Sicherheit personenbezogener Daten: Umgang mit Art. 32 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“

Autoren

Christoph Isele	Cerner Deutschland GmbH
Pierre Kaufmann	Agfa HealthCare
Lukas Mempel	Sana Kliniken AG
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Kanzlei Spyra / / Ratajczak und Partner mbB Rechtsanwälte

Stand: xx.02.2018

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:

Inhaltsverzeichnis

Zusammenfassung

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist eines der grundlegenden Ziele der EU Datenschutz-Grundverordnung (DS-GVO), wie man in Art. 1 Abs. 1 DS-GVO) nachlesen kann. Dabei verfolgt die DS-GVO einen Risiko-orientierten Ansatz. Dementsprechend muss neben dem Vorliegen eines Erlaubnistatbestandes und der Einhaltung der Grundsätze des Datenschutzes (Art. 5 DS-GVO) insbesondere auch die Sicherheit der Verarbeitung gewährleistet sein. Dabei ist nicht das höchstmögliche Maß an Sicherheit der Verarbeitung zu gewährleisten, sondern es muss ein angemessenes Schutzniveau sichergestellt werden: Art. 32 DS-GVO schreibt vor, dass unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten,
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten

geeignete technische und organisatorische Maßnahmen getroffen werden müssen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Verantwortlich für die Gewährleistung ist nach Art. 32 DS-GVO sowohl der für die Verarbeitung Verantwortliche als auch – sofern vorhanden - der Auftragsverarbeiter. Letzterer natürlich nur für den Teil, den der Auftragsverarbeiter zu verantworten hat. Aus Art. 5 DS-GVO folgt eine Nachweispflicht, die aber indirekt auch von Art. 32 Abs. 3 DS-GVO verlangt wird.

Der Schutz der Daten ist entsprechend der DS-GVO also nicht absolut. Allerdings verlangt die DS-GVO auch, dass dieser dem Risiko der Verarbeitung angemessene Schutz auf Dauer sicherzustellen ist. D. h. die

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit und
- Belastbarkeit

für Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten ist auf Dauer zu gewährleisten. Demgemäß muss z. B. die Verfügbarkeit und der Zugang der personenbezogenen Daten nach einem physischen oder technischen Zwischenfall (angemessen) „rasch“ wiederherstellbar sein; beides unter dem Aspekt, dass Schäden für die betroffene Person vermieden werden. Denn während die „klassische“ IT-Sicherheit die (Daten-)Sicherheit des Unternehmens gewährleistet, verlangt Art. 32 DS-GVO eine Betrachtung und Behandlung der Risiken für die betroffenen Personen; den Rechten und berechtigten Interessen der von der Verarbeitung betroffenen Personen und sonstiger von der Verarbeitung betroffener Menschen Rechnung zu tragen. Dabei ist der Begriff der „Verarbeitung“ in der DS-GVO weiter gefasst als im bisherigen deutschen Datenschutzrecht. Unter Verarbeitung ist alles zu verstehen, was mit den Daten geschieht, z.B. Erhebung, Auslesung, Änderung, Speicherung, Löschung – kurz alles, was man mit Daten tun kann.

Die DS-GVO verlangt für die Gewährleistung der Sicherheit der Verarbeitung letztlich ein Risikomanagement, welches die Risiken der Verarbeitung für die betroffenen Personen darstellt sowie die Ergreifung von Maßnahmen zur Vermeidung oder – falls dies ohne Verzicht auf die Verarbeitung nicht möglich ist – Minimierung der Risiken auf ein für die betroffenen Personen akzeptables Maß.

Fazit: Datenschutzbeauftragte müssen lernen, dass nicht die höchstmögliche Sicherheit gewährleistet werden muss, Verantwortliche müssen lernen, dass sie nachweisen müssen, warum mögliche Verfahren/Methoden zur Gewährleistung der Sicherheit der Verarbeitung nicht genutzt wurden. Verantwortliche und – sofern vorhanden – Auftragsverarbeiter müssen das für die Verarbeitung angemessene Schutzniveau für die gesamte Verarbeitungsdauer, d.h. für den gesamten Lebenszyklus der Daten gewährleisten.

1 Einleitung

Die EU Datenschutz-Grundverordnung (DS-GVO) verfolgt einen Risiko-orientierten Ansatz, demgemäß neben dem Vorliegen eines Erlaubnistatbestandes entsprechend Artt. 6 bzw. 9 DS-GVO und der Einhaltung der Grundsätze des Datenschutzes (Art. 5 DS-GVO) auch die Sicherheit der Verarbeitung gewährleistet ist, D. h. der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten muss gewährleistet sein (Art. 1 Abs. 1 DS-GVO).
Art. 32 DS-GVO schreibt vor, dass sowohl der für die Verarbeitung Verantwortliche als auch – sofern vorhanden - der Auftragsverarbeiter unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten,
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten

geeignete technische und organisatorische Maßnahmen treffen müssen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zugleich resultiert aus Art. 5 DS-GVO eine Nachweispflicht. Damit lässt sich festhalten:

1. Der Schutz der Daten ist nicht absolut. Es muss aus datenschutzrechtlichen Gründen nicht zwingend das höchstmögliche Schutzniveau umgesetzt werden, sondern ein unter Berücksichtigung der oben genannten Punkte angemessenes Niveau.
2. Es existiert bzgl. der Angemessenheit eine Nachweispflicht.

Dabei adressiert Art. 32 DS-GVO unterschiedliche Schutzziele:

1. An erster Stelle steht die Forderung ein angemessenes Schutzniveau hinsichtlich des Risikos für die Rechte und Freiheiten natürlicher Personen zu gewährleisten.
2. Hieraus abgeleitet resultiert die Forderung, dass
   - Vertraulichkeit,
   - Integrität,
   - Verfügbarkeit und
   - Belastbarkeit

   für Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten auf Dauer sicherzustellen ist. D. h. es muss nicht von Anfang an alles perfekt sein, insbesondere ist aus Fehlern zu lernen und die Verarbeitung immer sicherer im Sinne der Verordnung zu gestalten.
3. Die Verfügbarkeit der personenbezogenen Daten muss nach einem physischen oder technischen Zwischenfall „rasch“ wiederherstellbar sein, desgleichen der Zugang zu den Daten.

Gemäß ErwGr. 83 ist der Zweck dieser Sicherheitsmaßnahmen die Gewährleistung der Sicherheit. Aber auch die Vorbeugung gegen eine die Vorgaben der DS-GVO verstoßende Verarbeitung.

Während die „klassische“ IT-Sicherheit die Sicherheit des Unternehmens gewährleistet, verlangt Art. 32 DS-GVO eine Betrachtung der Risiken für die betroffenen Personen. D. h. die DS-GVO adressiert die Risiken der betroffenen Personen, nicht die Risiken des Unternehmens. Die Risiken können sich natürlich überscheiden, Risiken für die betroffenen Personen können zugleich auch Risiken des Unternehmens darstellen. Aber grundsätzlich sind auch Risiken zu betrachten, die der Verarbeiter darstellt wie z. B. Weiterverkauf personenbezogener Daten an interessierte Parteien,

was selbstverständlich auch in anonymisierter oder pseudonymisierter Form ein Re-Identifikationsrisiko für die betroffenen Personen beinhaltet und damit verbunden ein Missbrauchspotential bzgl. der Verarbeitung der personenbezogenen Daten darstellt.

2 Anforderungen der Norm

2.1 Grundlegende Anforderungen

Art. 32 DS-GVO richtet sich sowohl an den Verantwortlichen als auch an Auftragsverarbeiter und beinhaltet die Pflicht, durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau bzgl. der Verarbeitung zu gewährleisten. Dabei werden von Art. 32 Abs. 1 lit. a-d DS-GVO Maßnahmen benannt, die eingeschlossen werden müssen.

Im Folgenden wird einerseits dargelegt, was unter einem „angemessenen Schutzniveau" zu verstehen ist, anderseits werden die von der Schutznorm dargestellten Maßnahmen besprochen.

2.2 Nachweis der Normkonformität

2.2.1 Verpflichtung zum Nachweis

Entsprechend Art. DS-GVO besteht natürlich eine allgemeine Nachweisverpflichtung bzgl. der Einhaltung der Vorgaben des Verantwortlichen. Aber Art. 32 Abs. 3 DS-GVO verlangt selbst auch den Nachweis bzgl. der Einhaltung bzw. der Erfüllung seiner Vorgaben, und dies gilt sowohl für den Verantwortlichen wie auch – sofern vorhanden – für Auftragsverarbeiter[1].

2.2.2 Verhaltensregeln und Zertifizierung

Gemäß Art. 32 Abs. 3 DS-GVO können genehmigte Verhaltensregeln nach Art. 40 DS-GVO oder ein genehmigtes Zertifizierungsverfahren entsprechend Art. 42 DS-GVO als Faktoren herangezogen werden, um einen Nachweis bzgl. der Erfüllung der Anforderungen von Art. 32 Abs. 1 und 2 DS-GVO zu erbringen.

Die Aussage „kann als Faktor herangezogen werden" ist dabei nicht derart zu verstehen, dass den Aufsichtsbehörden hiermit ein Ermessen bzgl. der Berücksichtigung der Selbstregulierungsinstrumente eingeräumt wird[2]. Vielmehr bezieht sich das „kann" auf die Auswahlmöglichkeit des Verantwortlichen bzw. Auftragsverarbeiters: Verhaltensregeln bzw. Zertifizierung können genutzt werden, müssen aber nicht. Werden die Selbstregulierungsinstrumente genutzt, so sind sie als Nachweis bzgl. der Erfüllung der Anforderung entsprechend zu würdigen[2].

Auch bedeutet die Einhaltung von Verhaltensregeln oder Zertifizierungsmaßnahmen nicht zwangsläufig, dass damit sämtliche Pflichten des Art. 32 DS-GVO erfüllt werden müssen[3]. Entsprechend Art. 32 Abs. 4 sind diese Selbstregulierungsinstrumente als ein Faktor heranzuziehen, d. h. die Erfüllung kann auch durch den Einsatz weiterer Faktoren gewährleistet werden; wobei den

[1] Schreibauer M, Spittka J. Art. 32 Rn. 19 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0
Piltz C. Art. 44 Rn. 36 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

[2] Martini M. Art. 32 Rn. 63 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

[3] Piltz C. Art. 44 Rn. 46 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

Selbstregulierungsinstrumente bedingt durch ihre vorherige Prüfung seitens der Aufsichtsbehörde selbstverständlich eine entsprechende Gewichtung beigemessen werden muss.

Entsprechend § 38 BDSG n.F. erfolgt die Erteilung der Befugnis, als Zertifizierungsstelle gemäß Art. 43 Abs. 1 S. 1 DS-GVO zu agieren, durch die für die Zertifizierungsstelle zuständige Aufsichtsbehörde des Bundes oder der Länder auf Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle. D. h. in Deutschland existiert ein zweistufiges Vorgehen:

1) Zunächst ist eine Akkreditierung durch die Deutsche Akkreditierungsstelle erforderlich,
2) dann erteilt die zuständige Datenschutz-Aufsichtsbehörde auf dieser Grundlage die Befugnis.

