Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ( Art. 25 DS-GVO)

Eine Zusammenarbeit von



Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz & IT-Sicherheit



Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“



Gesellschaft für Datenschutz und Datensicherheit e. V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

**Autor(en)**

|  |  |
| --- | --- |
| Isele, Christoph | Cerner Health Services Deutschland GmbH |
| Kaufmann, Pierre | Kaufmann  |
| Koeppe, David | Vivantes - Netzwerk für Gesundheit GmbH |
| Neumann, Conrad | medatixx GmbH & Co. KG |
| Schütz, Thorsten | Klinikum Itzehoe |
| Schütze, Dr. Bernd | Deutsche Telekom Healthcare and Security GmbH |
| Spyra, Gerald | Ratajczak und Partner mbB Rechtsanwälte |

Version 1.0
Stand: 28.04.2018

# Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

# 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

# Inhaltsverzeichnis

[Zusammenfassung 2](#_Toc514832474)

[1 Einführung 3](#_Toc514832475)

[1.1 Entwicklungsgeschichte der Regelung 3](#_Toc514832476)

[1.2 Intention des europäischen Gesetzgebers 3](#_Toc514832477)

[2 Erläuterungen zum rechtlichen Hintergrund 4](#_Toc514832478)

[2.1 An wen wendet sich die Norm? („Normadressat“) 4](#_Toc514832479)

[2.2 Inhalte der Pflicht 4](#_Toc514832480)

[2.2.1 Geeignetheit der Maßnahmen 5](#_Toc514832481)

[2.2.2 Zeitpunkt 5](#_Toc514832482)

[2.2.3 Abwägungskriterien 6](#_Toc514832483)

[2.2.3.1 Art, Umfang, Umstände und Zwecke der Verarbeitung, Eintrittswahrscheinlichkeit und Schwere der Risiken 6](#_Toc514832484)

[2.2.3.2 Stand der Technik 8](#_Toc514832485)

[2.2.3.3 Implementierungskosten 9](#_Toc514832486)

[2.2.4 Umsetzung der Datenschutzgrundsätze 9](#_Toc514832487)

[2.3 Weitergehende Anforderungen 10](#_Toc514832488)

[2.3.1 Garantien des Verantwortlichen: Gewährleistung Betroffenenrechte und Datenschutzkonzept 10](#_Toc514832489)

[2.3.2 Voreinstellung 10](#_Toc514832490)

[2.3.3 Genehmigte Zertifizierungsverfahren 11](#_Toc514832491)

[2.3.4 Verhaltensregeln gem. Art. 40 DS-GVO 11](#_Toc514832492)

[2.3.5 Binding Corporate Rules 11](#_Toc514832493)

[2.3.6 Berücksichtigung bei öffentlichen Ausschreibungen 11](#_Toc514832494)

[2.4 Sanktionierung 11](#_Toc514832495)

[3 Privacy by Design: Eine mögliche Vorgehensweise 14](#_Toc514832496)

[4 Rechenschaftspflicht und Dokumentation 14](#_Toc514832497)

[4.1 Was mindestens dokumentiert werden sollte 14](#_Toc514832498)

[4.2 Welche Fragen muss die Dokumentation mindestens beantworten? 17](#_Toc514832499)

[4.3 Was wird wo dokumentiert? 19](#_Toc514832500)

[5 Checkliste 20](#_Toc514832501)

[5.1 Datenschutz durch Technikgestaltung (Privacy by Design) 20](#_Toc514832502)

[5.2 Datenschutz durch datenschutzfreundliche Voreinstellungen (Privacy by Default) 20](#_Toc514832503)

[6 Abkürzungen 21](#_Toc514832504)

[7 Literatur 22](#_Toc514832505)

[7.1 Fachzeitschriften 22](#_Toc514832506)

[7.2 Internet 22](#_Toc514832507)

[7.3 Bücher 24](#_Toc514832508)

# Zusammenfassung

Privacy by Design/by Default betrifft sowohl technische als auch organisatorische Komponenten, also Anforderungen an IT-Systeme als auch Organisationsabläufe. Die Anforderungen müssen sowohl bei der Planung als auch bei der Durchführung einer Verarbeitung berücksichtigt werden. Da der Begriff der „Verarbeitung“ in Art. 4 Ziff. 2 DS-GVO sehr weit gefasst ist, müssen die Maßnahmen für den gesamten Lebenszyklus der Daten gewährleistet werden. Da sich im zeitlichen Verlauf die Anforderungen bzgl. der Geeignetheit der Maßnahmen ändern können, handelt es sich bei Privacy by Design/Default nicht um einen einmaligen Vorgang, sondern vielmehr um einen fortlaufenden Prozess.

Dabei werden zwei Aspekte adressiert. Einerseits muss der Verantwortliche sowohl bei der Planung, also zum Zeitpunkt der Festlegung der Zwecke und Mittel der Verarbeitung, als auch zum „Zeitpunkt der eigentlichen Verarbeitung“ geeignete Maßnahmen ergreifen („Datenschutz durch Technikgestaltung“). Andererseits ist die Verarbeitung mit „datenschutzfreundliche Voreinstellungen“ durchzuführen.

Dabei müssen die getroffenen technischen und organisatorischen Maßnahmen geeignet sein,

* die Datenschutzgrundsätze wirksam umzusetzen und
* die notwendigen Garantien bieten, um den Anforderungen dieser Verordnung zu genügen und
* die Rechte der betroffenen Personen schützen.

Dabei kann eine betriebswirtschaftliche Abwägung zwischen verschiedenen gleichermaßen geeigneten Maßnahmen bzgl. der Implementierungskosten erfolgen, nicht jedoch der Durchführungs- oder Folgekosten.

Weiterhin ist der „Stand der Technik“ zu berücksichtigen, was im Kontext dieses Themas wohl bedeutet, dass die von Ann Cavoukian aufgestellten „The 7 Foundational Principles“ berücksichtigt werden müssen.

Auch für die Anforderungen von Art. 25 DS-GVO, also den Anforderungen bzgl. Privacy by Design und Privacy by Default, bestehen für den Verantwortlichen Nachweispflichten. Daher muss der Verantwortliche bei der Dokumentation der Verarbeitung stets auch die aus Art. 25 DS-GVO resultierenden Anforderungen adressieren und deren Erfüllung darstellen.

# Einführung

Der Begriff „Privacy by Design“ oder deutsch „Datenschutz durch Technikgestaltung“ wurde zum ersten Mal von Ann Cavoukian verwendet[[1]](#footnote-1). Danach stellt Privacy by Design ein Konzept dar, welches auf IT-Systeme, Geschäftspraktiken, physikalisches Design und auch auf Netzwerkarchitekturen anwendbar ist. Die Zielsetzung von Privacy by Design ist – wie es der Name schon ausdrückt - die ganzheitliche Gewährleistung von Datenschutz und die persönliche Kontrolle über die eigenen Daten. Um dies zu erreichen, muss eine Berücksichtigung von Datenschutzaspekten schon während der Designphase erfolgen, denn hinterher kann man nur Vorhandenes anpassen, was i.d.R. nicht so erfolgreich bzw. deutlich aufwändiger umzusetzen ist, als wenn man es von Anfang an berücksichtigt.

Art. 25 DS-GVO adressiert die für die Verarbeitung der Daten Verantwortlichen, nicht jedoch die Hersteller bzw. Anbieter von Systemen bzw. Lösungen (außer sie sind selbst die Verantwortlichen für die Datenverarbeitung). Jedoch heißt es in ErwGr. 78 DS-GVO: „sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Auslegung der Produkte, Dienste und Anwendungen zu berücksichtigen“. Demnach muss der Verantwortliche in Ausschreibungen, bei Anschaffungen usw. Privacy by Design als auch Privacy by Default vom Anbieter/Hersteller einfordern.

## Entwicklungsgeschichte der Regelung

Bereits Art. 17 Abs. 1 RL 95/46/EG[[2]](#footnote-2) verlangte, dass „geeignete technische und organisatorische Maßnahmen“ ergriffen werden müssen, „die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang […] und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten“ erforderlich sind. Diese Regelung richtete sich in erster Linie an die Sicherheit der Daten[[3]](#footnote-3).

Art. 25 DS-GVO geht über diese Zielsetzung hinaus: Nunmehr muss der Verantwortliche die in Art. 5 DS-GVO beschriebenen Datenschutzgrundsätze schon in der Planungsphase berücksichtigen und technische und organisatorische Maßnahmen vorsehen (by Design), umsetzen (by Default) und deren Einhaltung gewährleisten.

