitung Verantwortlicher' und ‚Auftragsverarbeiter' der Artikel-29-Datenschutzgruppe
[7] Name des Unternehmens, der Institution, der Organisation, …
[8] Es muss eine ladungsfähige Anschrift angegeben werden; die Angabe eines Postfachs ist nicht ausreichend, kann aber natürlich als Zusatzinformation angegeben werden.
[9] Sofern vorhanden.
[10] Nennung sämtlicher mit der Geschäftsleitung betrauten Personen. D.h. bei mehreren Geschäftsführern muss diese Tabelle individuell für die Geschäftsführer ausgefüllt werden; jeder Geschäftsführer muss separat aufgeführt werden.

1.2.2 Stellvertretende Geschäftsführung

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[5]	
E-Mail-Adresse[5]	
Internet-Adresse[5]	

1.2.3 Leitung der Datenverarbeitung[11]

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[5]	
E-Mail-Adresse[5]	
Internet-Adresse[5]	

1.2.4 Angaben zur Person des Datenschutzbeauftragten[12]

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[5]	
E-Mail-Adresse[5]	
Internet-Adresse[5]	

[11] Freiwillige Angabe, jedoch ist es für eine Aufsichtsbehörde im Prüfungsfall nützlich zu wissen, wer hier der zuständige Ansprechpartner ist.
[12] Sofern vorhanden, müssen die Kontaktdaten des Datenschutzbeauftragten zwingend angegeben werden.

2 Angaben zur Verarbeitungstätigkeit

2.1 Organisatorische Angaben

2.1.1 Ansprechpartner / Verfahrensverantwortliche

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[5]	
E-Mail-Adresse[5]	
Internet-Adresse[5]	

2.1.2 Zeitangaben

Datum der Einführung	
Datum der Erstbeschreibung	
Datum der letzten Änderung	

2.2 Zweck der Verarbeitung

2.2.1 Bezeichnung des Verfahrens

2.2.2 Zweckbestimmung[13]

[13] Hinweis: Working Paper „Opinion 03/2013 on purpose limitation“ der Artikel-29-Datenschutzgruppe berücksichtigen.

2.3 Rechtsgrundlage[14]

2.3.1 Verarbeitung von Daten, die nicht zu besonderen Kategorien gemäß Art. 9 Abs. 1 DS-GVO zählen

(Art. 6 DS-GVO)

Hinweis: Die Regelungen von Art. 6 bilden keine Erlaubnistatbestände für die Verarbeitung von besonderen Kategorien von Daten. Diesbezüglich enthält Art. 9 DS-GVO (abschließend) entsprechende Legitimationstatbestände.

	Rechtsgrundlage EU DS-GVO
	Einwilligung[15] (Art. 6 Abs. 1 lit. a)
	Zur Vertragserfüllung notwendig (Art. 6 Abs. 1 lit. b)
	Zur Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt, erforderlich (Art. 6 Abs. 1 Lit c)
	Erforderlich, um lebenswichtige Interessen[16] der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6 Abs. 1 lit. d)
	Verarbeitung liegt im öffentlichen Interesse oder erfolgt in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 lit. e)
	Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen nicht (Art. 6 Abs. 1 lit. f)

[14] Dies ist kein zwingender Bestandteil gemäß Art. 30 Abs. 1 DS-GVO, sondern soll beispielhaft zeigen, wie Anforderungen aus Art. 5 DS-GVO sinnvoll in das Verzeichnis integriert werden können. Die „Rechtschaffenheit“ bzw. die Legitimität der Verarbeitung muss entsprechend Art. 5 Abs. 1 DS-GVO (jederzeit) nachgewiesen werden können.

[15] Hinweis: siehe zum Thema „Einwilligung“ auch Working Paper 187 „Stellungnahme 15/2011 zur Definition von Einwilligung“ der Artikel-29-Datenschutzgruppe.

[16] Hinweis: in Working Paper 131 „Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“ der Artikel-29-Datenschutzgruppe wird hinsichtlich der „lebenswichtigen Interessen der betroffenen Person“ Stellung bezogen.