3 Angemessenes Schutzniveau

Bei der Auswahl der Maßnahmen sind

- der Stands der Technik,
- die Implementierungskosten,
- Art, Umfangs, Umstände und Zwecke der Verarbeitung sowie
- die unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten betroffener Personen

zu berücksichtigen. Daher müssen alle vier Sachverhalte dargestellt und betrachtet werden. Dabei ist eine Umsetzungspflicht abhängig von dem Ergebnis einer Verhältnismäßigkeitsprüfung[4, 5].

Zunächst ist zu klären, was unter dem „Stand der Technik“ zu verstehen ist. Dann sind die „Implementierungskosten“ zu berücksichtigen. Dies bedingt eine betriebswirtschaftliche Bewertung von Maßnahmen der Informationssicherheit. Hierzu ist einerseits die vollständige Erfassung und adäquate Quantifizierung der bestehenden Risiken erforderlich, andererseits müssen die Kosten und Wirksamkeit von Schutzmaßnahmen dargestellt werden. Da dies auch zur Darstellung der Eintrittswahrscheinlichkeit sowie der Schwere des Risikos benötigt wird, erfolgt dort die Betrachtung. Schwierig an dieser Betrachtung ist, dass gerade im Bereich der IT-Sicherheit häufig eine hinreichend präzise Quantifizierung der Risiken nicht möglich; hier muss eine bestmögliche Näherung erzielt werden. Zur Darstellung der Risiken werden insbesondere auch eine klare Beschreibung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung benötigt. Daher greifen die zu berücksichtigenden Tatbestände ineinander und ergänzen sich gegenseitig.

3.1 „Stand der Technik“

In der DS-GVO existiert keine Legaldefinition bzgl. „Stand der Technik“. in der Begründung zum IT-Sicherheitsgesetz[6] heißt es:

> „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

[4] Piltz C. Art. 32 Rn. 9 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

[5] Schreibauer M, Spittka J. Art. 32 Rn. 16 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0

[6] Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). S. 14, 15. Online, zitiert am 2017-08-31; Verfügbar unter https://dip21.bundestag.de/

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."

Aus europäischer Sicht bietet am ehesten der Terminus „beste verfügbare Technik" entsprechend Art. 3 Ziff. 10 Industrieemissions-Richtlinie[7] eine Definition bzgl. „Stand der Technik". Hier findet sich als Definition

> „beste verfügbare Techniken" den effizientesten und fortschrittlichsten Entwicklungsstand der Tätigkeiten und entsprechenden Betriebsmethoden, der bestimmte Techniken als praktisch geeignet erscheinen lässt, […] oder, wenn dies nicht möglich ist, zu vermindern:
>
> a) „Techniken": sowohl die angewandte Technologie als auch die Art und Weise, wie die Anlage geplant, gebaut, gewartet, betrieben und stillgelegt wird;
> b) „verfügbare Techniken": die Techniken, die in einem Maßstab entwickelt sind, der unter Berücksichtigung des Kosten/Nutzen-Verhältnisses die Anwendung unter in dem betreffenden industriellen Sektor wirtschaftlich und technisch vertretbaren Verhältnissen ermöglicht, gleich, ob diese Techniken innerhalb des betreffenden Mitgliedstaats verwendet oder hergestellt werden, sofern sie zu vertretbaren Bedingungen für den Betreiber zugänglich sind;
> c) „beste": die Techniken, die am wirksamsten zur Erreichung eines allgemein hohen Schutzniveaus […] sind".

Übertragen auf die IT-Sicherheit folgt daraus: Unter Berücksichtigung des Kosten/Nutzen-Verhältnisses muss die Technik eingesetzt werden, welche für den jeweiligen Bereich als Standard angesehen wird und dabei das höchstmögliche Schutzniveau gewährt. Wikipedia beschreibt den Begriff „Standard" wie folgt: „Ein Standard ist eine vergleichsweise einheitliche oder vereinheitlichte, weithin anerkannte und meist angewandte (oder zumindest angestrebte) Art und Weise, etwas herzustellen oder durchzuführen, die sich gegenüber anderen Arten und Weisen durchgesetzt hat."[8]

3.1.1 Stand der Technik und Normen

Normen und Richtlinien sind in erster Linie Empfehlungen privater Vereine, z. B. die vom Deutschen Instituts für Normung (DIN) herausgegebenen Normen. Die Verbindlichkeit einer Norm regelt sich durch die Vereinbarung der beteiligten Parteien, für welche die Norm(en) Leistungsgrundlage sein soll. Somit stellen Normen nicht zwangsläufig eine Regel oder Stand der Technik dar. Vielmehr ist eine Norm dann anerkannt, wenn Fachleute diese anwenden und sich dabei sicher sind, dass sie dem Stand der Technik entspricht. Dies beinhaltet, dass die Norm „gepflegt" wird, d. h. regelmäßig aktuell gehalten wird.

Ist die Anwendung von bestimmten Normen in einer Rechtsvorschrift vorgeschrieben, so ist deren Einhaltung selbstverständlich auch verpflichtend, auch wenn diese ggf. nicht mehr dem Stand der Technik entsprechen.

[7] Richtlinie 2010/75/EU des Europäischen Parlaments und des Rates vom 24. November 2010 über Industrieemissionen (integrierte Vermeidung und Verminderung der Umweltverschmutzung). Online, zitiert am 2017-09-04; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32010L0075

[8] Wikipedia „Standard". Online, zitiert am 2017-09-04; Verfügbar unter https://de.wikipedia.org/wiki/Standard

3.2 Implementierungskosten: Betriebswirtschaftliche Betrachtung

3.2.1 Return on Security Investment

Für diese betriebswirtschaftliche Abwägung und Maßnahmenbewertung wird in der Praxis häufig der Return on Security Investment (RoSI) als Kennzahl eingesetzt. Die Rentabilität einer IT-Sicherheitsmaßnahme wird anhand eines Vergleichs des gesenkten IT-Sicherheitsrisikos durch die Implementierung einer IT-Sicherheitsmaßnahme mit den Kosten für die Maßnahme ermittelt.

Hierzu ist es zunächst erforderlich den der zu erwartenden jährlichen Verlust (Annual Loss Expectancy, ALE) zu bestimmen. Der ALE errechnet sich aus der finanziellen Höhe (Loss, L) und der Eintrittswahrscheinlichkeit (Probability, P) eines potentiellen Schadens: $ALE = L \cdot P$.
Der zu erwartende Gesamtverlust ist dann die Summe der Erwartungswerte aller betrachteten Einzelrisiken: $ALE_{tot} = \sum_{i=1}^{n} L_i \cdot P_i$.

Die Reduktion eines betriebswirtschaftlichen Risikos kann einerseits durch eine Verringerung der Eintrittswahrscheinlichkeit erfolgen, andererseits durch eine Begrenzung der Auswirkungen des Schadens. Für das „klassische“ Controlling der IT-Sicherheit steht beides gleichberechtigt nebeneinander. Art. 32 DS-GVO verlangt jedoch eine Begrenzung des Risikos für die betroffene Person. D. h. wenn durch Maßnahmen das finanzielle Risiko z. B. durch verhängte Bußgelder reduziert wird, das Risiko für die betroffene Person unverändert ist, so ist dies keine risikoreduzierende Maßnahme aus Sicht des Art. 32 DS-GVO. (Gleichwohl kann die Ergreifung der Maßnahme aus Sicht des die Daten verarbeitenden Unternehmens natürlich wünschenswert sein.)

Leider existieren für die wenigsten Schäden im Bereich der IT belastbaren Erfahrungswerte, sodass die Berechnung des ALE-Wertes nur als Schätzung erfolgen kann. Berücksichtigt werden müssen bei der Kalkulation eines zu erwartenden Verlustes insbesondere

- Umsatzeinbußen, z. B. durch Ausfall eines Shopsystems
- Produktivitätskosten, wenn beispielsweise durch den Ausfall Produkte nicht weiterentwickelt werden können
- Wertverlust, z. B. durch Imageschaden
- Wiederherstellungskosten
- Schadensersatzleistungen, z. B. gegenüber betroffenen Personen
- Sanktionsmaßnahmen, wie z. B. von Aufsichtsbehörden verhängte Bußgelder.

Beispiel: Ausfall Mail-Gateway bei Denial-of-Service-Attacke

Kostenart	Kosten
Wiederherstellungskosten: – externer Berater (4 Stunden, Stundensatz 250 Euro)	1.000,00 €
Umsatzeinbußen – 0,5 Aufträge /Stunde Ausfall (pro Auftrag ~ 5.600 Euro)	11.200,00 €
Produktivitätskosten: – 12 Beschäftigte im Marketing (Ausfall 4 Stunden, Stundenlohn 18,60 Euro) – Fax statt Mailbestätigung für eingegangene Aufträge (25 x, Kosten je Fax 0,10 Euro)	892,80 € 2,50 €
Kosten einmaliger Ausfall:	13.095,30 €

Auch die Kosten für die Implementierung einer Schutzmaßnahme setzen sich aus unterschiedlichen Kostenblöcken zusammen:

- Konzeptionskosten, z. B. Entwicklung bzw. Auswahl der Lösung, Testbetrieb, Anpassungen an die eigene Infrastruktur
- Investitionskosten, wie beispielsweise anzuschaffende Hardware, Software, Schulungskosten, Installation/Konfiguration
- Betriebskosten, Kosten für Support. Lizenzkosten, usw.

Aus diesen drei Kostenblöcken werden die Gesamtkosten der Sicherheitsmaßnahmen (Total Cost of Ownership, TCO) berechnet. Hierbei ist zu beachten, dass Einmalkosten über den Betriebszeitraum abgeschrieben werden: $TCO = \frac{Konzeptionskosten + Investitionskosten}{Betriebszeitraum} + Betriebskosten.$

RoSI berechnet sich jetzt dadurch, dass der ALE-Wert vor und nach Einführung der IT-Sicherheitsmaßnahmen betrachtet wird: $RoSI = \frac{(ALE_{alt} - ALE_{neu}) - TCO}{TCO}$. Oder in Worte gefasst: die erwartete Ersparnis beim ALE-Wert ($ALE_{Alt} - ALE_{neu}$) muss über den Anschaffungs- und Betriebskosten liegen, dann ist die Maßnahme aus betriebswirtschaftlicher Sicht sinnvoll.