## Intention des europäischen Gesetzgebers

Sinn und Zweck der in Art. 25 DS-GVO enthaltenen Regelung ist, den Datenschutz zu einem frühestmöglichen Zeitpunkt zu berücksichtigen und über den gesamten Lebenszyklus der Verarbeitung personenbezogener Daten zu gewährleisten.

# Erläuterungen zum rechtlichen Hintergrund

## An wen wendet sich die Norm? („Normadressat“)

Der europäische Gesetzgeber verpflichtet mit Art. 25 DS-GVO ausschließlich die oder den Verantwortlichen zur Beachtung und Einhaltung der Pflichten von Art. 25 DS-GVO; Hersteller von Produkten, Diensten und Anwendungen sind grundsätzlich nicht den Pflichten unterworfen. Gemäß ErwGr. 78 sollen Hersteller, wenn sie keine Verantwortlichen sind, vom Verantwortlichen „ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Diensten und Anwendungen zu berücksichtigen“. Der Grundgedanke bei der Regelung von Art. 25 DS-GVO geht dahin, dass die Pflichten des Verantwortlichen ihn zur Nachfrage nach entsprechenden Produkte, Diensten und Anwendungen Hersteller zu entsprechendem Handeln zwingen. Mithin soll auf die Hersteller ein mittelbarer Marktdruck entstehen, nur noch datenschutzfreundliche Produkte anzubieten.

Da sich Art. 25 DS-GVO nur an Verantwortliche richtet, werden auch Auftragsverarbeiter nicht direkt von dieser Regelung adressiert. Jedoch darf entsprechend Art. 28 Abs. 1 DS-GVO der Verantwortliche nur solche Auftragsverarbeiter beauftragen, die auch Art. 25 DS-GVO erfüllen: „[…] so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt […]“.Mithin muss ein Verantwortlicher zur Gewährleistung der gesetzlichen Anforderungen von einem Auftragsverarbeiter verlangen, dass er „Privacy by Design“ als auch „Privacy by Default“ bei sich im erforderlichen Maße umgesetzt hat, damit „seine“ Daten ausreichend geschützt sind. Denn es darf niemals zu einer Verschlechterung des Schutzniveaus in der Lieferkette kommen.

## Inhalte der Pflicht

Die Inhalte der aus Art. 25 DS-GVO resultierenden Pflichten bestehen insbesondere im Treffen geeigneter technisch-organisatorische Maßnahmen ( Art. 25 Abs. 2)

* zur **Umsetzung der Datenschutzgrundsätze** ( Art. 5 DS-GVO)
* zur **Durchsetzung der Betroffenenrechte** (Kap. 3, Artt. 12-22 DS-GVO)

unter Berücksichtigung ( Art. 25 Abs. 1)

* des Stands der Technik
* der Implementierungskosten
* der Art, Umfang, Umstände und Zwecke
* der Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

Dabei kann ein genehmigtes Zertifizierungsverfahren gemäß Art. 42 DS-GVO die Möglichkeit bieten, diese Anforderungen nachzuweisen.

Weiterhin heißt es in Art. 25 Abs. 1 DS-GVO: „[…] trifft der Verantwortliche sowohl

* zum **Zeitpunkt der Festlegung der Mittel** für die Verarbeitung als auch
* zum **Zeitpunkt der eigentlichen Verarbeitung**

geeignete technische und organisatorische Maßnahmen [...], die dafür ausgelegt sind,

* die Datenschutzgrundsätze *(siehe Art. 5 DS-GVO[[4]](#footnote-4))* [...] wirksam umzusetzen und
* die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und
* die Rechte der betroffenen Personen zu schützen.“

Dementsprechend müssen die Prinzipien „Privacy by Design“ und „Privacy by Default“ sowohl bei der Planung als auch bei der Durchführung der Verarbeitung berücksichtigt werden. Dabei enthält Art. 25 DS-GVO im Gegensatz zu Art. 32 DS-GVO keine Beschränkung bzgl. „Angemessenheit“ der Maßnahmen; die Maßnahmen müssen „geeignet“ sein, um den Ansprüchen der Regelungen von Art. 25 DS-GVO zu genügen. D. h. wird diesen Anforderungen nicht genügt, darf die Verarbeitung nicht durchgeführt werden.

Entsprechend des Gesetzeswortlauts sind die Forderungen des europäischen Gesetzgebers bzgl. Technikgestaltung und datenschutzfreundliche Voreinstellungen aber nicht absolut. So beinhaltet Art. 25 Abs. 1 einige Abwägungsfaktoren, die bei der Implementierung zu berücksichtigen sind und die „Spielraum“ für Argumentationen eröffnen.

### Geeignetheit der Maßnahmen

Es müssen immer **geeignete** technische und organisatorische Maßnahmen getroffen werden, welche

* die Datenschutzgrundsätze wirksam umzusetzen und
* die notwendigen Garantien bieten, um den Anforderungen dieser Verordnung zu genügen und
* die Rechte der betroffenen Personen schützen.

Unabhängig von allen anderen Abwägungen **müssen** die technischen und organisatorischen Maßnahmen daher immer diesen drei Bedingungen genügen, ansonsten darf die Verarbeitung nicht durchgeführt werden.

### Zeitpunkt

Die Maßnahmen sind entsprechend Art. 25 Abs. 1 DS-GVO bereits zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung zu treffen. Somit sind die zu treffenden Datenschutzmaßnahmen bereits in der Planungsphase zu berücksichtigen.

Darüber hinaus gelten die Pflichten bzgl. Privacy By Design / by Default jedoch immer auch für den Zeitpunkt der Verarbeitung. Da der Begriff der „Verarbeitung“ in Art. 4 Ziff. 2 DS-GVO sehr weit gefasst ist, müssen die zur Gewährleistung dieser Prinzipien erforderlichen Maßnahmen für den gesamten Lebenszyklus der Daten gewährleistet werden.

Da sich im zeitlichen Verlauf die Anforderungen bzgl. der Geeignetheit der Maßnahmen (z. B. hinsichtlich der eingesetzten kryptographischen Methoden) ändern können, handelt es sich bei Privcy by Design/Default nicht um einen einmaligen Vorgang[[5]](#footnote-5), sondern vielmehr um einen andauernden PDCA-Prozess[[6]](#footnote-6), der einer regelmäßigen Sichtung und ggf. Anpassung der Maßnahmen erfordert.

### Abwägungskriterien

#### Art, Umfang, Umstände und Zwecke der Verarbeitung, Eintrittswahrscheinlichkeit und Schwere der Risiken

Art. 25 DS-GVO adressiert nicht nur riskante Verarbeitungen, wie andere Regelungen der DS-GVO, sondern alle Verarbeitungen und alle Risiken, die mit einer Datenverarbeitung einhergehen.

Damit die zu ergreifenden Maßnahmen „geeignet“ sind, müssen entsprechend Art. 25 Abs. 1DS-GVO einerseits Art, Umfang, Umstände und Zwecke der Verarbeitung berücksichtigt werden. Andererseits anderen gilt es bei der Auswahl der Maßnahmen auch die Eintrittswahrscheinlichkeit und die Schwere der Risiken einfließen zu lassen. Dabei handelt es sich hierbei um unbestimmte Rechtsbegriffe, die maßgeblichen Kriterien werden im Nachfolgenden näher erläutert.

##### Art und Umfang, der Verarbeitung

Je mehr Daten verarbeitet werden und um so schützenswerter/sensibler die Art der Daten sind, desto wirksamer müssen die Maßnahmen zum Schutz dieser Daten sein. Der Hinweis bzgl. Sensitivität der Daten gilt natürlich insbesondere für die in Art. 9 Abs. 1 DS-GVO genannten besonderen Arten/Kategorien personenbezogener Daten; bei diesen Datenarten ist der Schutzbedarf sicherlich mit am größten.

Aus ErwGr. 75 bzw. 91 DS-GVO wird ersichtlich, dass im Bereich des „Umfangs der Datenverarbeitung“ als Einflussgrößen einerseits die Anzahl der betroffenen Personen zu berücksichtigen ist, andererseits die Menge der verarbeiteten Daten selbst. Hier gilt:

1. Je mehr Daten zu einer Person vorhanden sind, desto weitreichendere Aussagen sind über diese Person möglich und desto größer ist das Risiko für diese Person.
2. Je höher die Anzahl der von der Verarbeitung betroffenen Personen ist, desto mehr und desto bessere/genauere Aussagen sind über diese Personengruppe, aber ggf. auch über Einzelpersonen möglich. Z. B. könnten etwaige Verbindungen zwischen diesen Personen hergestellt werden, woraus ggf. wiederum weitere Schlüsse über die betroffene Person gezogen werden könnten. Daraus leiten sich wiederum höhere Risiken hinsichtlich der informationellen Selbstbestimmung für die betroffenen Personen ab.