2.3.2 Verarbeitung besondere Kategorien personenbezogener Daten[17]

(Art. 9 DS-GVO)

	Rechtsgrundlage EU DS-GVO	Ergänzende national-gesetzliche Regelung
	Einwilligung[15] (Art. 9 Abs. 2 lit. a)	
	Patientenbehandlung[18] (Art. 9 Abs. 2 lit. h)	
	Weitergabe von Daten an Mit-/Nachbehandler[18] (Art. 9 Abs. 2 lit. h)	
	Verarbeitung ist zum Schutz lebenswichtiger Interessen[16] der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben Art. 9 Abs. 2 lit. c)	
	Abrechnung von Leistungen (Art. 9 Abs. 2 lit. f)	
	Qualitätssicherung der Patientenversorgung[18] (Art. 9 Abs. 2 Lit i)	
	Gesetzlich geregelte Krankheitsregister[18] (Art. 9. Abs. 2 lit. h)	
	Gesundheitsstatistik des Bundes und der Länder[18] (Art. 9 Abs. 2 lit. j in Verbindung mit Art. 89 Abs. 1)	
	Arbeitsmedizinische Untersuchung[18] (Art. 9 Abs. 2 Lit h in Verbindung mit Art. 9. Abs. 3)	
	Untersuchung durch Gesundheitsamt[18] (Art. 9. Abs. 2 Lit i)	
	Impfungen in Schule usw. durch Ämter[18] (Art. 9. Abs. 2 Lit i)	
	Verteidigung der behandelnden Person vor Gericht[18] (Art. 9 Abs. 2. lit. f)	
	Wissenschaftliche u. historische Forschung[18] (Art. 9 Abs. 2 lit. j in Verbindung mit Art. 89 Abs. 1)	
	Gesetzlich vorgeschriebene Archivierung zu hist. Zwecken[18] (Art. 9 Abs. 2 lit. j in Verbindung mit Art. 89 Abs. 1)	
	Verarbeitung von seitens der betroffenen Person öffentlich zugänglich gemachten Daten	

[17] Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ,Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

[18] Angabe einer nationalen gesetzlichen Regelung zwingend für die gelb markierten Feldern erforderlich, da ohne diese kein wirksamer Erlaubnistatbestand entsprechend DS-GVO vorliegt.

	Rechtsgrundlage EU DS-GVO	Ergänzende national-gesetzliche Regelung
	(Art. 9 Abs. 2 lit. e)	
	…	

2.4 Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

2.4.1 Beschreibung der Kategorien betroffener Personen[19]

Kategorien betroffener Personen	Beschreibung
Patienten	
Mitarbeiter, Angestellte, Rentner, Bewerber, Auszubildende, Praktikanten, gewerbliche Mitarbeiter	
Lieferanten sowie andere Geschäftspartner, sofern diese zur Erfüllung der in Abschnitt 2.2.2 genannten Zwecke erforderlich sind	
Kunden, Mitarbeiter von Kunden,	

2.4.2 Beschreibung der Kategorien personenbezogener Daten[19]

Kategorien personenbezogener Daten	Beschreibung
Daten der Patientenbehandlung, insbesondere – Anamnestische Daten – Diagnosedaten – Therapie- u. Versorgungsdaten – Nachsorgedaten	
Angaben zur Person (des Betroffenen) – Name – Anschrift – Geburtsdatum – Religion – schwerbehindert oder dem gleichgestellt	
Adressdaten	
Lieferantendaten	
Kundendaten	
Bestell- und Abrechnungsdaten	
Logistikdaten	
Mitarbeiterdaten zur Personalverwaltung, insbesondere: – Kostenstelle – Vorgesetzter – Schicht – Vollzeit/Teilzeit – Dauer Betriebszugehörigkeit	

[19] Hinweis: bzgl. der Personenbeziehbarkeit siehe auch Working Paper 136 „Stellungnahme 4/2007 zum Begriff ‚personenbezogene Daten' " der Artikel-29-Datenschutzgruppe

– Tätigkeiten im Unternehmen – Fehlzeiten	
Mitarbeiterdaten zur Lohn- und Gehaltsabrechnung, insbesondere: – Personalstammdaten – Zeiterfassungsdaten	
Bewerberdaten, insbesondere – Name – Anschrift – Kontaktdaten – Ausbildung – Qualifikation – Stelle, auf die sich beworben wurde	
...	