3.2.2 Grenzen der RoSI-Methode

Im Berechnungsansatz wird vereinfachend davon ausgegangen, dass ein Risiko von einer Sicherheitsmaßnahme adressiert wird. In der Praxis adressiert eine Maßnahme häufig mehr als ein Sicherheitsrisiko, z. B. soll eine Firewall Denial-of-Service-Attacken ebenso verhindern wie das Eindringen unbefugter in das eigene Rechnernetz. Andererseits können Maßnahmen auch neue Risiken in sich bergen, z. B. muss zur Fernwartung Dritten Zugriff auf das eigene Rechnernetz gewährt werden, was grundsätzlich einen potentiellen Missbrauch des Zugangs beinhaltet (z. B. durch einen Zugriff Unbefugter auf das Netz der fernwartenden Partei) und somit immer auch eine Sicherheitslücke darstellt. Weiterhin wird davon ausgegangen, dass eine Schadenswiederholung einen gleichbleibenden Schaden verursacht. Jedoch wird ein einmaliger Sicherheitsvorfall in einer Bank oder einem Krankenhaus durch die Öffentlichkeit anders bewertet, als wenn einmal pro Monat ein entsprechender Vorfall passiert, was wiederum in einem gesteigerten Imageverlust resultiert. Ferner besteht der „Gewinn“ in der Betrachtung in einer Verminderung eines operationellen Risikos, also eines Erwartungswertes für die Kosten von Sicherheitsvorfällen; ob dadurch tatsächlich Einsparungen erzielt worden sind, lässt sich selbst nachträglich nach Eintritt eines Schadensfalls selten feststellen.

D. h. die Abschätzung wird sicherlich nicht die Wirklichkeit widerspiegeln, jedoch kann RoSI die Tendenz recht gut darstellen[9]. Daher erscheint RoSI gut geeignet, um für Dritte wie z. B. Aufsichtsbehörden nachvollziehbar darlegen zu können, warum Investitionskosten für IT-Sicherheitsmaßnahmen für ein Unternehmen tragbar sind oder nicht.

[9] Adrian Mizzi entwickelte im Rahmen einer MBA Dissertation die Methode des „Return On Information Security Investment“, welche eine Empfehlung für die maximal sinnvollen Ausgaben für IT-Sicherheit geben soll. Dazu nutzt das Modell Annahmen, welche Investitionen ein Angreifer tätigen würde. Letztlich beruht auch diese Methoden auf Abschätzungen, welche auf Grund mangelnder validierter Werte die Wirklichkeit nicht abbilden kann. Informationen zu dieser Methode sind zu finden unter

- Mizzi A (2005) Return on Information Security Investment. Online, zitiert am 2017-09-06; Verfügbar unter http://www.adrianmizzi.com/ROISI-Paper.pdf
- Adrian Mizzi. Return On Information Security Investment. Verlag: lulu.com (2005) ISBN 978-1409209164

3.3 Art, Umfangs, Umstände und Zwecke der Verarbeitung

3.3.1 Verarbeitung

Der Begriff der Verarbeitung ist in der DS-GVO weiter gefasst als im bisherigen deutschen Datenschutzrecht. Art. 4 Ziff. 2 DS-GVO nennt als Arten der Verarbeitung insbesondere:

- Erheben,
- Erfassen,
- Organisation,
- Ordnen,
- Speicherung,
- Anpassung oder Veränderung,
- Auslesen,
- Abfragen,
- Verwendung,
- Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- Abgleich oder die Verknüpfung,
- Einschränkung,
- Löschen oder Vernichtung.

3.3.2 Art der Verarbeitung

Unter der Art der Daten sind die einzelnen Datenkategorien zu verstehen[10]. Grundlegend ist hierbei zwischen der Verarbeitung personenbezogener Daten entsprechend Art. 6 DS-GVO und der Verarbeitung besonderer Kategorien gemäß Art. 9 Abs. 1 DS-GVO zu unterscheiden. Der Verantwortliche hat zu prüfen, welcher Datenkategorien die zu verarbeitenden Daten zuzuordnen sind, da sich hieraus auch unterschiedliche Bewertungen hinsichtlich des Risikos der Verarbeitung ergeben können.

Beispiele für die Darstellung der Datenarten sind insbesondere

1. Identifizierende Daten
    a. Sozialversicherungsnummer
    b. Personalausweisnummer
    c. Reisepassnummer
    d. Führerschein-ID
    e. Kreditkartennummer
    f. Krankenversicherungsnummer
    g. Patient-ID aus Informationssystem (benennen welches)
    h. Andere (spezifizieren)
2. Stammdaten
    a. Name/Vorname
    b. Geburtsname
    c. Geburtsdatum
    d. Geburtsort
    e. Geschlecht

[10] Jandt S. Art 32 Rn. 12 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702129

f. Alter
g. Religionszugehörigkeit
h. Anschrift
i. Kontaktdaten (Telefon, Fax, E-Mail, …)
j. Ethnische Zugehörigkeit
k. Ausbildung
l. Titel
m. Krankenkasse
n. Andere (spezifizieren)

3. Beschäftigtendaten
    a. Gelernte(r) Beruf(e)
    b. Ausgeübter Beruf
    c. Job-Beschreibung
    d. Dienstliche Anschrift
    e. Dienstliche Kontaktdaten (Telefon, Fax, E-Mail, …)
    f. Gehalt/Vergütung
    g. Bisheriges Arbeitsleben (bisherige Arbeit- bzw. Auftraggeber, …)
    h. Zugehörigkeit zu Berufsverbänden oder anderen Organisationen
    i. Andere (spezifizieren)
4. Biometrische Daten
    a. Fingerprint
    b. Handflächen-Scan
    c. Stimmerkennung
    d. Fotos (Gesicht)
    e. Besondere Kennzeichen (Narben, Tätowierungen, …)
    f. Gefäß-Scan
    g. Retina/Iris-Scan
    h. DNA-Profil
    i. Andere (spezifizieren)
5. Administrative Daten
    a. User-ID
    b. IP-Adresse
    c. Datum/Uhrzeit von Zugriffen (An-/abmelden vom System, Zugriff auf bestimmte Daten)
6. Gesundheitsdaten
    a. Physiologische Auffälligkeiten
    b. Allgemeine Gesundheitsdaten (z. B. von Fitness-Trackern)
    c. Klinische Informationen

3.3.3 Umfang der Verarbeitung

Aus ErwGr. 75 bzw. 91 wird ersichtlich, dass im Bereich des „Umfangs der Datenverarbeitung“ zwei Einflussgrößen zu berücksichtigen sind: Zum einen die Anzahl der Personen, zum anderen die Menge der verarbeiteten Daten. Daraus folgt zum einen, dass je mehr Daten zu einer Person vorhanden sind, desto weitreichendere Aussagen sind über eine bestimmte Person möglich, wodurch sich das Risiko für diese Person erhöht. Zum anderen folgt daraus, dass je höher die Anzahl der betroffenen Personen ist, deren Daten verarbeitet werden, desto bessere/genauere Aussagen sind möglich z. B. über etwaige Verbindungen zwischen diesen Personen. Aus diesen Verbindungen lassen sich

wiederum weitere, möglicherweise für die Personen negative Schlüsse ziehen, sodass sich daraus wiederum höhere Risiken für die betroffenen Personen ergeben. Zugleich erhöht sich mit einem größeren Verarbeitungsumfang auch die Eintrittswahrscheinlichkeit etwaiger Risiken[11].

In der Fassung der DS-GVO vom europäischen Parlament war in dem ErwGr. 63 und 75 und auch im Art. 32a („Risk analysis“) von der Verarbeitung der Daten von 5000 betroffenen Personen innerhalb von 12 Monaten die Rede[12]. Auch wenn dieser Ansatz nicht in der finalen Version des DS-GVO Einzug fand, bietet dieser Wortlaut einen Hinweis, was sich der europäische Gesetzgeber unter einer großen Anzahl von betroffenen Personen vorstellte.

3.3.4 Umstände der Verarbeitung

Bei den Umständen der Verarbeitung ist zunächst einmal zu unterscheiden, wer den Nutzen der Verarbeitung hat: werden Gesundheitsdaten im Rahmen einer Heilbehandlung verwendet, dient die Verarbeitung der Daten in erster Linie dem Wohl des Patienten, in zweiter Linie der Abrechnung der erbrachten Leistung, was letztlich auch im Sinne des Patienten liegt.

Werden Gesundheitsdaten für die Zwecke anderer verarbeitet, z. B. für Pharmaforschung oder für Statistiken, damit Krankenkassen ihre Beiträge anpassen können, so ist der Profiteur nicht die betroffene Person, ggf. hat die betroffene Person bei Kenntnis aller Informationen sogar ein Interesse daran, dass eine Verarbeitung nicht stattfindet, z. B., wenn dadurch ihre Krankenkassenbeiträge steigen.

3.3.5 Zwecke der Verarbeitung

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[13]. Daraus folgt zwangsläufig auch, dass ein unzulässiger Zweck wie beispielsweise eine unverhältnismäßige Datenverarbeitung nicht die Verarbeitungsbefugnisse des Verantwortlichen erweitern kann[13].

Die Norm DIN CEN ISO/TS 14265 „Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen“[14] bietet einen Anhalt, wie der Zweck der Verarbeitung entsprechend dem Stand der Technik (im Sinne der Anwendung dieser Norm) klassifiziert werden kann.

3.4 Eintrittswahrscheinlichkeit und Schwere des Risikos

Die DS-GVO definiert nicht den Begriff „Risiko“. ErwGr. 75 führt aus, dass „aus einer Verarbeitung personenbezogener Daten“ Risiken für die Rechte und Freiheiten natürlicher Personen „mit

[11] 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

[12] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). Online, zitiert am 2017-09-04; Verfügbar unter http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212#BKMD-6

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

[14] DIN CEN ISO/TS 14265; Medizinische Informatik - Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen. Online, zitiert am 2017-09-04; Verfügbar unter https://www.beuth.de/de/technische-regel/din-cen-iso-ts-14265/149023541

unterschiedlicher Eintrittswahrscheinlichkeit und Schwere“ resultieren können, „die zu einem physischen, materiellen oder immateriellen Schaden führen“ können. Daraus folgt, dass die Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne des Art. 35 DS-GVO somit in Abhängigkeit der beiden Größen „Eintrittswahrscheinlichkeit“ und „Schadensschwere“ darzustellen sind[15].

3.4.1 Identifizierung der Risiken

In der DS-GVO geht es darum, den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger von der Verarbeitung betroffener Menschen Rechnung zu tragen. Entsprechend adressiert Art. 32 DS-GVO mit seinen Anforderungen die Risiken für die betroffenen Personen, Risiken für das datenverarbeitende Unternehmen sind nur relevant, wenn diese zugleich auch Risiken für die von der Verarbeitung betroffenen Personen darstellen.

Eine Kategorisierung der Risiken für die Rechte und berechtigten Interessen betroffener Personen bei einer Verarbeitung personenbezogener Daten können z. B. sein[16]:

- Strukturelle Risiken, beispielsweise gesellschaftlich-politische Risiken (wie z. B. die Informationsmacht, die gegenüber einem Individuum gewonnen wird) oder wirtschaftliche Risiken
- Individuelle Risiken, wie z. B. die Erhöhung individueller Verletzlichkeit für Straftaten, da jemand erfährt, wo betroffene Personen angreifbar sind
- Risiken für Gesellschaft und Individuum, z. B. durch Bildung von Persönlichkeitsprofilen oder Fremdbestimmung oder auch die Enttäuschung von Vertraulichkeitserwartungen.