Zugleich erhöht sich mit einem größeren Verarbeitungsumfang auch die Eintrittswahrscheinlichkeit etwaiger Risiken[[7]](#footnote-7).

##### Zwecke der Verarbeitung

Entsprechend Art. 25 Abs. 1 DS-GVO müssen die Zwecke der Verarbeitung berücksichtigt werden. Die Norm DIN CEN ISO/TS 14265 „Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen“ bietet Anhaltspunkte, wie der Zweck / bzw. die Zwecke der Verarbeitung entsprechend dem, Stand der Technik klassifiziert werden können[[8]](#footnote-8).

Grundsätzlich gibt die DS-GVO nicht vor, wie detailliert der Verarbeitungszweck dargestellt werden muss. Art. 5 Abs. 1 lit. b DS-GVO gibt vor, dass personenbezogene Daten nur zu festgelegten, eindeutigen und legitimen Zwecken verarbeitet werden dürfen. D. h., der Verarbeitungszweck muss derart umfassend beschrieben werden, dass die Zwecke eindeutig erkennbar sind und somit keine Deutungsmöglichkeiten bzgl. des beabsichtigten Verarbeitungszweckes bestehen.

Auch aus Artt. 13 und 14 DS-GVO ist zu ersehen, dass der Verarbeitungszweck bzw. die Zwecke derart genau beschrieben sein müssen, damit daraus die betroffenen Personen erkennen können, wie und wozu der Verantwortliche die sie betreffenden Daten verarbeiten will bzw. verarbeitet.

Der Verantwortliche muss die Notwendigkeit der von ihm verwendeten Daten zur Erreichung des Verarbeitungszweckes nachweisen. Das gleiche gilt für die Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck. Ein solcher Nachweis ist jedoch nur möglich, wenn der Zweck hinreichend genau dargestellt ist.

Somit liegt die Detailliertheit der Zweckangabe beim Verantwortlichen, dem die schwierige Aufgabe zukommt, einerseits den Zweck hinreichend konkret anzugeben, andererseits den Grad der Detailliertheit aber nicht so tief zu setzen, dass die daraus resultierenden administrativen Aufgaben nicht mehr zu bewältigen sind.

##### Risiken der Verarbeitung

Die DS-GVO definiert nicht den Begriff „Risiko“, sondern umschreibt ihn vielmehr. So ist gem. ErwGr. 75 DS-GVO darunter die Einschätzung zu verstehen, ob eine Verarbeitung personenbezogener Daten „zu einem physischen, materiellen oder immateriellen Schaden“ bei der von der Verarbeitung betroffenen Person führen kann, wobei diese Betrachtung die „unterschiedliche Eintrittswahrscheinlichkeit und Schwere“ berücksichtigen muss. Die Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen ist bzgl. der von Art. 25 Abs. 1 DS-GVO geforderten zu treffenden Schutzmaßnahmen somit in Abhängigkeit der beiden Größen „Eintrittswahrscheinlichkeit“ und „Schadensschwere“ darzustellen[[9]](#footnote-9): ein „hohes“ Risiko erfordert umfangreichere und wirksamere Schutzmaßnahmen als ein „normales“ (im Sinne des „Lebensrisikos“[[10]](#footnote-10)) Risiko.

Gemäß ErwGr. 76 DS-GVO soll die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person „in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung“ bestimmt werden.“ Weiterhin soll das Risiko anhand einer objektiven Bewertung beurteilt werden. Dabei gibt die DS-GVO jedoch nicht vor, wann das Risiko einer Verarbeitung „hoch“ ist.

Ein Risiko ist zumindest immer dann als „hoch“ einzustufen, wenn mit „hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten natürlicher Personen“ anzunehmen ist.[[11]](#footnote-11) Eine hohe Schadenswahrscheinlichkeit kann sowohl aus einer hohen Eintrittswahrscheinlichkeit als auch aus einem hohen Schaden resultieren. Weiterhin ergibt sich aus ErwGr. 91 DS-GVO, dass insbesondere auch die Sensibilität der zu verarbeitenden Daten die Wahrscheinlichkeit eines „hohen“ Risikos vermuten lässt.

Laut ErwGr. 75 DS-GVO ist von „hohen“ Risiken für die Rechte und Freiheiten natürlicher Personen insbesondere dann auszugehen ist, wenn die Verarbeitung zu

* einer Diskriminierung,
* einem Identitätsdiebstahl oder -betrug,
* einem finanziellen Verlust,
* einer Rufschädigung,
* einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
* der unbefugten Aufhebung der Pseudonymisierung

oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann. Desgleichen, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren. Insbesondere wenn personenbezogene Daten verarbeitet werden, die zu den besonderen Kategorien von Daten gemäß Art. 9 DS-GVO gehören, muss von hohen Risiken ausgegangen werden.

#### Stand der Technik

Der in Art. 25 DS-GVO geforderte „Stand der Technik“ beinhaltet u.a. die Anforderung, fortschrittliche Verfahren, Einrichtungen oder Betriebsweisen mit praktischer Eignung bzgl. Maßnahmen zum Schutz der Funktionsfähigkeit (i.S.v. Art. 25 DS-GVO der Schutz der Rechte und Freiheiten natürlicher Personen) einzusetzen. Die konkreten Anforderungen an den Stand der Technik bzgl. Privacy by Design lassen sich aus den von Ann Cavoukian aufgestellten „The 7 Foundational Principles“ ableiten, die da sind[[12]](#footnote-12):

1. Proactive not Reactive; Preventative not Remedial

Der Privacy by Design Ansatz ist von proaktiven, nicht von reaktiven Maßnahmen geprägt, Privacy by Design soll Datenschutzverletzungen verhindern. Jedoch bietet Privacy by Design keine Abhilfe, wenn Datenschutzverletzungen eingetreten sind.

1. Privacy as the Default Setting

Datenschutz als Standardeinstellung soll den bestmöglichen Schutz der Privatsphäre gewährleisten. Die Zielsetzung dabei ist, dass die von der Verarbeitung betroffenen Personen nichts für den Schutz leisten müssen, denn der Schutz ist systemimmanent als Standardeinstellung vorhanden. Jedoch muss die betroffene Person stets die Möglichkeit haben, das Schutzniveau (freiwillig) zu verringern.

1. Privacy Embedded into Design

Privacy by Design ist in das Design und die Architektur von IT-Systemen und Geschäftspraktiken eingebettet. D. h. Datenschutz ist ein wesentlicher Bestandteil des Systems, ohne Abstriche bei der Funktionalität.

1. Full Functionality — Positive-Sum, not Zero-Sum

Privacy by Design bietet volle Funktionalität, es stellt eine Positivsumme dar, keine Nullsumme. D. h. Privacy by Design kommt allen berechtigten Interessen und Zielen entgegen, sowohl denen von Verarbeitern der Daten als auch denen der betroffenen Personen. Datenschutz stellt damit einen konstruktiven Begleitansatz und keine Verhinderung der Verarbeitung dar.

1. End-to-End Security — Full Lifecycle Protection

Privacy by Design bietet eine durchgängige Sicherheit, d. h. einen Schutz während des gesamten Lebenszyklus der Daten. Von der Ersterfassung bis zum Löschen der Daten wird Privacy by Design umgesetzt.

1. Visibility and Transparency — Keep it Open

Privacy by Design bietet allen Beteiligten eine Sichtbarkeit und Transparenz bzgl. der Verarbeitung der Daten. D. h. einzelne Komponenten und Verfahren bleiben sichtbar und transparent; gleichermaßen für Nutzer und Anbieter.

1. Respect for User Privacy — Keep it User-Centric

Es wird eine nutzerzentrierte Gestaltung gewährleistet. Die Wahrung der Privatsphäre der Nutzer ist jederzeit gesichert. Grundsätzlich stehen die Interessen der von der Verarbeitung betroffenen Personen an erster Stelle.

#### Implementierungskosten

Art. 25 Abs. 1 DS-GVO erlaubt eine betriebswirtschaftliche Abwägung und Maßnahmenbewertung hinsichtlich der Implementierungskosten. D. h. es müssen nicht beliebige Kosten zur Ergreifung geeigneter technischer und organisatorischer Maßnahmen aufgewendet werden. Vielmehr müssen die Kosten immer im Verhältnis zum Schutzziel stehen. Daher steht es dem Verantwortlichen grundsätzlich frei, bei einer Auswahl verschiedener Maßnahmen diejenigen zu ergreifen, die ihm aus betriebswirtschaftlicher Sicht am genehmsten ist. Das Korrektiv bildet dabei jedoch die „Geeignetheit“ der Maßnahme. Erfüllt die Maßnahme nicht die in Abschnitt 2.2.1 genannten Kriterien, ist sie nicht geeignet.

