PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Leitlinien zu ethischen und rechtlichen Fragen des Datenschutzes in der IKT-Forschung und -Innovation.

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) – GRUNDSÄCHE

Dieses Projekt wurde aus Mitteln des Forschungs- und Innovationsprogramms Horizont 2020 der Europäischen Union unter der Finanzhilfevereinbarung Nr. 788039 finanziert. Die Verantwortung für den Inhalt dieses Dokuments tragen allein die Verfasser; die Agentur haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

1 Grundsätze

Bud P. Bruegger (ULD)

Danksagung: Die Autoren danken Giuseppe D'Acquisto, Senior Technology Advisor, italienische Datenschutzbehörde (Garante per la Protezione dei Dati Personali), für die Überprüfung und die Anregungen.

Dieser Abschnitt der Leitlinien wurde von José Luis Piñar, ehemaliger Präsident der spanischen Datenschutzbehörde und derzeit Cátedra Google on Privacy, Society and Innovation Universidad CEU-San Pablo, Madrid, validiert.

Der obige Abschnitt *Datenschutz verstehen: Die EU-Verordnung in Kurzform* hat einen Überblick über die DSGVO gegeben. Darin wurden auch die *Datenschutzgrundsätze* vorgestellt, die in Kapitel 2 „Grundsätze" der DSGVO und dort insbesondere in Art. 5 „Grundsätze für die Verarbeitung personenbezogener Daten" enthalten sind. Während „*Datenschutz verstehen: Die EU-Verordnung in Kurzform"* eine Struktur gewählt hat, die dem Inhalt der Datenschutz-Grundverordnung in Bezug auf die Macht folgt, folgt der vorliegende Abschnitt der Struktur von Art. 5 DSGVO. Er erörtert jeden Grundsatz im Detail.

Die Grundsätze weisen die folgende Struktur auf:

- **Bedingungen für die Zwecke** der Verarbeitung: Welche Art von *Zwecken* mit der Verarbeitung personenbezogener Daten verfolgt werden dürfen, ist in **Art. 5 Absatz 1 Buchstabe a** und **5 Absatz 1 Buchstabe b** DSGVO beschrieben. Die Verarbeitung personenbezogener Daten für Zwecke, die diese Bedingungen nicht erfüllen, ist nicht zulässig. Die Bedingungen sind:
    - ***Rechtmäßigkeit*** (Art. 5 Absatz 1 Buchstabe a DSGVO);
    - ***Legitimität*** (Art. 5 Absatz 1 Buchstabe b DSGVO).
- **Bedingungen für die Durchführung** der Verarbeitung: Wenn der Zweck die oben genannten Kriterien erfüllt, muss die Durchführung der Verarbeitung zusätzlich bestimmte Bedingungen erfüllen, um zulässig zu sein. Diese sind in Art. 5 Absatz 1 Buchstabe a bis 5 Absatz 1 Buchstabe f beschrieben, und zwar muss die Verarbeitung:
    - ***nach Treu und Glauben*** erfolgen (Art. 5 Absatz 1 Buchstabe a DSGVO);
    - ***transparent*** sein (Art. 5 Absatz 1 Buchstabe a DSGVO);
    - ***auf die angegebenen Zwecke beschränkt*** sein (Art. 5 Absatz 1 Buchstabe b DSGVO);
    - auf das für die Zwecke der Verarbeitung notwendige Maß **beschränkt sein** (Art. 5 Absatz 1 Buchstabe c DSGVO);
    - **nur sachlich richtige Daten** verwenden (Art. 5 Absatz 1 Buchstabe d DSGVO);
    - **die Identifizierung der betroffenen Personen nur so lange ermöglichen**, wie es für die Zwecke erforderlich ist (Art. 5 Absatz 1 Buchstabe e DSGVO);

- eine angemessene **Sicherheit** gewährleisten (Art. 5 Absatz 1 Buchstabe f DSGVO).