Dabei müssen neben aus früheren Erfahrungen gewonnenen Erkenntnissen (d. h. in der Vergangenheit eingetretene Ereignisse) ableitbaren Risiken gemäß Art. 35 DS-GVO ebenso „voraussichtliche“ Risiken betrachtet werden. Hierzu gibt es verschiedene Methoden, mit denen sich die entsprechenden Risiken identifizieren lassen. Zu den bekanntesten zählen sicherlich:

- Die Expertenkonsultation, z.B. in Form von
    - Brainstorming
    - Interviews (strukturiert/semistrukturiert)
    - Delphi-Methode[17]
- Szenario-Analysen, bei welchem in Szenarien der geplante Ablauf durchgespielt wird und dabei festgestellte potentielle Ereignisse, welche zu einem Sicherheitsvorfall führen könnten, erfasst werden.
- Business Impact Analysen als Sonderform der Expertenkonsultation: es werden kritische Geschäftsprozesse sowie entsprechende Ressourcen betrachtet, die Abhängigkeiten dargestellt und überlegt, welche Auswirkungen ein Ereignis auf diese kritischen Geschäftsprozesse/Ressourcen hat.
- Die Ursachenanalyse, bei welcher tatsächliche Sicherheitsvorfälle untersucht werden und dargestellt wird, wie es zu diesen Sicherheitsvorfällen kommen konnte.

Dabei wird eine objektive (ErwGr. 76) Bewertung bzgl. des Risikos verlangt. Die Richtigkeit der Bewertung kann von unabhängigen Stellen – insbesondere auch von der zuständigen Datenschutz-

[15] 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

[16] Stefan Drackert (2014) Die Risiken der Verarbeitung personenbezogener Daten - Eine Untersuchung zu den Grundlagen des Datenschutzrechts. Duncker & Humblot GmbH. ISBN '978-3-428-1 4730-4

Aufsichtsbehörde – überprüft werden, ggf. muss die Bewertung einer gerichtlichen Prüfung standhalten. Der Verarbeiter muss sich bewusst sein, dass die DS-GVO den Spielraum bzgl. der Bewertung des Risikos nicht bei ihm sieht. Vielmehr ist eine nachvollziehbare Bewertung des Risikos aufgrund der Berücksichtigung der relevanten und überprüfbaren Risikofaktoren aus objektiver Sicht der betroffenen Person(en) erforderlich.

Dies bedeutet jedoch nicht, dass später eintretende Tatsachen oder nicht vorhersehbare Entwicklungen die Richtigkeit der Bewertung nachträglich verändern. Für die Beurteilung bzgl. der Bewertung ist einzig und allein relevant, dass zum Zeitpunkt der Erstellung eine Analyse der zu diesem Zeitpunkt vorhandenen Informationen erfolgte. Bei geänderter Informationslage muss jedoch ggf. die Datenschutz-Folgenabschätzung angepasst oder auch neu durchgeführt werden.

ErwGr. 75 führt beispielhaft einige Risiken auf, die bei einer Verarbeitung personenbezogener Daten zu berücksichtigen sind:

Risiko	Mögliche Folgen für die betroffenen Personen
– Diskriminierung – Identitätsdiebstahl – Identitätsbetrug – Finanziellen Verlust – Rufschädigung – Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten – Unbefugte Aufhebung der Pseudonymisierung – Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteilen	– Betroffene Personen werden um ihre Rechte und Freiheiten gebracht – Betroffene Personen werden daran gehindert, die sie betreffenden personenbezogenen Daten zu kontrollieren – Verarbeitung besonderer Kategorien von Daten, d. h. Daten bzgl. • Rassischer oder ethnischer Herkunft, • Politische Meinungen • Religiöse oder weltanschauliche Überzeugungen • Zugehörigkeit zu einer Gewerkschaft • Genetische Daten • Gesundheitsdaten • Sexualleben • Strafrechtliche Verurteilungen und Straftaten – Bewertung persönliche Aspekte, insbesondere Daten betreffend • Arbeitsleistung • Wirtschaftlicher Lage • Gesundheit • Persönliche Vorlieben oder Interessen • Zuverlässigkeit • Verhalten • Aufenthaltsort • Ortswechsel – Verarbeitung von Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern – Großer Verarbeitungsumfang • Große Menge personenbezogener Daten betreffend • Große Anzahl von betroffenen Personen betreffend

ErwGr. 83 benennt ebenfalls verschiedene Risiken, die berücksichtigt werden sollen:

- Vernichtung personenbezogener Daten
- Verlust personenbezogener Daten
- Veränderung personenbezogener Daten
- Unbefugte Offenlegung personenbezogener Daten bzw. unbefugter Zugang zu personenbezogenen Daten,

insbesondere, wenn diese zu einem physischen, materiellen oder immateriellen Schaden führen können.

Entsprechend ErwGr. 83 ist es unerheblich, ob die Risiken aus einer beabsichtigten, einer unbeabsichtigten oder auch einer unrechtmäßigen Handlung resultieren.

Die Risiken für die betroffenen Personen können aus Sicht der IT-Sicherheit i. d. R. auf drei Fälle eingegrenzt werden:

1. Unbefugte erhalten Zugriff auf die Informationen.
2. Informationen erfahren eine unerwünschte Änderung.
   2.1. Dies geschieht ungewollt durch einen Anwender, dem entsprechend Rechte zugewiesen wurde (z. B. Fehlbedienung oder Unachtsamkeit).
   2.2. Dies geschieht durch einen Angreifer, der sich entsprechende Rechte verschaffte.
3. Informationen werden vernichtet.
   3.1. Dies geschieht ungewollt durch einen Anwender, dem entsprechende Rechte zugewiesen wurden (z. B. Fehlbedienung oder Unachtsamkeit).
   3.2. Dies geschieht durch einen Angreifer, der sich entsprechende Rechte verschaffte.

3.4.2 Quantifizierung der Risiken

Eine Quantifizierung erkannter Risiken kann u. a. durch die nachfolgend vorgestellten Ansätze erfolgen:

1. Experten-Befragung: Mit Hilfe von meist strukturierten Fragebögen wird versucht, IT-Sicherheitsrisiken zu identifizieren und zu quantifizieren. Hierzu bieten sich zum einen strukturierte oder semstrukturierte Interviews an, zum anderen kann die Delphi-Methode[17] eingesetzt werden.
2. Indikator-Ansatz: Anhand bestimmter Kennzahl bzw. eines Kennzahlensystems werden vorliegende IT-Sicherheitsrisiken indirekt ermittelt.
3. Stochastische Methoden: Basierend auf historischen Schadensdaten bzgl. der Häufigkeit und Schwere von eingetretenen Schäden werden statistische Verteilungsfunktionen zur Simulation genutzt, um so die das Eintreten künftiger IT-Sicherheitsrisiken abzuschätzen.
4. Kausal-Methoden: Zwischen den identifizierten Risikoquellen bzw. -treibern und den daraus resultierenden Schäden werden mittels statistischer Methoden Zusammenhänge dargestellt.
5. Rechtsnormanalyse: Risiken können sich aus Verträgen, AGBs und Vereinbarungen sowie aus den gesetzesrechtlichen Rahmenbedingungen (EU-Verordnungen, EU-Richtlinien,

[17] Zur Beschreibung er Delphi Methode siehe z. B.

- Gabler Wirtschaftslexikon: Delphi-Technik. Online, zitiert am 2017-09-06; Verfügbar unter http://wirtschaftslexikon.gabler.de/Definition/delphi-technik.html
- Universität Augsburg, Bereich Qualitative Sozialforschung: Delphi-Studie. Online, zitiert am 2017-09-06; Verfügbar unter http://qsf.e-learning.imb-uni-augsburg.de/node/542
- Wikipedia: Delphi-Methode. Online, zitiert am 2017-09-06; Verfügbar unter https://de.wikipedia.org/wiki/Delphi-Methode

Bundesgesetze, Bundesverordnungen, Ländergesetze, länderspezifische Verordnungen, aktuelle Rechtsprechung) ergeben. Die Quantifizierung richtet sich bei dieser Methode nach dem Strafmaß wie z. B. den Bußgeldern.

Aufgrund der Tatsache, dass die Risiken der informationstechnischen Daten-Verarbeitung i. d. R. nur abgeschätzt werden können, eignet sich zur Quantifizierung ein Skalenniveau wie bspw.

Bewertung	Kriterien	Geschätzte Kosten
Katastrophal	Keine Kontrolle möglich	> 1 Mill. €
Kritisch	Gravierende Mängel / Schäden	≤ 1. Mill. €
Mittelmäßige Auswirkungen	Beträchtliche Abweichungen vom Soll	50 – 100.000 €
Geringe Auswirkungen	Geringe Folgen	< 50.000 €
Vernachlässigbare Auswirkungen	Unbedeutende Folgen	Keine

3.4.3 Eintrittswahrscheinlichkeit der Risiken

Die Eintrittswahrscheinlichkeit kann wie folgt klassifiziert werden:

Hoch	Tritt wahrscheinlich auf, oft, häufig
Mittel	Kann auftreten, jedoch nicht häufig
Niedrig	Unwahrscheinliches Auftreten, selten, fernliegend

Bei der Berücksichtigung der Frage der Eintrittswahrscheinlichkeit werden zu deren Beantwortung oftmals Erfahrungswerte aus der Vergangenheit herangezogen. Hierbei reicht ein Hinweis wie „ein derartiges Vorkommnis gab es in der Vergangenheit nicht, daher niedrig“ nicht aus, um den Anforderungen der DS-GVO hinsichtlich der Nachvollziehbarkeit zu genügen. Hier muss immer auch dargestellt werden, was unternommen wurde, um derartige Ereignisse festzustellen. Dazu gehört die Beantwortung von Fragen wie beispielsweise:

- Erfolgte eine Klassifizierung der Daten hinsichtlich des Schutzbedarfs?
- Wurde ein Intrusion Detection System eingesetzt?
  Wenn ja:
  - Auf welche Ereignisse in Bezug auf die Fragestellung „unbefugte Offenbarung personenbezogener Daten“ reagiert es?
  - Wie sind die Meldewege für entsprechende Vorfälle?
- Werden Zugriffe auf personenbezogene Daten protokolliert?
  Wenn ja:
  - Gibt es ein Protokollierungskonzept?
  - Wie erfolgt die Protokollierung von Zugriffen auf personenbezogene Daten?
  - Erfolgt eine Auswertung der Protokolle? Wenn ja: Welche Ereignisse werden ausgewertet?