Daraus folgt, dass, wenn aus Sicht des Verantwortlichen keine Maßnahme existiert, die einerseits finanzierbare Implementierungskosten beinhaltet und anderseits die Geeignetheit abbildet, die Verarbeitung der Daten nicht erfolgen darf.

Die Abwägung bezieht sich aber ausdrücklich nur auf die Implementierungskosten[[13]](#footnote-13). Die für die Durchführung der Maßnahme anfallenden Kosten finden keine Berücksichtigung. Dies ist auch ein bewusster Akt des europäischen Gesetzgebers. In Art. 17 Abs. 2 RL 95/46/EG hieß es noch bei „bei ihrer Durchführung entstehenden Kosten“, jedoch wurde dies in der DS-GVO auf Implementierungskosten geändert.

### Umsetzung der Datenschutzgrundsätze

 Art. 5 DS-GVO benennt die Datenschutzgrundsätze für die Verarbeitung personenbezogener Daten:

* Rechtmäßige Verarbeitung ( Art. 5 Abs. 1 lit. a DS-GVO)
* Verarbeitung nach Treu und Glauben ( Art. 5 Abs. 1 lit. a DS-GVO)
* Transparente Verarbeitung für die betroffenen Personen ( Art. 5 Abs. 1 lit. a DS-GVO)
* Beachtung der Zweckbindung ( Art. 5 Abs. 1 lit. b DS-GVO)
* Datenminimierung ( Art. 5 Abs. 1 lit. c DS-GVO)
* Gewährleistung der Richtigkeit der Daten ( Art. 5 Abs. 1 lit. d DS-GVO)
* Begrenzung der Speicherdauer ( Art. 5 Abs. 1 lit. e DS-GVO)
* Sicherstellung von Integrität und Vertraulichkeit ( Art. 5 Abs. 1 lit. f DS-GVO)
* Erfüllung der Rechenschaftspflicht bzgl. der Umsetzung der Anforderungen der Datenschutz-Grundverordnung ( Art. 5 Abs. 2 DS-GVO).

Um der Nachweispflicht zu genügen, muss in der Dokumentation zu der Entscheidungsfindung wie auch zu den Maßnahmen selbst beschrieben werden, wie die Maßnahmen die Umsetzung der Datenschutzgrundsätze gewährleisten.

## Weitergehende Anforderungen

### Garantien des Verantwortlichen: Gewährleistung Betroffenenrechte und Datenschutzkonzept

Entsprechend Art. 25 Abs. 1 DS-GVO sind Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. D. h. der Verantwortliche muss die technischen und organisatorischen Maßnahmen so gestalten, dass diese entsprechende Garantien enthalten.

Bzgl. Betroffenenrechte sind Prozesse vorzusehen, welche die Betroffenenrechte proaktiv gewährleisten[[14]](#footnote-14). D. h. es darf nicht erst dann reagiert werden, wenn eine betroffene Person eines oder mehrere ihrer Rechte wahrnimmt, sondern es müssen bei der Konzeption eines Produktes, einer Dienstleistung oder Anwendung entsprechende Prozesse berücksichtigt und implementiert werden.

Die Forderung, Garantien zur Wahrung der Anforderungen der DS-GVO zu berücksichtigen, ist sehr weit gefasst. In ErwGr. 78 DS-GVO findet sich die Forderung, der Verantwortliche soll interne Strategien festlegen. Diese Strategien sollten in einem **Datenschutzkonzept** festgehalten und regelmäßig überprüft und ggf. angepasst werden, damit das Datenschutzkonzept Garantien bietet, wie der Verantwortliche seiner Pflicht genügt. Hierbei sollte das Datenschutzkonzept

* Risikoanalyse
* Auswahl, Festlegung und Umsetzung konkreter technischer und organisatorischer Maßnahmen

beinhalten14.

### Voreinstellung

 Art. 25 Abs. 2 DS-GVO verlangt, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen trifft, die sicherstellen, dass durch Voreinstellung grundsätzlich nur die personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Diese Pflicht gilt für

* die Menge der erhobenen personenbezogenen Daten,
* den Umfang ihrer Verarbeitung,
* ihre Speicherfrist und
* ihre Zugänglichkeit.

Dabei bedingt das Kriterium der „Erforderlichkeit“, dass es kein milderes (= in die Rechte Betroffener weniger eingreifendes) Mittel gibt, welches den gleichen Erfolg mit vergleichbarem Aufwand erzielt. Um die Erforderlichkeit / Notwendigkeit beurteilen zu können, müssen daher drei Fragen beantwortet werden:

1. Gibt es ein anderes Mittel?
2. Ist dieses in gleicher Weise geeignet, den Zweck zu erreichen?
3. Ist dieses Mittel ein milderes, also die Rechte Anderer weniger belastendes Mittel?

Bzgl. der in Art. 5 DS-GVO verankerten Rechenschaftspflicht ist festzuhalten, dass auch die Erforderlichkeit nachgewiesen werden muss. D. h. diese Fragen müssen in der Dokumentation adressiert und beantwortet werden.

### Genehmigte Zertifizierungsverfahren

Entsprechend den Vorgaben von Art. 25 Abs. 3 DS-GVO kann ein genehmigtes Zertifizierungsverfahren[[15]](#footnote-15) als Faktor herangezogen werden, um die Erfüllung der Anforderungen von Art. 25 Abs. 1,2 DS-GVO nachzuweisen. Dabei hängt die dem Zertifizierungsverfahren innewohnende Nachweiskraft stark von der Art und dem Umfang des Verfahrens ab.

### Verhaltensregeln gem. Art. 40 DS-GVO

Verhaltensregeln („Code of Conduct“), die Verbände und andere Vereinigungen aufstellen dürfen, können entsprechend Art. 40 Abs. 2 lit. h DS-GVO branchenspezifisch die unspezifischen Anforderungen von Art. 25 konkretisieren, so dass der gesetzlich geforderte Nachweis der Einhaltung der Anforderungen vom jeweiligen Verantwortlichen leichter geführt werden kann.

### Binding Corporate Rules

Verbindliche interne Datenschutzvorschriften („Binding Corporate Rules“) müssen entsprechend Art. 47 Abs. 2 lit. d DS-GVO auch Angaben dazu enthalten, wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen berücksichtigt und eingehalten werden.

### Berücksichtigung bei öffentlichen Ausschreibungen

Entsprechend ErwGr. 78 DS-GVO soll den „Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen auch bei öffentlichen Ausschreibungen Rechnung getragen werden“. Demgemäß sind die Vorgaben von Art. 25 DS-GVO bei öffentlichen Ausschreibungen ein wichtiges Kriterium[[16]](#footnote-16). D.h. öffentliche Ausschreibungen sollten künftig datenschutzsparsame Techniken in Ausschreibungen fordern.

## Sanktionierung

Werden die Vorgaben aus Art. 25 DS-GVO von einem Verantwortlichen nicht eingehalten, so findet das „kleinere“ Bußgeld (von bis zu 10.000.000 Euro bzw. 2 % des weltweit erzielten Umsatzes, s.o.) Anwendung.

Bei der Verhängung des Bußgeldes sind auch die Vorgaben von Art. 83 Abs. 2 lit. a-k DS-GVO zu berücksichtigen, insbesondere sind hierbei zu beachten:

| Inhalt Art. 83 (2) DS-GVO | Hinweise zur Interpretation |
| --- | --- |
| Art, Schwere und Dauer des Verstoßes(Art. 83 Abs. 2 lit. a) | Hierzu ist z. B. zu betrachten:* Liegt ein genereller Verstoß vor, d. h. man kann generell der gesetzlichen Pflicht nicht genügen?
* Sind es nur die konkreten Umstände des Einzelfalles, die ein Genügen der gesetzlichen Pflicht verhindern?
* Wie groß ist der potentielle Schaden für jeden einzelnen Betroffenen? Wie groß ist der Schaden insgesamt?
 |
| Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes(Art. 83 Abs. 2 lit. b) | Hierzu ist z. B. zu betrachten:* Wurde die gesetzliche Pflicht vom Verantwortlichen im Ablauf seiner Prozesse ignoriert?
* Wurde fahrlässig einem einzelnen Betroffenen sein Recht verweigert?
 |
| Maßnahmen zur Minderung des Schadens für betroffene Personen(Art. 83 Abs. 2 lit. c) | * Wenn die Zugriffsrechte auf die Daten nicht hinreichend eingeschränkt werden, kann durch Dienstanweisungen das freie Surfen verboten werden.
 |
| Grad der Verantwortung Verantwortlicher/ Auftragsverarbeiter(Art. 83 Abs. 2 lit. d) | Hierzu ist z. B. zu betrachten:* Bemühen des Verantwortlichen bzw. Auftragsverarbeiters, betroffenen Personen einen entstandenen (materiellen oder auch immateriellen) Schaden möglichst gering zu halten (bzw. auszugleichen)?
 |
| Etwaige einschlägige frühere Verstöße(Art. 83 Abs. 2 lit. e) | Handelt es sich um einen Wiederholungstatbestand? |
| Umfang der Zusammenarbeit mit der Aufsichtsbehörde(Art. 83 Abs. 2 lit. f) | Hierzu ist z. B. zu betrachten:* Wurden der Aufsichtsbehörde unverzüglich alle benötigten Informationen gegeben?
* Wurden Anstrengungen unternommen, um nachteilige Auswirkungen zu mildern?
* Wurden Anstrengungen unternommen, damit künftig Verstöße dieser Art nicht mehr vorkommen?
 |
| Kategorien personenbezogener Daten(Art. 83 Abs. 2 lit. g) | Im Kontext der Gesundheitsversorgung/-forschung handelt es sich immer um besondere Kategorien von Daten, sodass ein Verstoß schwerer wiegt. |
| Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde(Art. 83 Abs. 2 lit. h) | Hierzu ist z. B. zu betrachten:* Meldete der Verantwortliche bzw. der Auftragsverarbeiter selbst das Vergehen an die Aufsichtsbehörde?
* Erfuhr die Aufsichtsbehörde vom Betroffenen davon? Ggfs. aufgrund der Tatsache, dass der Verantwortliche den Betroffenen auf diese Möglichkeit hinwies?
* Wurde die Aufsichtsbehörde erst über Dritte (z.B. Presse) informiert?
 |
| Einhaltung früherer Vorgaben der Aufsichtsbehörden bzgl. aktuell beanstandeter Verarbeitung(Art. 83 Abs. 2 lit. i) | Wurden frühere Vorgaben an dem beanstandeten Gegenstand vormals berücksichtigt und werden erneut beanstandet (Wiederholungsfall)?  |
| Einhaltung genehmigter Verhaltensregeln(Art. 83 Abs. 2lit. j) | Wurden genehmigte Verhaltensregeln nach Art. 40 umgesetzt aber nicht in Gänze eingehalten? |
| Einhaltung genehmigter Zertifizierungsverfahren(Art. 83 Abs. 2lit. j) | Wurde ein genehmigtes Zertifizierungsverfahren nach Art. 42 wirksam umgesetzt, jedoch in Teilen nicht eingehalten? |
| Jegliche anderen erschwerenden oder mildernden Umstände(Art. 83 Abs. 2 lit. k) | Haben sich durch den Verstoß finanzielle Vorteile ergeben? |

Weiterhin muss sich die Höhe der Geldbuße bei einem Verstoß „europäisch“ einordnen lassen. D. h. für einen Verstoß muss theoretisch in allen Ländern ein den Umständen entsprechendes, einheitliches Bußgeld verhängt werden.

# Privacy by Design: Eine mögliche Vorgehensweise

Der Grundgedanke ist die Ausrichtung der Verarbeitung am Betroffenen. Hierzu müssen insbesondere folgende Fragen beantwortet werden:

* Was hat der Betroffene von der Verarbeitung?
* Welchen Nutzen zieht der Betroffene aus der Verarbeitung?
* Ist der Nutzen größer als (potentieller) Schaden?
* Kann der Betroffene (jederzeit) aktiv agieren? D.h. Einfluss auf die Verarbeitung nehmen?
* Erfolgt die Verarbeitung transparent?

Grundprinzip dabei ist, dass die personenbezogenen Daten explizit für einen bestimmten Zweck erhoben werden und eine weitere Verarbeitung nur in dessen Rahmen geschieht. Eine Zweckbindung wird von der Erhebung bis zur Löschung der Daten beibehalten. Dabei ist das Prinzip der Datensparsamkeit umsetzen:

* Nur erforderliche, notwendige Daten verarbeiten,
* nach Möglichkeit anonymisieren oder wenigstens pseudonymisieren,
* nach Möglichkeit nur temporär speichern.

Während der gesamten Dauer der Verarbeitung der personenbezogenen Daten erfolgt eine Wahrung der Verhältnismäßigkeit, d. h. die Verarbeitung ist für den vorgegebenen Zweck geeignet und erforderlich, es existiert kein milderes Mittel, welches weniger in die Rechte und Freiheiten der betroffenen Personen eingreift.

Dementsprechend ist ein strenges Berechtigungskonzept umzusetzen. Die Datenverwaltung bzw. der Datenzugriff darf ausschließlich entsprechend dem „Need-to-know“-Prinzip erfolgen. Dementsprechend ist eine Datenminimierung für den jeweiligen Verarbeiter vorzusehen. Wenn möglich erfolgt ein direkter Personenbezug der Daten erst beim Eintritt eines bestimmten Ereignisses, vorher erfolgt nur eine pseudonyme Nutzung.

Die Wahrung der Betroffenenrechte ist zu jedem Zeitpunkt der Verarbeitung gewährleistet. Erfolgt eine Einschränkung dieser Rechte, so erfolgt diese nur bei entsprechendem Allgemeininteresse. Die Dokumentation muss die Nachprüfbarkeit dieser Entscheidung gewährleisten.

Über den gesamten Lebenszyklus der Daten hinweg ist die Sicherheit der Daten gewahrt. Die aus Art. 32 DS-GVO resultierenden Anforderungen sind gewährleistet. Insbesondere ist berücksichtigt, dass auch Art. 32 DS-GVO eine Beurteilung der Gefährdungen aus Sicht des Betroffenen fordert, d. h. dass eine Umsetzung dieser Anforderungen auch den Anforderungen der betroffenen Person genügen muss.

Auf automatisierte Einzelentscheidung wird verzichtet.

# Rechenschaftspflicht und Dokumentation

## Was mindestens dokumentiert werden sollte

Auch Art. 25 DS-GVO unterliegt der Rechenschaftspflicht. Daher ist eine gute Dokumentation unabdingbar. Die Entscheidungsfindung, warum welche Maßnahmen ergriffen wurden, wie auch die Beschreibung der Maßnahmen selbst ist essentialer Bestandteil.

Dabei ist u.a. die Erforderlichkeit der Daten für den beschriebenen Verwendungszweck darzustellen, sowohl für

* die Daten selbst als auch
* für die Menge der erhobenen personenbezogenen Daten,
* den Umfang ihrer Verarbeitung,
* ihre Speicherfrist und
* ihre Zugänglichkeit.

Wie in Abschnitt 2.3.2 beschrieben müssen daher die drei folgenden Fragen beantwortet werden:

1. Gibt es ein anderes Mittel?

Hier wird dargestellt, mit welchen Verarbeitungen der gewünschte Verarbeitungszweck erreicht werden kann und was für die jeweilige Verarbeitung benötigt wird, d. h. welche Daten wie verarbeitet werden müssen.

1. Ist dieses in gleicher Weise geeignet, den Zweck zu erreichen?

Danach werden die verschiedenen Verarbeitungsvorgänge daraufhin untersucht, in welcher Güte welcher Verarbeitungsvorgang den gewünschten Verarbeitungszweck abbildet. D. h.

* + Welcher Verarbeitungsvorgang ist ggf. am ehesten in der Lage, den beabsichtigten Zweck zu erreichen?
	+ Welche Verarbeitungsvorgänge sind ggf. gleichermaßen geeignet?
1. Ist dieses Mittel ein milderes, also die Rechte Anderer weniger belastendes Mittel?

Danach werden die verschiedenen Verarbeitungsvorgänge, die den gewünschten Verarbeitungszweck erreichen könnten, bzgl. ihres Eingriffs in die die Rechte Betroffener beurteilt und der Verarbeitungsvorgang ausgewählt, welcher am wenigsten in diese Rechte eingreift.

Bei der Beschreibung der Maßnahmen, welche die Umsetzung der Datenschutzgrundsätze (siehe Abschnitt 2.2.4) gewährleisten, finden sich einige dieser Aspekte wieder. Aus den Datenschutzgrundsätzen resultieren Nachweispflichten bzgl.:

* Rechtmäßige Verarbeitung

Eine Verarbeitung darf nur erfolgen, wenn eine Rechtsgrundlage für die Verarbeitung existiert. D. h. diese Rechtsgrundlage der Verarbeitung muss beschrieben werden.

Die Maßnahmen müssen eine rechtswidrige Verarbeitung verhindern. An organisatorischen Maßnahmen gibt es hier beispielsweise

* + Verpflichtung auf das Datengeheimnis
	+ Schulung der Beschäftigten
	+ Anweisungen, wie mit den Daten umgegangen wird.