2.5 Kategorien von Empfängern[20]

2.5.1 Interne Empfänger

Empfänger	Rechtsgrundlage[21]

2.5.2 Externe Empfänger

Empfänger	Rechtsgrundlage[22]

2.6 Übermittlungen an ein Drittland oder an eine internationale Organisation[23]

Name des Drittstaates	
Empfänger oder Kategorien von Empfängern	
Art der Daten oder Datenkategorien	
Rechtsgrundlage	
Angabe der geeigneten Garantien[24]	

2.7 Fristen für die Löschung

Kategorien personenbezogener Daten	Löschfristen

[20] Hinweise (Art. 30 Abs. 1 lit. d):
1. Empfänger im Sinne der DS-GVO, also z. B. auch Auftragsverarbeiter
2. Es sind auch Empfänger anzugeben, denen die Daten zukünftig offengelegt werden (sollen)
3. Ebenfalls sind Empfänger in Drittländern anzugeben
4. Desgleichen internationale Organisationen als Empfänger

[21] Rechtsgrundlage für die Offenlegung, z.B. AV-Vertrag oder ein nationales Gesetz.
[22] Rechtsgrundlage für die Offenlegung, z.B. Auftragsverarbeitungs-Vertrag oder ein nationales Gesetz.
[23] Nur wenn im Einsatz oder geplant.
[24] Wenn Art. 49 Abs. 1 lit. b DS-GVO zutreffend ist.

2.8 Getroffene technische und organisatorische Maßnahmen[19][25]

(gemäß Art. 32 Abs. 1 DS-GVO)

2.8.1 Pseudonymisierung personenbezogener Daten[26]

Kategorien betroffener Daten	Verfahrensbeschreibung

2.8.2 Verschlüsselung personenbezogener Daten

Kategorien betroffener Daten	Verfahrensbeschreibung

2.8.3 Beschreibung des Verfahrens zur Gewährleistung der Verfügbarkeit der personenbezogenen Daten

Kategorien betroffener Daten	Verfahrensbeschreibung

2.8.4 Beschreibung des Verfahrens zur Gewährleistung Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall, rasch wiederherzustellen

Kategorien betroffener Daten	Verfahrensbeschreibung

2.8.5 Beschreibung des Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Kategorien betroffener Daten	Verfahrensbeschreibung

[25] Hier kann auf bestehende Dokumente wie bspw. ein IT-Sicherheitskonzept verwiesen werden, in welchem die die im Verfahren verwendeten Daten schützenden Maßnahmen konkret beschrieben sind

[26] Hinweis: bzgl. Abgrenzung Anonymisierung/Pseudonymisierung siehe auch Working Paper 216 „Stellungnahme 5/2014 zu Anonymisierungstechniken“ der Artikel-29-Datenschutzgruppe.

Abschnitt III: Verzeichnis von Verarbeitungstätigkeiten: (beim) Auftragsverarbeiter

1 Stammdaten

1.1 Namen und die Kontaktdaten des Auftragnehmers[27]

Name / Bezeichnung der datenverarbeitenden Stelle[28]	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[29]	
E-Mail-Adresse[29]	
Internet-Adresse[29]	

1.2 Nennung der verantwortlichen Personen beim Auftragnehmer

1.2.1 Geschäftsführung

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[29]	
E-Mail-Adresse[29]	
Internet-Adresse[29]	

1.2.2 Stellvertretende Geschäftsführung

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[29]	
E-Mail-Adresse[29]	
Internet-Adresse[29]	

[27] Hinweis: siehe hierzu auch Working Paper 169 „Stellungnahme 1/2010 zu den Begriffen ‚für die Verarbeitung Verantwortlicher' und ‚Auftragsverarbeiter' der Artikel-29-Datenschutzgruppe.
[28] Name des Unternehmens, der Institution, der Organisation, usw.
[29] Sofern vorhanden.