Darüber hinaus sind gemäß Art. 5 Absatz 2 DSGVO die Verantwortlichen für die **Einhaltung** der DSGVO verantwortlich, was bedeutet, dass die **Verarbeitung**:

- **alle oben genannten Bedingungen erfüllt** und
- die Verantwortlichen in der Lage sind, **dies nachzuweisen**.

Um den Lesern das Verständnis der Datenschutz-Grundverordnung zu erleichtern, folgt die ausführliche Erörterung der oben genannten Grundsätze der vom Gesetz vorgegebenen Struktur. Das bedeutet, dass jeweils ein Punkt der Datenschutz-Grundverordnung erörtert wird. **Jeder Punkt** von Art. 5 Absatz 1 und Art. 5 Absatz 2 wird dann als ***Grundsatz*** bezeichnet. Die Bezeichnung des Grundsatzes, die in der DSGVO vorgesehen ist, entspricht der in dene folgenden Abschnitte verwendeten Bezeichnung. In einigen Fällen können mehrere der oben genannten Bedingungen in einem einzigen Grundsatz zusammengefasst werden.

Es gibt zwei Ausnahmen von der Gliederung der folgenden Ausführungen nach den Absätzen von Art. 5 DSGVO. Grund ist eine größere Klarheit, wobei Aussagen erörtert werden, die in einem Absatz der DSGVO unter dem Grundsatz (d. h. der Hauptbedeutung) eines anderen Absatzes bereitgestellt werden. Die Ausnahmen sind:

- Die Anforderung, dass die Zwecke *festgelegt, eindeutig und legitim* sein müssen (Artikel 5 Absatz 1 Buchstabe b DSGVO), wird zusammen mit *Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz* (Artikel 5 Absatz 1 Buchstabe a DSGVO) erörtert.
- Die Erklärung über die Speicherfrist für bestimmte Arten der Verarbeitung (Art. 5 Absatz 1 Buchstabe e DSGVO) wird zusammen mit der Datenminimierung (Art. 5 Absatz 1 Buchstabe c DSGVO) diskutiert, da die Speicherfrist damit zusammenhängt, dass die Daten (zeitlich) „*auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt"* sind.

Die folgende Tabelle gibt einen Überblick darüber, wie sich die Grundsätze auf die Buchstaben von Artikel 5 DSGVO beziehen.

	Art. 5 Absatz 1 Buchstabe a	**Art. 5 Absatz 1 Buchstabe b**	**Art. 5 Absatz 1 Buchstabe c**	**Art. 5 Absatz 1 Buchstabe d**	**Art. 5 Absatz 1 Buchstabe e**	**Art. 5 Absatz 1 Buchstabe f**	**Art. 5 Absatz 2**
Legitimität und Rechtmäßigkeit							
Verarbeitung nach Treu und Glauben							
Transparenz							
Zweckbindung							
Datenminimierung							

Richtigkeit							
Speicherbegrenzung (Minimierung des Identifikationspotenzials)							
Integrität und Vertraulichkeit							
Rechenschaftspflicht							

Die Erörterung der einzelnen Grundsätze ist wie folgt aufgebaut:

- abstrakte **Beschreibung** des Grundsatzes,
- kurze Erörterung **verwandter Artikel und Erwägungsgründe der Datenschutz-Grundverordnung**, die geeignet sind, ein tieferes Verständnis des Grundsatzes zu vermitteln, und
- Beispiele für konkrete **technische oder organisatorische Maßnahmen**, die zur Umsetzung des Grundsatzes genutzt werden können.

Die Beschreibung versucht, das Wesentliche des Grundsatzes zu erfassen. Der Abschnitt über verwandte Artikel und Erwägungsgründe verweist auf Stellen in der Datenschutz-Grundverordnung, in denen ausführlicher beschrieben wird, wie der Grundsatz konkret angewendet werden muss. Dieser Abschnitt kann in einer ersten Lesung konsultiert werden, wenn ein tieferes Verständnis gewünscht ist. Der Abschnitt über Maßnahmen enthält eine nicht erschöpfende Liste von Beispielen, wie jeder Grundsatz in der Praxis umgesetzt werden kann.