Technische Maßnahmen müssen die organisatorischen Maßnahmen begleiten, z. B. durch ein entsprechendes Rechtemanagement.

* Verarbeitung nach „Treu und Glauben“

Eine Verarbeitung nach „Treu und Glauben“ verlangt eine Beachtung des Verhältnismäßigkeitsgrundsatzes[[17]](#footnote-17). D.h. die Verarbeitung der personenbezogenen Daten muss

* zur Erreichung des (legitimen) Zweckes geeignet und
* das mildeste aller gleich effektiven Mittel sein.

Weiterhin muss eine Abwägung der Interessen der betroffenen Person sowie des Verantwortlichen erfolgt sein, welche ergab, dass die Verarbeitung zur Erreichung des Zweckes angemessen ist17.

* Beachtung der Zweckbindung

 Art. 25 Abs. 2 S.1 DS-GVO verlangt, dass die im Rahmen der Voreinstellungen zu treffenden technischen und organisatorischen Maßnahmen in Bezug auf den Zweck festzulegen sind. Da sich diese Anforderung auf Datenmenge, Verarbeitungsumfang Datenspeicherfrist und Datenzugänglichkeit auswirkt, ist diese Anforderung als Umsetzung der datenschutzrechtlichen Zweckbindungs- und Erfordernisgrundsätze anzusehen[[18]](#footnote-18). Somit sind die Verarbeitungszwecke (bzw. der Verarbeitungszweck) eindeutig festzulegen und zu beschreiben und auch die technischen und organisatorischen Maßnahmen, welche eine Beschränkung der Verarbeitung der Daten auf die genannten Zwecke gewährleisten, sind zu dokumentieren.

* Transparente Verarbeitung für die betroffenen Personen

Gemäß ErwGr. 39 DS-GVO sollt Transparenz dahingehend bestehen, dass eine betroffene Person Informationen bekommt, welche Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden, desgleichen in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden sollen. Die Person soll in die Lage versetzt werden, die Verarbeitung „nachvollziehen“ zu können. Hierzu sind insbesondere Maßnahmen zu ergreifen, welche die Umsetzung der Anforderungen von Artt. 12-15 DS-GVO gewährleisten und in der Dokumentation ist darzustellen, wie dies gewährleistet wird.

* Datenminimierung

Die Verarbeitung muss „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ ( Art. 5 Abs. 1 lit. c DS-GVO).

Bzgl. der „Erheblichkeit“ findet sich in der DS-GVO keine Begriffserläuterung, der im englischen Text verwendete Begriff „relevant“ legt nahe, dass „erheblich“ am ehesten im Sinne von „geeignet“ zu interpretieren ist[[19]](#footnote-19). Insgesamt erfolgt durch die Regelung eine Beschränkung der Verarbeitung: ausschließlich die zur Erreichung des Zweckes erforderliche Verarbeitung darf durchgeführt werden; ErwGr. 39 DS-GVO verlangt, dass die Verarbeitung auf das notwendige Maß beschränkt sein soll. Weiterhin ist im ErwGr. 39 DS-GVO zu finden, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.

Die Dokumentation muss also einerseits die Notwendigkeit der Verarbeitung zur Erreichung des Zweckes beinhalten, andererseits auch die Maßnahmen, welche eine anderweitige Verarbeitung verhindern.

* Gewährleistung der Richtigkeit der Daten

Die Daten müssen sachlich richtig und auf dem neuesten Stand sein[[20]](#footnote-20). Demgemäß müssen technische und organisatorische Maßnahmen vorhanden sein. In ErwGr. 39 DS-GVO findet sich hierzu, dass „alle vertretbaren Schritte unternommen werden sollen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden“. Der Hinweis bzgl. „alle vertretbaren Schritte“ weist darauf hin, dass auch hier keine absolute Forderung besteht, sondern „geeignete“ Maßnahmen i.S.v. Art. 25 Abs. 1 DS\_GVO zu treffen sind.

In der Dokumentation müssen die technischen und organisatorischen Maßnahmen aufgeführt werden, welche die Verarbeitung von „richtigen“ Daten gewährleistet.

* Begrenzung der Speicherdauer

Die Identifizierung der betroffenen Personen darf gemäß Art. 5 Abs. 1 lit. e DS-GVO nur so lange möglich sein, wie es für den Verarbeitungszweck erforderlich ist. D. h. die Speicherung personenbezogene Daten muss schnellstmöglich beendet werden.

Dies kann einerseits durch die Löschung der Daten geschehen, andererseits dadurch erreicht werden, dass die Daten dergestalt geändert werden, dass keine personenbezogenen Daten mehr vorliegen – also Herstellung einer absoluten Anonymisierung: eine Identifizierung wird unmöglich gemacht. Korrespondierend hierzu verlangen die Informationspflichten in Artt. 13 Abs. 2 lit. a,14 Abs. 2 lit. a DS-GVO eine Angabe der Speicherdauer und Art. 17 Abs. 1 lit. a DS-GVO enthält eine Löschpflicht bei Wegfall der Erforderlichkeit zur Zweckerfüllung.

Entsprechend ErwGr. 39 DS-GVO soll der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. D.h. der Verantwortliche sollte Speicher-/Archivierungs- und Löschkonzepte für die Verarbeitung personenbezogener Daten erstellen[[21]](#footnote-21).

* Sicherstellung von Integrität und Vertraulichkeit ( Art. 5 Abs. 1 lit. f DS-GVO)

Personenbezogene Daten müssen in einer Art und Weise verarbeitet werden, welche eine angemessene Sicherheit der verarbeiteten Daten gewährleistet. Geeignete technische Maßnahmen müssen insbesondere Schutz vor

* unbefugter Verarbeitung (= Verarbeitung durch unbefugte Dritte),
* unrechtmäßiger Verarbeitung (z. B. Verarbeitung ohne ausreichende Rechtsgrundlage),
* unbeabsichtigtem Verlust (z. B. die Daten kommen abhanden oder werden gelöscht),
* unbeabsichtigter Zerstörung (z. B. wenn die Daten so geändert werden, dass sie zum vorgesehenen Zweck nicht mehr verwendet werden können) sowie
* unbeabsichtigter Schädigung (z. B. wenn die Daten so geändert werden, dass sie zum vorgesehenen Zweck nur noch eingeschränkt verwendet werden können)

gewährleisten.

* Erfüllung der Rechenschaftspflicht bzgl. der Umsetzung der Anforderungen der Datenschutz-Grundverordnung ( Art. 5 Abs. 2 DS-GVO)

Aus Art. 5 Abs. 2 DS-GVO resultiert einerseits die Verantwortlichkeit als auch eine Nachweispflicht: der Verantwortliche muss die Grundsätze einhalten und der Verantwortliche muss dies nachweisen können. ErwGr. 78 DS-GVO führt aus, dass der Verantwortliche „interne Strategien festlegen und Maßnahmen ergreifen“ soll, „um die Einhaltung dieser Verordnung nachweisen zu können“.

Weiterhin ist zu dokumentieren, welche Maßnahmen die Wahrung der Betroffenenrechte zu jedem Zeitpunkt der Verarbeitung gewährleisten.

## Welche Fragen muss die Dokumentation mindestens beantworten?

Rechtmäßige Verarbeitung

* Was ist die Rechtsgrundlage der Verarbeitung?
* Ist die Rechtsgrundlage ausreichend für die Verarbeitung?
* Existiert ein Berechtigungskonzept/ ein Rechtemanagement, welches sicherstellt, dass nur eine legitime Verarbeitung erfolgen kann?

Zweckbindung/Datenminimierung

* Ist der (bzw. sind die) Verarbeitungszweck(e) eindeutig festgelegt?
* Welche technischen und organisatorischen Maßnahmen gewährleisten eine Beschränkung der Verarbeitung der Daten auf die festgelegten Verarbeitungszwecke?

Verhältnismäßigkeit

* Gibt es ein anderes Mittel?
* Ist dieses in gleicher Weise geeignet, den Zweck zu erreichen?
* Welches der vorhandenen Mittel ist das „mildeste, also die Rechte der betroffenen Personen am wenigsten belastendes Mittel?
* Erfolgte eine Abwägung der Interessen der betroffenen Person sowie des Verantwortlichen?

Erforderlichkeit hinsichtlich Erreichung des Verarbeitungszweck bzgl.