Weiterhin ist zu beachten, dass auch die Verwertbarkeit von entsprechenden Ereignissen in anderen Ländern nur bedingt gegeben ist. Gesundheitsdaten in den USA beinhalten i. d. R. alle Daten, welche kriminelle Personen für einen Identitätsdiebstahl und den damit verbundenen Möglichkeiten z. B. zur Erlangung von Kreditkarten, Führerschein usw. benötigen. Dies ist in Deutschland nicht der Fall, daher ist zwangsläufig die Motivation in den USA eine andere als in Deutschland, die Eintrittswahrscheinlichkeit von dem einen Land auf das andere Land daher eher nicht übertragbar.

3.4.4 Größe der Risiken

Die DS-GVO gibt nicht an, wann das Risiko einer Verarbeitung „hoch“ ist. Ein Risiko ist zumindest dann als „hoch“ einzustufen, wenn mit „hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten natürlicher Personen“ anzunehmen ist.[18] Eine hohe Wahrscheinlichkeit kann sowohl aus einer hohen Eintrittswahrscheinlichkeit (des Schadens) als auch aus einem hohen Schaden resultieren. Daneben ergibt sich aus ErwGr. 91, dass insbesondere die Sensibilität der Daten die Wahrscheinlichkeit eines „hohen“ Risikos vermuten lässt.

ErwGr. 75 führt weiter aus, dass von entsprechenden 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. Aber auch, wenn personenbezogene Daten verarbeitet werden, die zu den besonderen Kategorien von Daten entsprechend Art. 9 DS-GVO gehören, muss von hohen Risiken ausgegangen werden.

Bei der Verarbeitung sensibler Daten wie Gesundheitsdaten oder genetischen Daten ist immer von einem hohen Risiko und dementsprechend von einem hohen Schutzbedarf auszugehen.[19]

3.5 Geeignetheit und Angemessenheit der Schutzmaßnahmen

Die von Art. 32 DS-GVO geforderte Geeignetheit der technischen und organisatorischen Maßnahmen bezieht sich auf die Umsetzung von dessen Zielen, also auf die Gewährleistung der Sicherheit der Verarbeitung als auch der Vorbeugung einer nicht den Anforderungen der DS-GVO genügenden Verarbeitung[20]. Die Forderung nach Angemessenheit der Schutzmaßnahmen verweist darauf, dass ein Risiko nicht völlig ausgeschlossen werden kann und dies auch nicht Ziel der Maßnahmen ist[21].

Bzgl. der Beurteilung der Angemessenheit des Schutzniveaus muss entsprechend ErwGr. 83 insbesondere berücksichtigt werden, ob ein Sicherheitsproblem zu einem „physischen, materiellen oder immateriellen Schaden“ führen kann. Beispiele hierzu werden in ErwGr. 75 genannt (siehe auch Kapitel 3.4.1). Letztlich ist eine umfassende Interessenabwägung erforderlich, wobei die Abwägung

[18] 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

[19] Siehe z.B.

- Grages JM. Art. 32 Rn. 10 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

[20] Piltz C. Art. 32 Rn. 10 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

[21] Schreibauer M, Spittka J. Art. 32 Rn. 16 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0

gemäß ErwGr. 76 objektiv zu erfolgen hat[22]. Damit verbunden ist insbesondere, dass individuelle, nur auf einzelne Personen zutreffende Sachverhalte, ggf. nicht berücksichtigt werden (müssen), wenn diese die Mehrzahl der von der Verarbeitung betroffenen Personen nicht betreffen[22].

In den Ingenieurswissenschaften ist die „Fehlermöglichkeits- und –einflussanalyse“ („Failure Mode and Effects Analysis, FMEA)[23] eine anerkannte analytische Methode um Fehler, deren Auftretens- und Entdeckungswahrscheinlichkeit sowie deren Beeinflussbarkeit nachvollziehbar darzustellen. Eine FMEA zielt darauf, Fehler von vornherein zu vermeiden, statt sie nachträglich zu entdecken und zu korrigieren. Damit entspricht sie dem risiko-orientierten Ansatz der DS-GVO.

Sofern eine entsprechend Art. 35 DS-GVO durchgeführte Datenschutz-Folgenabschätzung vorhanden ist, bietet deren Ergebniss natürlich eine sehr gute Ausgangslage zur Beurteilung der Angemessenheit des Schutzniveaus. Im Umkehrschluss empfiehlt sich die Durchführung einer Datenschutz-Folgenabschätzung, wenn sich der Verantwortliche bzgl. der Angemessenheit des Schutzniveaus nicht sicher ist.

Grundsätzlich ist zu beachten, dass Art. 32 DS-GVO nicht die Einhaltung des Stands der Technik verlangt, sondern deren Berücksichtigung bei der Beurteilung der Angemessenheit der getroffenen Schutzmaßnahmen.

4 Anforderungen bzgl. Sicherheit der Verarbeitung

4.1 Pseudonymisierung

4.1.1 Was bedeutet Pseudonym?

Art. 4 Abs. 5 definiert Pseudonymisierung als „die Verarbeitung personenbezogener Daten in einer Weise, dass

- die personenbezogenen *Daten ohne Hinzuziehung zusätzlicher Informationen* **nicht mehr einer spezifischen betroffenen Person zugeordnet werden können**,
- sofern diese zusätzlichen Informationen gesondert aufbewahrt werden
- und technischen und organisatorischen Maßnahmen unterliegen,
- die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

Aus der in der DS-GVO enthaltenen Begriffsbestimmung lassen sich somit verschiedene implizit enthaltene Feststellungen ableiten:

a) Pseudonyme Daten stellen gemäß Art. 4 Abs. 1 personenbezogene oder personenbeziehbare Daten dar, da eine grundsätzliche Möglichkeit zur Identifikation der Person besteht.

[22] Grages JM. Art. 32 Rn. 10 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

[23] Weitere Informationen zur FMEA z. B. bei

- Deutsche Gesellschaft für Qualität (DGQ): FMEA – Fehlermöglichkeits- und Einflussanalyse. 5. Auflage 2012. ISBN/Best.-Nr.: 3-410-32333-3. Online, zitiert am 2017-09-08; Verfügbar unter https://www.dgq.de/produkte/fmea-fehlermoeglichkeits-und-einflussanalyse/
- QZ-online.de: Grundlagen der Fehlermöglichkeits- und Einfluss-Analyse. Online, zitiert am 2017-09-08; Verfügbar unter https://www.qz-online.de/qualitaets-management/qm-basics/methoden/fmea/artikel/grundlagen-der-fehlermoeglichkeits-und-einfluss-analyse-903982.html
- Quality Services & Wissen GmbH: FMEA – Fehlermöglichkeits und Einflussanalyse. Online, zitiert am 2017-09-08; Verfügbar unter https://www.quality.de/fmea-fehlermoeglichkeits-einflussanalyse/

b) Der Vorgang der Pseudonymisierung stellt eine Verarbeitung im Sinne von Art. 4 Abs. 2 dar, somit gelten für eine Pseudonymisierung alle Vorgaben bzgl. der Verarbeitung, insbesondere die Vorgaben von Art. 5 und Art. 6 bzw. Art. 9. D. h. auch bei einer Pseudonymisierung der Daten muss immer die Rechtmäßigkeit der Verarbeitung gewährleistet sein. Insbesondere muss bei der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 ein Erlaubnistatbestand zur Pseudonymisierung vorhanden sein.
c) Pseudonyme Daten gelten nur dann als pseudonym, wenn der die Daten Verarbeitende keine Möglichkeit hat, die Zuordnungsvorschrift zwischen Pseudonym und Personenkennung zu erhalten und eine „De-Pseudonymisierung" mittels dieser Liste vornehmen kann.

Pseudonymisierte Daten sind nicht mit anonymisierten Daten gleichzusetzen[24]. D. h., dass für pseudonymisierte Daten alle Anforderungen der DS-GVO gelten. Pseudonymisierung verringert lediglich die Verknüpfbarkeit eines Datenbestands mit der wahren Identität einer betroffenen Person. Somit stellt eine Pseudonymisierung eine sinnvolle Sicherheitsmaßnahme dar.

4.1.2 Arten von Pseudonymen

Es gibt verschiedene Arten von Pseudonymen. Grundsätzlich werden Personen- und Rollenpseudonyme unterschieden:

- Personenpseudonyme
  - Öffentliches Personenpseudonym wie z. B. eine einer natürlichen Person zugewiesene Telefonnummer
  - Nichtöffentliches Personenpseudonym wie z. b. die Nummer eines Kontos bei einer Bank
  - Anonymes Personenpseudonym, wie es z. B. das eigene Genom darstellt
- Rollenpseudonyme
  - Geschäftsbeziehungspseudonym, dies kann z. B. ein Chat-Name sein
  - Transaktionspseudonym wie beispielsweise eine PIN oder eine TAN, wie sie für Bankgeschäfte verwendet werden.

Weiterhin können Pseudonyme entsprechend dem Inhaber der Zuordnungsregel gruppiert werden:

- Pseudonyme werden ausschließlich vom Betroffenen selbst vergeben, wie z. B. der Nickname im Chat.
- Pseudonyme werden von einem vertrauenswürdigen Dritten vergeben. Dies geschieht beispielsweise durch eine Thrusted-Third-Party in medizinischen Forschungsnetzen.
- Der ursprüngliche Dateiverwender vergibt das Pseudonym, hierzu wäre ein Beispiel die Vergabe einer IP-Adresse durch den Provider.

Ferner können Pseudonyme an Hand ihrer Erzeugungsart eingeteilt werden:

- Deterministische Erzeugung: Das Pseudonym wird durch eine schlüsselabhängige Einweg- oder Hashfunktion aus invarianten Daten (Bsp. Identitätsdaten) erzeugt.
- Willkürlich Erzeugung: Das Pseudonym wird nach einem festen Einweg-Algorithmus vom Benutzer aus einem Geheimnis (z. B. Passphrase) erzeugt.
- Zufällige Erzeugung: Das Pseudonym wird frei gewählt oder nach einem Zufallsverfahren erzeugt.

[24] Artikel-29-Datenschutzgruppe: Stellungnahme 5/2014 zu Anonymisierungstechniken. Online, zitiert am 2017-09-04; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

4.1.3 Güte einer Pseudonymisierung

Primäre Identifikationsmerkmale sind Attribute oder Attributkombinationen, die eine eindeutige Identifizierung einer Person erlauben. Sekundäre Identifikationsmerkmale sind Attribute, die durch die Kombination mit anderen Attributen und der Verbindung mit externen Informationen (Telefonbuch) unter Umständen eine eindeutige Identifizierung des Personenbezugs erlauben. Beispiele für primäre Identifikationsmerkmale sind: Name, Kontonummer, Personalnummer, Patienten-Identifikationsnummer oder auch die Mitgliedsnummer in einem Verein. Beispiele für sekundäre Identifikationsmerkmale sind seltene Berufe oder Erkrankungen, die gemeinsam mit einem Wohnort mit einer geringen Einwohnerzahl eine Re-Identifizierung ermöglichen.