Im weiteren Verlauf dieses Kapitels werden die in Art. 5 DSGVO aufgeführten Grundsätze anhand der beschriebenen Struktur beschrieben.

1.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz

Bud P. Bruegger (ULD)

Danksagung: Die Autoren sind dankbar für den Beitrag von Iñigo de Miguel Beriain (UPV/EHU), der eine Analyse dieses Grundsatzes als Beitrag zu der hier vorgestellten Beschreibung verfasst hat.

Im Folgenden wird der Grundsatz der *Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz* erörtert, der in Art. 5 Absatz 1 Buchstabe a DSGVO definiert ist.

***Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz* auf einen Blick:**

Nach der Datenschutz-Grundverordnung muss die Verarbeitung *rechtmäßig sein* und

legitime Zwecke verfolgen. Außerdem muss sie *fair* und *transparent* sein.

Die Rechtmäßigkeit ist in der DSGVO sehr genau definiert und ist gegeben, wenn der Zweck der Verarbeitung in eine der sechs Kategorien (auch *Rechtsgrundlagen* genannt) fällt, die in Art. 6 Absatz 1 DSGVO aufgeführt.

Legitim ist ein sehr viel weiter gefasster Begriff, der die Einhaltung des Buchstabens des Gesetzes, des Geistes des Gesetzes, der Werte der Gesellschaft (insbesondere der *Europäischen Charta der Grundrechte*) und der *ethischen* Grundsätze bedeutet.

Der Begriff Verarbeitung nach Treu und Glauben wird in seinem allgemeinen Verständnis verwendet. Dies verbietet zum Beispiel manipulative Praktiken seitens des Verantwortlichen, wie etwa Nudging. Natürlich geht es in den meisten Artikeln der Datenschutz-Grundverordnung um Verarbeitung nach Treu und Glauben. Die ausdrückliche Nennung des Grundsatzes kann als Ausweichlösung für den Fall dienen, dass eine Konsequenz der Verarbeitung nach Treu und Glauben nicht ausdrücklich in der Datenschutz-Grundverordnung genannt wird. Dadurch werden Schlupflöcher vermieden.

Die Transparenz der Verarbeitung ist eine wichtige Strategie, um ein Machtgleichgewicht zwischen dem Verantwortlichen und der betroffenen Person herzustellen. Sie funktioniert, indem sie alles ins Licht rückt und so einer Überprüfung zugänglich macht. Sie ist in der Datenschutz-Grundverordnung in Form von detaillierten Informationsanforderungen dargelegt, die der Verantwortliche sowohl den betroffenen Personen als auch den Aufsichtsbehörden zur Verfügung stellen muss.

1.1.1 Beschreibung

In „*Datenschutz verstehen: Die EU-Verordnung in Kurzform“ wurden die* meisten der in diesem Grundsatz geforderten Eigenschaften im Hinblick auf ein ausgewogenes Machtverhältnis zwischen dem Verantwortlichen und den betroffenen Personen erörtert. Dies wird im Folgenden zusammengefasst: Sowohl die *Rechtmäßigkeit* als auch die *Legitimität* der Zwecke wird als Voraussetzung für die Zulässigkeit der Verarbeitung dargestellt. Siehe *1.5 „Zu welchen Zwecken ist die Verarbeitung zulässig“ für weitere Einzelheiten*. Der Aspekt der *Verarbeitung nach Treu und Glauben* wurde in der Einleitung nicht erörtert. Durch das Gleichgewicht der Macht zwischen dem Verantwortlichen und den betroffenen Personen geht es bei der gesamten Datenschutz-Grundverordnung um Verarbeitung nach Treu und Glauben. *Transparenz* wurde als Voraussetzung für die Rechenschaftspflicht dargestellt. Siehe *1.6.1 Die Verantwortlichen sind in* Bezug auf Einzelheiten *voll rechenschaftspflichtig*.