* die zu verarbeitenden Daten,
* für die Menge der erhobenen personenbezogenen Daten,
* den Umfang ihrer Verarbeitung,
* ihre Speicherfrist und
* ihre Zugänglichkeit

Transparente Verarbeitung

* Können die von der Verarbeitung betroffenen Personen die Verarbeitung „nachvollziehen“?
* Wurden die der Anforderungen von Artt. 12-15 DS-GVO umgesetzt?

Gewährleistung der Richtigkeit der Daten

* Sind alle vertretbaren Schritte unternommen worden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden?
* Welche technischen und organisatorischen Maßnahmen gewährleisten die Verarbeitung von „richtigen“ Daten?

Begrenzung der Speicherdauer

* Wurden Fristen für die Löschung der personenbezogenen Daten bzw. Fristen für die regelmäßige Überprüfung hinsichtlich zu erfolgender Löschung festgelegt?
* Existieren Speicher-/Archivierungs- und Löschkonzepte für die Verarbeitung der personenbezogener Daten?

Sicherstellung von Integrität und Vertraulichkeit

* Existieren geeignete technische Maßnahmen zum Schutz der personenbezogenen Daten?
* Ist insbesondere Schutz vor
	+ unbefugter Verarbeitung (= Verarbeitung durch unbefugte Dritte),
	+ unrechtmäßiger Verarbeitung (z. B. Verarbeitung ohne ausreichende Rechtsgrundlage),
	+ unbeabsichtigtem Verlust (z. B. die Daten kommen abhanden oder werden gelöscht),
	+ unbeabsichtigter Zerstörung (z. B. wenn die Daten so geändert werden, dass sie zum vorgesehenen Zweck nicht mehr verwendet werden können) sowie
	+ unbeabsichtigter Schädigung (z. B. wenn die Daten so geändert werden, dass sie zum vorgesehenen Zweck nur noch eingeschränkt verwendet werden können)

gewährleistet?

Erfüllung der Rechenschaftspflicht

* Wurden interne Strategien festgelegt und Maßnahmen ergriffen, um die Einhaltung der Anforderungen der DS-GVO nachweisen zu können?
* Ist sichergestellt, dass Datenschutzfragen schon in der Planungsphase berücksichtigt werden und für die Umsetzung der zur Gewährleistung der Anforderungen der DS-GVO geplanten Maßnahmen ausreichend Ressourcen zur Verfügung stehen?

## Was wird wo dokumentiert?

Dokumentation wird nicht nur von Art. 25 DS-GVO verlangt. Es gibt eine Vielzahl von Stellen, die neben den Anforderungen aus Art. 25 DS-GVO auch eine Dokumentation verlangen, die nachfolgende Tabelle zeigt beispielhaft ein paar Stellen auf:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|   | Datenschutz-Grundsätze | Einwilligung | Tätigkeits-verzeichnis | Datenschutz-Folgenabschätzung | Dokumentation TOMs | Daten-pannen |
| Rechtmäßigkeit | X |  |  | X |  |  |
| Verantwortlicher[[22]](#footnote-22) | X | X |  |  |  |  |
| Zweck(e) | X | X | X | X | X | X |
| Betroffene (Kategorien) | X |  | X | X |  | X |
| Daten (Kategorien) | X | X | X | X | X | X |
| Empfänger (Kategorien) | X | X | X | X | X |  |
| Löschfristen | X | X | X | X | X |  |
| Drittland-Verarbeitung | X | X | X | X | X |  |
| Risikobetrachtung |  |  |  | X |  | X |
| TOM |  | X | X | X | X | X |

Dabei muss natürlich nicht alles doppelt dokumentiert werden. Ein entsprechendes Datenschutz-Managementsystem vorausgesetzt werden die entsprechenden Punkte an einer Stelle dokumentiert und stehen dann überall dort zur Verfügung, wo sie benötigt werden.

# Checkliste

## Datenschutz durch Technikgestaltung (Privacy by Design)

|  | **Ja** | **Nein** |
| --- | --- | --- |
| Wurde bereits bei der Entwicklung des Verarbeitungsprozesses dieser so konstruiert, dass Anforderungen des Datenschutzes standardmäßig implementiert sind? |  |  |
| Berücksichtigt und gewährleistet der Verarbeitungsprozess die Erfüllung der Betroffenenrechte aus den Art. 12–23 DS-GVO? |  |  |
| Ist eine Funktion implementiert, die der betroffenen Person nutzen kann, um die zu seiner Person gespeicherten Daten einsehen zu können? |  |  |
| Ist eine Funktion implementiert, die der betroffenen Person eine Kopie seiner Daten zur Verfügung stellt? |  |  |
| Ist eine Funktion zur Löschung der Daten implementiert? |  |  |
| Ist eine Funktion zur Übertragbarkeit der Daten implementiert? |  |  |
| Wird die Einhaltung des Grundsatzes des Datenschutzes durch Technik durch Vorlage eines Auditnachweises (z. B. ein entsprechendes Zertifikat) belegt? |  |  |

## Datenschutz durch datenschutzfreundliche Voreinstellungen (Privacy by Default)

|  | **Ja** | **Nein** |
| --- | --- | --- |
| Ist der Datenumfang, der für den Verarbeitungsprozessgenutzt wird, hinsichtlich der personenbezogenen Daten auf das zur Zweckerfüllung absolut Notwendige beschränkt? |  |  |
| Verfügt das Verarbeitungssystem über ein Berechtigungskonzept, welches gewährleistet, das ein Zugriff nur nach dem Need-to-know-Prinzip erfolgt? |  |  |
| Verfügt das Verarbeitungssystem über ein Berechtigungskonzept, welches gewährleistet, das ein Zugriff auf besonders schützenswerte Daten nur unter Einhaltung eines Vier-Augen-Prinzips erfolgt? |  |  |
| Werden Daten von vornherein mit einem Verfallsdatum gespeichert? |  |  |
| Werden Daten nach Erreichen der Speicherhöchstdauer (= Ablauf der gesetzlichen Aufbewahrungsfrist) / des Verfallsdatums automatisch durch das System gelöscht |  |  |
| Ist die Nutzung bestimmter Funktionen unmittelbar an das Vorliegen einer wirksamen Rechtsgrundlage (z. B. Einwilligung der betroffenen Person) gebunden? |  |  |
| Wird die Einhaltung des Grundsatzes der datenschutzfreundlicher Voreinstellung durch Vorlage eines Auditnachweises (z. B. ein entsprechendes Zertifikat) belegt? |  |  |

# Abkürzungen

|  |  |
| --- | --- |
| Abs | Absatz |
| Art | Artikel |
| Artt | Artikel (Mehrzahl) |
| BCR | Binding Corporate Rules |
| bvitg | Bundesverband Gesundheits-IT e.V. |
| DSG | Datenschutzgesetz |
| DS-GVO | Datenschutz-Grundverordnung |
| ErwGr | Erwägungsgrund/Erwägungsgründe |
| EU | Europäische Union |
| GDD | Gesellschaft für Datenschutz und Datensicherheit e.V. |
| GMDS | Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. |
| IT | Informationstechnik, informationstechnisches… |
| Kap | Kapitel |
| lit | littera (lat. „Buchstabe“) |
| RL | Richtlinie |
| Ziff | Ziffer |

# Literatur

## Fachzeitschriften

* Aldeen YAAS, Salleh M, Razzaque MA. (2015) A comprehensive review on privacy preserving data mining. SpringerPlus (4): 694-730
* Baumgartner U, Gausling T. (2017) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. ZD: 308-313
* Bieker F, Hansen M. (2017) Datenschutz "by Design" und "by Default" nach der neuen europäischen Datenschutz-Grundverordnung. RDV: 165-170
* Cavoukian A. (2010) Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. IDIS (3): 247–251
* Cavoukian A, Taylor S, Abrams ME. (2010) Privacy by Design: essential for organizational accountability and strong business practices. IDIS (3): 405–413
* David JS, Prosch M. (2010) Extending the value chain to incorporate privacy by design principles. IDIS (3): 295–318
* Hansen M. (2011) Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. IFIP AICT (375): 14–31
* Hansen M. (2013) Data Protection by Default in Identity-Related Applications. IFIP AICT (396): 4–17
* Hustinx P. (2010) Privacy by design: delivering the promises. IDIS (3): 253–255
* Jandt S. (2017) Datenschutz durch Technik in der DS-GVO. DuD: 562-566
* Nordgren A. (2015) Privacy by Design in Personal Health Monitoring. Health Care Anal (23): 148–164
* Ochs C, Richter P, Uhlmann, M. (2016) Technikgestaltung demokratisieren – Partizipatives Privacy by Design. ZD-Aktuell: 05424
* PearsonS, Benameur A. (2010) A Decision Support System for Design for Privacy. IFIP AICT (352): 293-296
* Richter P. (2012) Datenschutz durch Technik und die Grundverordnung der EU-Kommission. DuD: 576-580
* Schaar P. (2010) Privacy by Design. IDIS (3) 267–274