Bei einer Pseudonymisierung sind grundsätzlich alle primären Identifikationsmerkmale zu bearbeiten, wenn eine einfache Re-Identifikationsmöglichkeit ausgeschlossen werden muss. Je höher der Schutzbedarf ist, desto mehr Wert muss auf die Identifizierung und Veränderung der sekundären Identifikationsmerkmale gelegt werden. Die Identifikation dieser Merkmale ist nicht immer einfach, Hinweise geben Merkmale, die sich gar nicht (z. B. Geburtsort oder Geburtsdatum) bzw. selten ändern (z. B. Wohnort oder Familienstand), aber auch ausgefallene Merkmale wie z. B. der Mann mit Brustkrebs.

Zur Abschätzung der Güte der Pseudonymisierung sind sowohl die primären als auch die sekundären Merkmale zu betrachten und an Hand der genutzten Pseudonymisierungsmethode das Restrisiko einer Re-Identifizierung abzuschätzen.

4.1.4 Methoden der Pseudonymisierung

Zur Pseudonymisierung personenbezogener Daten können verschiedene Methoden angewandt werden. Dabei lassen sich die eingesetzten Pseudonymisierungs-Verfahren auf die folgenden Methoden zurückführen:

- Nichtangabe: Bei dieser Methode wird das zu schützende Datum weggelassen, z. B. wird die Spalte mit dem Datum nicht exportiert oder nachträglich aus dem Export gelöscht.
- Maskierung: Hierbei werden die zu schützenden Daten mit einem konstanten oder sich ändernden Wert ersetzt. Beispiele hierfür sind der Austausch der letzten 2 Ziffern einer Postleitzahl durch zwei feste Werte wie z. B. „00“ oder der Ersatz aller Nachnamen durch die Angabe „Muster“.
- Shuffeling: Hierbei werden Datensätze miteinander vermischt, D. h. die in einem Datensatz enthaltenen Daten werden untereinander getauscht, z. B. erhält Person „b“ die Hausnummer von Person „A“. Dabei ist bei dieser Methode darauf zu achten, dass eindeutige Informationen (insbesondere alle primären Identifikationsmerkmale) wie z. B. eine Telefonnummer zusätzlich verfremdet werden müssen, da ansonsten der Personenbezug vorhanden bleibt. Weiterhin muss geprüft werden, ob das getauschte Datum mit dem ursprünglichen Datum übereinstimmt oder ob zufällig ein Austausch mit einem übereinstimmendem Datum stattfinden soll.
- Varianzen: Auf zahlen basierende Daten werden in festgelegten Streuungsintervallen verändert, wobei das Streuungsintervall zufällig erhöht oder verringert wird.
- Kryptographische Methoden: Durch den Einsatz von Verschlüsselungs- oder Hashalgorithmen wird verhindert, dass die ursprünglichen Daten einsehbar sind. Die Güte dieser Pseudonymisierung ist stark von der Güte der ausgewählten kryptographischen Verfahren abhängig, insbesondere von der Schlüssellänge bzw. von der Kollisionsresistenz der Hashmethode.

4.2 Verschlüsselung

Eine Verschlüsselung bedeutet einen zusätzlichen Schutz personenbezogener Daten. Dabei ist die Güte des Schutzes abhängig von der Güte der Verschlüsselungsalgorithmen. In „Technische Richtlinie 02102: Kryptographische Verfahren“[25] empfiehlt das BSI Algorithmen und Schlüssellängen, so dass hierdurch die Abschätzung des Schutzes personenbezogener Daten ermöglicht wird.

Bzgl. der Erzeugung von Signaturschlüsseln, Hashen zu signierender Daten oder Erzeugung/Prüfung elektronischer Signaturen finden sich Empfehlungen bei der Bundesnetzagentur[26], wobei diese Empfehlungen jährlich aktualisiert werden.

4.3 Gewährleistung Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

Die klassischen Schutzziele der Informationssicherheit werden oftmals durch das Kürzel „CIA“ dargestellt:

- Confidentiality (Vertraulichkeit)
- Integrity (Integrität)
- Availability (Verfügbarkeit).

Dieses klassische Trias der IT-Sicherheit wird durch die DS-GVO um die Anforderung „Belastbarkeit“ erweitert.

4.3.1 Vertraulichkeit der Systeme und Dienste

In der IT-Sicherheit wird von Vertraulichkeit gesprochen, wenn keine unautorisierte Informationsgewinnung möglich ist: Nur Personen, die dazu berechtigt sind, können von schützenswerten Daten Kenntnis nehmen.

Das Mittel der Wahl zur Gewährleistung des Schutzes der Informationsinhalte ist der Einsatz kryptographischer Methoden, d. h. der Verschlüsselung der Daten bzw. der Verschlüsselung der Übertragungsmethoden. Bei einer wirksamen Verschlüsselung können die verschlüsselten Informationen zwar weiterhin von einem unbefugten Dritten „abgefangen“ werden, jedoch bestehen keine Zugriffsmöglichkeiten auf die Inhalte, d. h. eine Offenbarung der Inhalte ist verhindert.

4.3.2 Integrität der Systeme und Dienste

Die Integrität beinhaltet sowohl die Richtigkeit der Daten („Datenintegrität“) als auch die ordnungsgemäße Funktionsweise des Systems („Systemintegrität“). Die Gewährleistung der Integrität schließt damit das Verhindern von nicht autorisierten Veränderungen an Informationen

[25] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie 02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Online, zitiert am 2017-09-04; Verfügbar unter (https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html. 4 Teile:

- BSI TR-02102-1: Bewertung der Sicherheit ausgewählter kryptographischer Verfahren, ermöglicht längerfristige Auswahl geeigneter Verfahren
- BSI TR-02102-2: Empfehlungen bzgl. Einsatz TLS
- BSI TR-02102-3: Empfehlungen bzgl. IPSec, und Internet Key Exchange
- BSI TR-02102-4: Empfehlungen bzgl. SSH

[26] Bundesnetzagentur: Auflistung geeigneter Algorithmen und Parameter. Online, zitiert am 2017-09-04; Verfügbar unter https://www.bundesnetzagentur.de/DE/Service-Funktionen/ElektronischeVertrauensdienste/QES/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen_node.html

oder Systemen ein. Eine „starke Integrität“ lässt keine Manipulationsmöglichkeiten zu, während eine „schwache Integrität“ Manipulationen zwar nicht verhindert, diese jedoch immer entdeckt werden.

4.3.3 Verfügbarkeit der Systeme und Dienste

Das Schutzziel Verfügbarkeit wird dann eingehalten, wenn gewährleistet ist, dass die Systeme jederzeit betriebsbereit sind und die Verarbeitung der Daten korrekt abläuft. Je nach konkreter Anforderung der Verfügbarkeit muss dabei dem Ausfall des gesamten IT-Systems oder auch nur eines Teilbereiches durch geeignete Maßnahmen vorgebeugt werden.

Berechnet wird die Zuverlässigkeit über das Verhältnis zur Zeit, in dem das System tatsächlich zur Verfügung stand und der vereinbarten Zeit, in dem das System zu Verfügung stehen sollte. Häufig werden die Verfügbarkeitszeiten in einem Service-Level-Agreement vereinbart.

4.3.4 Belastbarkeit der Systeme und Dienste

Die geforderte „Belastbarkeit der Systeme und Dienste“ ist kein klassisches Ziel der IT-Sicherheit. In der englischen Fassung findet sich der Begriff „resilience“, welcher in der deutschen Informatik-Fachliteratur i. d. R. mit „Widerstandsfähigkeit“ oder „Ausfallsicherheit“ übersetzt wird[27].

D. h. es handelt sich hierbei um eine funktionale Anforderung[28]. Mögliche Methoden zur Schaffung von Resilienz sind beispielsweise

- Verteilte Systeme
- Redundanzplanung
- Nutzung von adaptiven Systemen.

4.4 Recovery: Wiederherstellung der Verfügbarkeit und des Zugangs zu personenbezogenen Daten

In der IT-Sicherheit ist der Begriff des „IT Continuity Planning“, d.h. der Planung der Fortführung bzw. Wiederaufnahme der Geschäftsfähigkeit im Falle schwerer Störungen etabliert. Im Rahmen des IT Continuity Planning erfolgt auch eine Planung des Notfall-Recovery. Dabei beschreibt das Notfall-Recovery Konzept die Wiederherstellung des Regelbetriebs nach einem Notfallereignis („Disaster Recovery“).

Dabei adressiert die IT-Sicherheit die für ein Unternehmen relevanten Daten, d. h. die Daten und Prozesse, die aus Sicht des Unternehmens für die Wiederaufnahme der Geschäftsfähigkeit notwendig sind. Die datenschutzrechtliche Anforderung des Art. 32 DS-GVO adressiert als Schutzobjekt jedoch die betroffene Person: Welche Daten, Verarbeitungsvorgänge/Prozesse müssen wieder hergestellt werden, damit der von der Verarbeitung betroffenen Person kein Nachteil oder gar Schaden bei einem physischen oder technischen Zwischenfall entsteht?

---

[27] Siehe z. B.

- Schaumüller-Bichl I, Kolberger A (2016) Information Security RiskAnalysis in komplexen Systemen - neue Herausforderungen und Lösungsansätze. Online, zitiert am 2017-09-04; Verfügbar unter https://pdfs.semanticscholar.org/f72b/610fb2d1ae28ba22ec04d54a9b8f6635e565.pdf
- Wagner SM, Bode C. Empirische Untersuchung von SC-Risiken und SC-Risikomanagement in Deutschland. In: Vahrenkamp/ Siepermann (Hrsg.) Risikomanagement in Supply Chains: Gefahren abwehren, Chancen nutzen, Erfolg generieren. Erich Schmidt Verlag. 2007 ISBN 978-3503100415

Allgemeiner siehe auch Wikipedia: „Resilienz (Ingenieurwissenschaften)“. Online, zitiert am 2017-09-04; Verfügbar unter https://de.wikipedia.org/wiki/Resilienz_(Ingenieurwissenschaften)

[28] Jandt S. Art 32 Rn. 26 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702129

Die Verfahren zur Wiederherstellung bleiben dabei gleich, jedoch müssen ggf. andere Daten oder Prozesse zusätzlich berücksichtigt werden.

Die Norm fordert zudem eine „rasche“ Wiederherstellung. Naturgemäß kann eine nähere Eingrenzung nicht seitens des Normgebers vorgenommen werden, da der Wiederherstellungszeitraum zwangsläufig mit der Schwere des Zwischenfalls korrespondiert[29]. Je nachdem, ob bspw. die Infrastruktur wiederhergestellt werden muss (z.B. durch Brand zerstörte Räume), die Systemumgebung (z.B. Wiederherstellung eines Servers auf Grund eines Hardwaredefekts) neu aufgesetzt werden muss oder allein die Daten wiederhergestellt werden müssen – all dies hat Auswirkungen auf die benötigte Zeitdauer.