1.2.3 Leitung der Datenverarbeitung[30]

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[29]	
E-Mail-Adresse[29]	
Internet-Adresse[29]	

1.2.4 Angaben zur Person des Datenschutzbeauftragten[31]

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[29]	
E-Mail-Adresse[29]	
Internet-Adresse[29]	

[30] Freiwillige Angabe, jedoch ist es für eine Aufsichtsbehörde im Prüfungsfall nützlich zu wissen, wer hier der zuständige Ansprechpartner ist.
[31] Sofern vorhanden, ist die Angabe der Kontaktdaten des Datenschutzbeauftragter zwingend notwendig.

2 Angaben zur Verarbeitungstätigkeit

2.1 Angaben zum Verantwortlichen[32]

2.1.1 Namen und Kontaktdaten des Verantwortlichen[33]

Name / Bezeichnung der datenverarbeitenden Stelle[34]	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[35]	
E-Mail-Adresse[29]	
Internet-Adresse[29]	

2.1.2 Nennung der verantwortlichen Personen beim Verantwortlichen

2.1.2.1 Geschäftsführung

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[29]	
E-Mail-Adresse[29]	
Internet-Adresse[29]	

2.1.2.2 Stellvertretende Geschäftsführung

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[29]	
E-Mail-Adresse[29]	
Internet-Adresse[29]	

[32] Im Sinne des Auftraggebers: „in dessen Auftrag der Auftragsverarbeiter tätig ist“ (Art. 30 Abs. 2 lit. a DS-GVO)
[33] Hinweis: siehe hierzu auch Working Paper 169 „Stellungnahme 1/2010 zu den Begriffen ‚für die Verarbeitung Verantwortlicher‘ und ‚Auftragsverarbeiter‘ der Artikel-29-Datenschutzgruppe
[34] Name des Unternehmens, der Institution, der Organisation, …
[35] Sofern vorhanden

2.1.2.3 Angaben zur Person des Datenschutzbeauftragten[36]

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[29]	
E-Mail-Adresse[29]	
Internet-Adresse[29]	

2.2 Organisatorische Angaben

2.2.1 Verantwortliche Person beim Auftragnehmer

Vollständiger Name (n)	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax[5]	
E-Mail-Adresse[5]	
Internet-Adresse[5]	

2.2.2 Zeitangaben

Datum der Einführung	
Datum der Erstbeschreibung	
Datum der letzten Änderung	

2.3 Arten der Verarbeitungen

Arten	Beschreibung

2.4 Übermittlungen an ein Drittland oder an eine internationale Organisation[37]

Name des Drittstaates	
Empfänger oder Kategorien von Empfängern	
Art der Daten oder Datenkategorien	
Rechtsgrundlage	

[36] Sofern vorhanden Angabe Kontaktdaten Datenschutzbeauftragter zwingend notwendig
[37] Nur wenn im Einsatz oder geplant

Angabe der geeigneten Garantien[38]	

2.5 Getroffene technische und organisatorische Maßnahmen[39]

(gemäß Art. 32 Abs. 1 DS-GVO)

2.5.1 Pseudonymisierung personenbezogener Daten

Kategorien betroffener Daten	Verfahrensbeschreibung

2.5.2 Verschlüsselung personenbezogener Daten

Kategorien betroffener Daten	Verfahrensbeschreibung

2.5.3 Beschreibung des Verfahrens zur Gewährleistung der Verfügbarkeit der personenbezogenen Daten

Kategorien betroffener Daten	Verfahrensbeschreibung

2.5.4 Beschreibung des Verfahrens zur Gewährleistung Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Kategorien betroffener Daten	Verfahrensbeschreibung

2.5.5 Beschreibung des n Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Kategorien betroffener Daten	Verfahrensbeschreibung

[38] Wenn Art. 49 Abs. 1 lit. b DS-GVO zutreffend ist.

[39] Hinweis: bzgl. der Personenbeziehbarkeit siehe auch Working Paper 136 „Stellungnahme 4/2007 zum Begriff ‚personenbezogene Daten' " der Artikel-29-Datenschutzgruppe.