## Internet

* ENISA - European Union Agency for Network and Information Security (2015) Privacy and Data Protection by Design. [Online, zitiert am 2018-02-14]; Verfügbar unter <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport>
* ENISA - European Union Agency for Network and Information Security (2015) Privacy by design in big data. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.enisa.europa.eu/publications/big-data-protection/at\_download/fullReport
* Gurses S, Troncoso, C, Diaz C. (2015) Engineering Privacy by Design. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf
* Gurses S, Troncoso, C, Diaz C. (2015) Engineering Privacy by Design Reloaded. In Amsterdam Privacy Conference. [Online, zitiert am 2018-02-14]; Verfügbar unter <https://www.esat.kuleuven.be/cosic/publications/article-2589.pdf>
* Privacy Commissioner of Ontario (2009) Privacy by Design: The 7 Foundational Principles. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
* Privacy Commissioner of Ontario (2009) A Pragmatic Approach to Privacy Risk Optimization: Privacy by Design for Business Practices. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-risk.pdf
* Privacy Commissioner of Ontario (2009) Privacy by Design … Take the Challenge. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/PrivacybyDesignBook.pdf
* Privacy Commissioner of Ontario (2009) Whole Body Imaging in Airport Scanners: Building in Privacy by Design. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/wholebodyimaging.pdf
* Privacy Commissioner of Ontario (2010) Access by Design: The 7 Fundamental Principles. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/2010/05/accessbydesign\_7fundamentalprinciples.pdf
* Privacy Commissioner of Ontario (2012) Privacy by Design and User Interfaces: Emerging Design Criteria – Keep it User-Centric. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-user-interfaces\_Yahoo.pdf
* Privacy Commissioner of Ontario (2012) Privacy by Design and the Emerging Personal Data Ecosystem. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-pde.pdf
* Privacy Commissioner of Ontario (2013) Privacy by Design. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf
* Privacy Commissioner of Ontario (2013) Privacy and Security by Design: An Enterprise Architecture Approach. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf
* Privacy Commissioner of Ontario (2013) Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual’s Pursuit of Radical Control. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/digital-enlightenment-yearbook2013.pdf
* Privacy Commissioner of Ontario (2014) Privacy Engineering: Proactively Embedding Privacy, by Design. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-priv-engineering.pdf
* Privacy Commissioner of Ontario (2014) Privacy by Design Solutions for Biometric One-to-Many Identification Systems. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/2014/06/pbd-solutions-biometric.pdf
* Privacy Commissioner of Ontario (2014) A New Possibility for Security and Privacy by Design: Fault-Free Software. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/2014/06/pbd-fault-free-software.pdf
* Privacy Commissioner of Ontario (2018) Privacy by Design - Seven foundational principles. [Online, zitiert am 2018-02-14]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf
* Rubinstein IS, Good N. (2013) Privacy by Design: A Counterfactual Analysis of Google and Facebook privacy incidents. [Online, zitiert am 2018-02-14]; Verfügbar unter https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.de/&httpsredir=1&article=2007&context=btlj

## Bücher

* Blokdyk G. (2017) Privacy by Design: A Hands-On Tutorial. Verlag CreateSpace Independent Publishing Platform. ISBN 978-1978276338
* Bartschat N. (2018) Datenschutzprinzipien für vernetzte Fahrzeuge. Umsetzung von Privacy by Default und Privacy by Design: Herausforderungen und Gestaltungsempfehlungen. Verlag Grin. ISBN 978-3668598386
* Tschersich M. (2015) Privacy by Default in the European Union Proposal for Data Protection Regulation: Studies on the Impact of Restrictive Default Privacy. Verlag Dr. Kovac. ISBN 978-3830082118
* Vagts HH (2013) Privatheit und Datenschutz in der intelligenten Überwachung: Ein datenschutzgewährendes System, entworfen nach dem „Privacy by Design“ Prinzip. Verlag KIT Scientific Publishing. ISBN 978-3-7315-0041-4
1. Ann Cavoukian: Privacy by Design: Strong Privacy Protection - Now, and Well into the Future. [Online, zitiert am 2017-12-07]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf [↑](#footnote-ref-1)
2. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. [Online, zitiert am 2017-12-07]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A31995L0046 [↑](#footnote-ref-2)
3. Wenngleich ErwGr. 46 der RL 95/46/EG bereits darstellte, dass die Maßnahmen „sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung“ eine unrechtmäßige Verarbeitung verhindern müssen. [↑](#footnote-ref-3)
4. Hinweis bzgl. Art. 5 DS-GVO nicht in der DS-GVO, sie stammen von den Verfassern dieser Ausarbeitung [↑](#footnote-ref-4)
5. So z. B. Nolte N, Werkmeister C. Art. 25 Rn. 13 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8 [↑](#footnote-ref-5)
6. Demingkreis oder PDCA-Zyklus (PDCA steht für das englische Plan-Do-Check-Act): ein iterativer Prozess für Lernen und Verbesserung eines Prozesses: der Prozess wird geplant („plan“, dann umgesetzt („do“), anschließend Prozessablauf und Ergebnisse überprüft („check“) und basierend auf den Ergebnissen der Prüfung der Vorgang bei Bedarf angepasst („act“) [↑](#footnote-ref-6)
7. Martini M. Art. 24 Rn. 33 in Plath (Hrsg.) BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. ottoschmidt Verlag 2016. ISBN 978-3-504-56074-4 [↑](#footnote-ref-7)
8. DIN CEN ISO/TS 14265 (Stand 2014-03) „Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen“. [Online, zitiert am 2018-01-16]; Verfügbar unter [https://www.beuth.de/de/ technische-regel/din-cen-iso-ts-14265/149023541](https://www.beuth.de/de/technische-regel/din-cen-iso-ts-14265/149023541) [↑](#footnote-ref-8)
9. Martini M. Art. 35 Rn. 15 in Plath (Hrsg.) BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. ottoschmidt Verlag 2016. ISBN 978-3-504-56074-4 [↑](#footnote-ref-9)
10. Bzgl. Lebensrisiko siehe auch: BGH Urt. V. 1993-05-04, AZ VI ZR 283/92. Online, zitiert am 2017-11-21; Verfügbar unter [https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=04.05.1993 &Aktenzeichen=VI%20ZR%20283/92](https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=04.05.1993&Aktenzeichen=VI%20ZR%20283/92) [↑](#footnote-ref-10)
11. Martini M. Art. 35 Rn. 25 in Plath (Hrsg.) BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. ottoschmidt Verlag 2016. ISBN 978-3-504-56074-4 [↑](#footnote-ref-11)
12. Ann Cavoukian: Privacy by Design - The 7 Foundational Principles. [Online, zitiert am 2017-12-07]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf [↑](#footnote-ref-12)
13. Martini M. Art. 25 Rn. 41 in Paal /Pauly (Hrsg.) GVO Datenschutz-Grundverordnung. C.H.Beck Verlag 2017. ISBN 978-3-406-69570-4 [↑](#footnote-ref-13)
14. So z. B. Nolte N, Werkmeister C. Art. 25 Rn. 19 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8 [↑](#footnote-ref-14)
15. Der Begriff „genehmigte Zertifizierungsverfahren“ ist hierbei im Sinne von Art. 42 DS-GVO zu interpretieren, d.h. um Verfahren die gemäß Art. 42 Abs. 5 DS-GVO durch „Zertifizierungsstellen nach Art. 43 oder durch die zuständige Aufsichtsbehörde anhand der von dieser zuständigen Aufsichtsbehörde gemäß Art. 58 Abs. 3 oder - gemäß Art. 63 - durch den Ausschuss genehmigten Kriterien“ zertifiziert wurden. [↑](#footnote-ref-15)
16. Hanßen H. Art. 25 Rn. 16 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0 [↑](#footnote-ref-16)
17. Böhm WT, Ströbel L. Art. 5 Rn. 8 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0 [↑](#footnote-ref-17)
18. Hanßen H. Art. 25 Rn. 46 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0 [↑](#footnote-ref-18)
19. So auch Böhm WT, Ströbel L. Art. 5 Rn. 18 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0 [↑](#footnote-ref-19)
20. Böhm WT, Ströbel L. Art. 5 Rn. 22 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0 [↑](#footnote-ref-20)
21. Böhm WT, Ströbel L. Art. 5 Rn. 29 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0 [↑](#footnote-ref-21)
22. Angaben zum Verantwortlichen: Adresse, Ansprechpartner wie Geschäftsführung, Datenschutzbeauftragter usw. [↑](#footnote-ref-22)