Mit „rasch“ ist vermutlich nicht die unverzügliche Wiederaufnahme „ohne schuldhaftes Verzögern“ gemeint, da ansonsten - wie an anderer Stelle auch – „unverzüglich“ als Anforderung verwendet worden wäre[30]. „Rasch“ dürfte daher eine größere Zeitspanne beinhalten, als die Forderung nach einer unverzüglichen Wiederherstellung (wobei aus Sicht des Unternehmens selbst natürlich unbenommen von der rechtlichen Vorgabe eine Notwendigkeit zum unverzüglichen Handeln bestehen kann.)

4.5 Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

Verantwortliche wie auch Auftragsverarbeiter müssen die Sicherheitsmaßnahmen nicht nur einmalig planen und umsetzen, sie müssen die Wirksamkeit dieser Maßnahmen regelmäßig überprüfen und ggf. die Maßnahmen anpassen[31] („Überprüfung, Bewertung und Evaluierung der Wirksamkeit“). Art. 32 Abs. 1 lit. d DS-GVO fordert vom Normadressaten letztlich die Etablierung eines Prozesses, der einen Demingkreis[32] bestehend aus den Komponenten „Plan – Do – Check – Act“ abbildet[33].

Dabei wird die „Regelmäßigkeit“ nicht vom Normgeber konkret vorgegeben, sondern muss vom jeweiligen Normadressaten entsprechend der jeweiligen Notwendigkeit festgelegt werden.

4.6 Verarbeitung personenbezogener Daten

Entsprechend Art. 32 Abs. 4 DS-GVO darf eine Verarbeitung personenbezogener Daten durch „unterstellte natürliche Personen“ nur **auf Weisung des Verantwortlichen** erfolgen. Dem Wortlaut zufolge gilt dies sowohl für Personen, die beim Verantwortlichen als auch beim Auftragsverarbeiter beschäftigt sind.

D. h. eine Weisung des Verantwortlichen muss auch für Beschäftigte des Auftragsverarbeiters existieren, eine alleinige Weisung des Auftragsverarbeiters reicht hier nicht aus[34, 35]. Entsprechende

[29] Jandt S. Art 32 Rn. 28 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702

[30] Piltz C. Art. 32 Rn. 33 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

[31] Jandt S. Art 32 Rn. 29 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702

[32] Wikipedia: Demingkreis. [Online, zitiert am 2017-09-25]; Verfügbar unter https://de.wikipedia.org/wiki/Demingkreis

[33] Piltz C. Art. 32 Rn. 37 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

[34] Grages JM. Art. 32 Rn. 13 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

Anweisungen des Auftragsverarbeiters müssen stets auf eine Weisung des Verantwortlichen rückführbar sein. Hier kann es sich als sinnvoll erweisen, entsprechend detaillierte Regelungen bzgl. Regelungen zur Erteilung entsprechender Einzelanweisungen aufzunehmen[36].

Eine Ausnahme von dieser Weisungspflicht durch den Verantwortlichen existiert nur, wenn die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten verpflichtend erfolgen muss.

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

Die nachfolgende Gegenüberstellung der von Art. 32 DS-GVO geforderten Maßnahmen mit den Maßnahmen bzw. Kontrollen aus der Anlage zu § 9 BDSG soll bei der Prüfung dahingehend unterstützen, wie bzw. wo die von der DS-GVO geforderten Maßnahmen möglicherweise schon heute, im Rahmen der Kontrollen der Anlage zu § 9 BDSG berücksichtigt wurden und wo ggf. noch Umsetzungs- oder Anpassungsbedarf besteht.

Art. 32 DS-GVO	Anlage zu § 9 BDSG
Art. 32 Abs. 1 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	-/-

[35] Piltz C. Art. 32 Rn. 50 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

[36] Siehe z.B. „Muster-Auftragsverarbeitungs-Vertrag für das Gesundheitswesen“, aktualisierte, der DS-GVO angepasste zweite Version, Stand 14.06. 2017. § 5 Weisungsbefugnis des Auftraggebers. Online, zitiert am 2016-07-12; Verfügbar unter http://ds-gvo.gesundheitsdatenschutz.org/html/adv-vertrag.php

Art. 32 DS-GVO	Anlage zu § 9 BDSG
Verarbeitung	

Die heute bekannten Maßnahmenkataloge können auch weiterhin als Leitlinien dienen[37], denn natürlich werden die bisher getroffenen Sicherheitsmaßnahmen unter der DS-GVO nicht obsolet. Allerdings ist darauf zu achten, dass die Maßnahmenkataloge auch nur die Maßnahmen enthalten, welche die entsprechende Verarbeitungssituation adressieren; eine Abarbeitung der Forderungen aus der Anlage zu § 9 BDSG ist allein schon unter dem Gesichtspunkt der erforderlichen europaweiten einheitlichen Auslegung der DS-GVO abzulehnen.

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[38]:

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

[37] Grages JM. Art. 32 Rn. 4 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

[38] 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

Schutzziel	Komponente	Maßnahmen
		Ansprechpartner für Änderungen/Löschungen, Change Management

5 Sanktionierung

Die DS-GVO selbst sanktioniert Verstöße gegen verschiedene Vorschriften der DS-GVO mit Bußgeldern. Die zu verhängenden Bußgelder sind verwaltungsrechtlicher Art und können von den jeweils zuständigen Aufsichtsbehörden verhängt werden. Dabei gibt es das „kleine“ Bußgeld mit Geldbußen von bis zu 10.000.000 Euro oder – sofern dies einen höheren Betrag darstellt - im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs. Darüber hinaus sieht die DS-GVO auch ein „großes“ Bußgeld mit Geldbußen von bis zu 20.000.000 Euro oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs vor, je nachdem, welcher der Beträge höher ist.

Werden die Vorgaben aus Art. 32 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:

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)? [39]
Etwaige einschlägige frühere Verstöße (Art. 83 Abs. 2 lit. e)	Handelt es sich um einen Wiederholungstatbestand?

[39] Popp in Sydow, Europäische Datenschutzgrund-Verordnung, Handkommentar 2017, Art. 83 Rn. 14, Nomos Kommentar, ISBN978-3-8487-1782-8.

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?

Es ist nicht damit zu rechnen, dass ein Verantwortlicher bei einem ersten Vergehen, welches auch nur darin bestehen kann, einem einzelnen Betroffenen sein Recht verweigert zu haben, die Höchststrafe angesetzt wird. Allerdings muss die Aufsichtsbehörde bei der Verhängung der Höhe des Bußgeldes auch bedenken, dass der europäische Gesetzgeber hier bewusst die höhere Version des Bußgeldes anordnete und nicht den kleineren Betrag aus Art. 83 Abs. 4 DS-GVO.

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.

6 Abkürzungen

Abs.	Absatz
ALE	Annual Loss Expectancy
Art.	Artikel
Artt.	Artikel (Mehrzahl)
BDSG	Bundesdatenschutzgesetz
BDSG n.F.	Bundesdatenschutzgesetz, gültig ab 25. Mai 2018 (Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEN	Europäische Komitee für Normung (franz. Comité Européen de Normalisation; engl. European Committee for Standardization)
DIN	Deutsche Institut für Normung e. V.
DSB	Datenschutzbeauftragter
DS-GVO	Datenschutz-Grundverordnung
EG	Europäische Gemeinschaft
ErwGr.	Erwägungsgrund
EU	Europäische Union
ISO	International Organization for Standardization
Lit.	Literal
RL	Richtlinie
Rn.	Randnote, -nummer, -zahl, -ziffer
RoSI	Return on Security Investment
TCO	Total Cost of Ownership
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOM	Technische und organisatorische Maßnahmen
TR	Technische Richtlinie
TS	Technical Specification(s)
WP	Working Paper
Ziff.	Ziffer

7 Glossar

Automatische Verarbeitung	Verarbeitung unter Nutzung von EDV; also z.B. Word- oder Excel-Datei, aber auch KIS, RIS, PACS, unabhängig ob Client-Server-Lösung oder Stand-alone PC, Tablet oder anderweitige Hardware genutzt wird
Betroffener	Genau genommen „betroffene Person“, in der gesamten Literatur aber als "Betroffener" aufgeführt; Art. 4 Ziff. 1 DS-GVO „’Personenbezogene Daten’ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“
Datei	Im informationstechnischem Sinn: Gruppe von gespeicherten oder als eine Einheit bearbeiteten Aufzeichnungen (Quelle: ISO/IEC 2382:2015)
Daten/Datum	Im Informationstechnischem Sinn: Die re-interpretierbare Darstellung von Information in einer formalisierten für Kommunikation, Interpretation, oder Bearbeitung geeigneten Weise (Quelle: ISO/IEC 2382:2015)
Datenschutzverletzung	Situation, in der Daten einer Person auf illegale Weise oder unter Verletzung einer oder mehrerer relevanter Datenschutzbestimmungen verarbeitet wurde (Quelle: DIN CEN ISO/TS 14265)
Genetische Daten	Art. 4 Ziff. 13 DS-GVO „’Genetische Daten’ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden“
Gesundheitsdaten	Art. 4 Ziff. 15 DS-GVO „’Gesundheitsdaten’ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“
Integrität	Eigenschaft, die bedingt, dass die Information in keiner Weise, weder absichtlich noch unabsichtlich, geändert wird (Quelle: DIN EN ISO 22600-2) Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten (Quelle: DIN ISO/IEC 27000)
Kryptographie	Disziplin, die Grundsätze, Mittel und Verfahren für die Umwandlung von Daten mit dem Ziel verkörpert, deren Informationsgehalt zu verbergen und ihre unerkannte Änderung und/oder nicht autorisierte Nutzung zu verhindern

	(Quelle: DIN EN ISO 22600-3)
Maßnahme	Mittel zum Management von Risiken, einschließlich von Leitlinien, Verfahren, Richtlinien, Methoden oder Organisationsstrukturen, die verwaltender, technischer, leitender oder gesetzlicher Natur sein können (Quelle: DIN ISO/IEC 27000)
Normadressat	Rechtssubjekt (z.B. natürliche Person, juristische Person, Personenvereinigung), an die sich die Regelung eines Gesetzes (= einer Norm) richtet
Offenlegung	Preisgabe von Daten an Personen, die nicht routinemäßig über die entsprechende Berechtigung verfügen (Quelle: DIN CEN ISO/TS 14265)
Restrisiko	nach der Risikobehandlung verbleibende Risiko (Quelle: DIN ISO IEC 27001)
Risiko	Kombination aus der (Eintritts-) Wahrscheinlichkeit eines Ereignisses und dessen Auswirkungen (Quelle: DIN ISO IEC 27000)
Risikoakzeptanz	Entscheidung, ein Risiko zu akzeptieren (Quelle: DIN ISO/IEC 27000)
Risikoanalyse	Systematischer Gebrauch von Informationen zur Identifizierung von Risikoquellen und zur Abschätzung des Risikos (Quelle: DIN ISO/IEC 27000)
Risikobehandlung	Prozess der Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos (Quelle: DIN ISO/IEC 27000)
Risikobestimmung	Tätigkeit, bei der der Wahrscheinlichkeit und den Auswirkungen eines Risikos Werte zugeordnet werden (Quelle: DIN ISO/IEC 27000)
Risikobewertung	Prozess, in dem das eingeschätzte Risiko mit den festgelegten Risikokriterien verglichen wird, um die Bedeutung des Risikos zu bestimmen (Quelle: DIN ISO/IEC 27000)
Risikoeinschätzung	Gesamter Prozess der Risikoanalyse und Risikobewertung (Quelle: DIN ISO/IEC 27000)
Risikokommunikation	Austausch oder gemeinsame Nutzung von Informationen über Risiken zwischen Entscheidungsträgern und anderen Stakeholdern (Quelle: DIN ISO/IEC 27000)
Risikokriterien	Bezugsrahmen für die Einschätzung der Bedeutung eines Risikos (Quelle: DIN ISO/IEC 27000)
Risikomanagement	Koordinierte Tätigkeit zur Leitung und Kontrolle einer Institution/Organisation in Bezug auf Risiken (Quelle: DIN ISO/IEC 27000)
Schwachstelle	Schwäche eines Werts oder einer Maßnahme, die von einer Bedrohung ausgenutzt werden kann (Quelle: DIN ISO/IEC 27000)
Sicherheit	Kombination von Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit (Quelle: DIN EN ISO 22600-1)
Verantwortlicher	Art. 4 Ziff. 7 DS-GVO „'Verantwortlicher' 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“
Verarbeitung	Art. 4 Ziff. 2 DS-GVO „’Verarbeitung’ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“
Verfahren	festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen (Quelle: DIN ISO IEC 27000)
Verfügbarkeit	Eigenschaft, auf Anforderung einer autorisierten Entität zugänglich und nutzbar zu sein (Quelle: DIN EN ISO 22600-1)
Vertrauen	im Allgemeinen kann davon ausgegangen werden, dass eine Entität einer anderen Entität „vertraut“, wenn sie annehmen kann, dass sich die zweite Entität genauso, wie von der ersten Entität erwartet, verhalten wird (Quelle: DIN EN ISO 22600-2)
Vertraulichkeit	Eigenschaft, die dazu führt, dass die betreffende(n) Information(en) keinen Personen, Entitäten oder Prozessen, die nicht über die entsprechende Autorisation verfügen, verfügbar gemacht oder diesen gegenüber offengelegt wird (Quelle: DIN EN ISO 22600-1)
Vorbeugungsmaßnahme	Maßnahme zur Beseitigung der Ursache eines möglichen Fehlers oder einer anderen möglichen unerwünschten Situation (Quelle: DIN ISO/IEC 27000)
Zertifizierung	Bestätigung durch eine dritte Stelle bezogen auf Produkte, Prozesse, Systeme oder Personen (Quelle: DIN CEN ISO/TS 14441)

8 Literatur

8.1 Zeitschriftenartikel

- Bergt M. (2016) Verhaltensregeln als Mittel zur Beseitigung der Rechtsunsicherheit in der Datenschutz-Grundverordnung - Wie ein Unternehmen mit nur einer Maßnahme EU-weit Datenschutz-Compliance erreichen kann. CR: 670-678
- Bock K, Meissner S. (2012) Datenschutz-Schutzziele im Recht - Zum normativen Gehalt der Datenschutz-Schutzziele. DuD: 425-431
- Eiermann H. (2017) Sicherheit der Verarbeitung nach der Europäischen Datenschutzgrundverordnung. Was ändert sich, was bleibt? BvD-News: 37-40
- Franck L. (2016) Datensicherheit als datenschutzrechtliche Anforderung. CR: 238-240
- Jandt S. (2017) Datenschutz durch Technik in der DS-GVO - Präventive und repressive Vorgaben zur Gewährleistung der Sicherheit der Verarbeitung. DuD: 562-566
- Karg M. (2015) Anonymität, Pseudonyme und Personenbezug revisited? DuD: 520-526
- Kieselmann O, Kopal N, Wacker A. (2015) „Löschen“ im Internet - Ein neuer Ansatz für die technische Unterstützung des Rechts auf Löschen. DuD: 31-36
- Kodde C. (2013) Die „Pflicht zu Vergessen“ - „Recht auf Vergessenwerden“ und Löschung in BDSG und DS-GVO. ZD: 115-118
- Lepperhoff N. (2017) Abschied von Fingerprint, Iris-Scan & Co? IT-Sicherheit (3/2017): 36-39
- Lepperhoff N. (2017) Sicherheit bei Telemedien - Der übersehene Paragraph und die DS-GVO. IT-Sicherheit (4/2017): 54-55
- Lepperhoff N. (2017) Das IT-Sicherheitskonzept in der DS-GVO. BvD-News (2/2017): 15-18 (Online, zitiert am 2017-09-04; Verfügbar unter https://www.bvdnet.de/wp-content/uploads/2017/08/BvD-News_2_2017_web.pdf)
- Lotz B, Wendler J. (2016) Datensicherheit als datenschutzrechtliche Anforderung: Zur Frage der Abdingbarkeit des § 9 BDSG - Eine Erörterung für den privaten Rechtsverkehr und für Betreiber Kritischer Infrastrukturen. CR; 31-36
- Sachs A. (2017) Vorgaben zur IT-Sicherheit in der EU-DSGVO. IT-Sicherheit: 62-64Sachs A. (2017) Sicherheit der Verarbeitung - Einbettung und Anwendung von Security-Methoden in der DS-GVO. BvD-News. 1/2017 (Online, zitiert am 2017-09-04; Verfügbar unter https://www.bvdnet.de/fileadmin/BvD_eV/BvDNews/17_BvDNews17-1.pdf)
- Sachs A. (2017) Vorgaben zur IT-Sicherheit in der EU-DSGVO. IT-Sicherheit: 62-64
- Schütze B. (2017) Controlling der IT-Sicherheit unter Berücksichtigung von Art. 32 Datenschutz-Grundverordnung. DANA: 137-139
- Schwartmann R, Weiss S. (2016) Ko-Regulierung vor einer neuen Blüte – Verhaltensregelungen und Zertifizierungsverfahren nach der Datenschutzgrundverordnung (Teil 1). RDV: 68-73
- Schwartmann R, Weiss S. (2016) Ko-Regulierung vor einer neuen Blüte – Impulse für datenschutzspezifische Zertifizierungsverfahren und Verhaltensregeln. RDV: 240-245
- Spindler G. (2016) Selbstregulierung und Zertifizierungsverfahren nach der DS-GVO - Reichweite und Rechtsfolgen der genehmigten Verhaltensregeln. ZD: 407-414
- Sydow G, Kring M. (2014) Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug - Konkurrierende Leitbilder für den europäischen Rechtsrahmen. ZD: 271-276
- Thoma F. (2013) Risiko im Datenschutz - Stellenwert eines systematischen Risikomanagements in BDSG und DS-GVO-E. ZD: 578-581

- Veil W. (2015) DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip - Eine erste Bestandsaufnahme. ZD: 347-353
- Weinmann S, Gerling R. (2017) IT-Sicherheit und Datenschutz - Praxisgerechte Vorbereitung auf die DS-GVO. IT-Sicherheit: 65-67
- Wolff H. (2017) Verhaltensregeln nach Art. 40 DS-GVO auf dem Prüfstand. ZD: 151-154

8.2 Internet

- BayLDA (2016) Sicherheit der Verarbeitung - Art. 32 DS-GVO. Online, zitiert am 2017-09-04; Verfügbar unter https://www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf
- Diercks Nina (2017) Die Datenschutzgrundverordnung macht IT-Richtlinien Feuer unter dem Hintern! Online, zitiert am 2017-09-04; Verfügbar unter http://www.socialmediarecht.de/2017/01/24/die-datenschutzgrundverordnung-macht-it-richtlinien-feuer-unter-dem-hintern-teil-7-oder-was-die-dsgvo-mit-it-richtlinien-arbeitsrecht-und-compliance-zu-tun-hat-und-warum-das-jetzt-fuer-unterneh/
- Eiermann H. (2017) Sicherheit der Verarbeitung nach der Europäischen Datenschutzgrundverordnung. Online, zitiert am 2017-09-04; Verfügbar unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Praesentation_Sicherheit_der_Verarbeitung_nach_der_EU_DSGVO.pdf
- Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (2017) Sicherheit der Verarbeitung nach der EU Datenschutz-Grundverordnung. Online, zitiert am 2017-09-04; Verfügbar unter https://www.datenschutz.rlp.de/de/themenfelder-themen/sicherheit-der-verarbeitung-nach-dsgvo/

8.3 Auswahl von Zertifizierungsmöglichkeiten bzgl. IT-Sicherheit

Bei den nachfolgend aufgelisteten Möglichkeiten zur Zertifizierung, dass entsprechend Art. 42 DS-GVO nur entsprechend Art. 42 Abs. 5 DS-GVO akkreditierte Verfahren entsprechend Art. 32 Abs. 3 DS-GVO als Faktor zu berücksichtigen sind. Insbesondere ist zu berücksichtigen, dass diese Standards i. d. R. keine *datenschutzspezifischen Zertifizierungsverfahren* darstellen, d. h. keine Standards im Sinne des Art. 42 DS-GVO darstellen.

Natürlich können national und international anerkannte Standards trotzdem bzgl. des Nachweises der Anforderungen von Art. 32 Abs. 1 DS-GVO hilfreich sein, insbesondere adressieren diese Standards viele der von Art. 32 Abs. 1 lit. b-d DS-GVO genannten Anforderungen.

- Cobit
  - ISACA International
    https://www.isaca.org/COBIT/Pages/default.aspx
  - ISACA German Chapter
    http://www.isaca.de/
  - COBIT-Campus
    http://www.isaca.org/Education/on-demand-learning/Pages/default.aspx bzw.
    https://www.isaca.org/ecommerce/Pages/vCampusLogin.aspx?returnurl=/ecommerce/Pages/ProcessLogin.aspx?vt=2
- IDW PS 330 Abschlussprüfung bei Einsatz von Informationstechnologie
  - Institut der Wirtschaftsprüfer
    https://shop.idw-verlag.de/product.idw?product=20068

- IDW Prüfungsnavigator Grundversion
  https://www.idw.de/idw/im-fokus/idw-pruefungsnavigator/idw-pruefungsnavigator-grundversion---zip-datei/28246
- IT-Auditor IDW - Richtlinie
  https://www.idw.de/blob/87038/eac3b57db3b9a8c8a8bb1417fa1ba1bc/down-it-au-richtlinie-data.pdf

– DIN ISO IEC 27001 „IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen“
– IT Infrastructure Library (ITIL)
  - Axelos: Best Practices
    https://www.axelos.com/best-practice-solutions/itil
  - Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge.
    https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
  - ITIL Wiki
    http://wiki.de.it-processmaps.com/index.php/Hauptseite
  - Studien des BSI bzgl. ITIL
    https://www.bsi.bund.de/DE/Publikationen/Studien/ITIL/index_htm.html
  - ITIL Blog
    https://www.itil.de/