In der Datenschutz-Grundverordnung wird dieser Grundsatz wie folgt definiert:

Definition in Art. 5 Absatz 1 Buchstabe a DSGVO:

Personenbezogene Daten müssen auf **rechtmäßige Weise, nach Treu und Glauben** und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz“ ″);

Auf Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz wird im Folgenden näher eingegangen.

1.1.1.1 Voraussetzung für die Rechtmäßigkeit: festgelegte, eindeutige Zwecke

Die Rechtmäßigkeit ist eine Voraussetzung für die Zwecke der Verarbeitung[62]. Es ist daher nicht möglich, eine Begründung zu geben, ohne vorher die genauen Zwecke zu kennen, die mit der Verarbeitung verfolgt werden. Aus diesem Grund wird die Anforderung aus **Art. 5 Absatz 1 Buchstabe b**, dass die Zwecke festgelegt und eindeutig sein müssen, hier als Voraussetzung diskutiert:

Personenbezogene Daten müssen für **festgelegte, eindeutige** und legitime **Zwecke** erhoben werden

Festgelegte Zwecke:

Die *Artikel-29-Datenschutzgruppe* schreibt[63]:

> „Die **Festlegung des Zwecks ist das Kernstück des Rechtsrahmens für den Schutz personenbezogener Daten**. Um **festzustellen, ob die Datenverarbeitung im Einklang mit dem Gesetz steht** und welche Datenschutzgarantien angewandt werden sollten, ist es eine **notwendige Voraussetzung, den/die spezifischen Zweck(e) zu bestimmen**, für **den/die** die Erhebung personenbezogener Daten erforderlich ist."

Die Festlegung kann als die erste Aufgabe der Konzeptualisierung einer Verarbeitungsaktivität angesehen werden, die alle nachfolgenden Entscheidungen leitet:

- ob die **Verarbeitung zulässig**, d. h. rechtmäßig und legitim **ist**,
- **was die Durchführung** der Verarbeitung, die zur Erreichung der Zwecke erforderlich ist, **mit sich bringt** und
- welche **Garantien** getroffen werden sollten.

Die *Artikel-29-Datenschutzgruppe* führt weiter aus:[64]

> „Der **Zweck** der Erhebung muss **klar** und **deutlich** angegeben werden: Er muss **detailliert** genug sein, um zu bestimmen, welche Art der Verarbeitung unter den angegebenen Zweck fällt und welche nicht, und um zu ermöglichen, dass die Einhaltung des Gesetzes beurteilt und Farantien angewendet werden können.

und

> Aus diesen Gründen erfüllt **ein vager oder allgemeiner Zweck** wie z. B. „Verbesserung der Nutzererfahrung", „Marketingzwecke", „IT-Sicherheitszwecke" oder „künftige Forschung" ohne nähere Angaben in der Regel **nicht das Kriterium eines festgelegten Zwecks.**

Eindeutige Zwecke:

Die Artikel-29-Datenschutzgruppe führt weiter aus:[65]

---

62 Es liegt außerhalb des Rahmens dieses Dokuments, eine gründliche rechtliche Analyse des Begriffs „Zweck" über seine Bedeutung im allgemeinen Sprachgebrauch hinaus vorzunehmen. Es soll lediglich darauf hingewiesen werden, dass die Zwecke der Verarbeitung in der Regel mit einem Ziel verbunden sind, das der Verantwortliche verfolgt. Solche Ziele sollten konkret (und nicht nur theoretisch) sein, und es ist oft möglich, festzustellen, ob das Ziel erreicht wurde oder zu messen, in welchem Maße es erreicht wurde.

63 Hervorhebung durch den Autor, Zitat siehe Seite 15: Artikel 29 Datenschutzgruppe, 00569/13/EN, WP203, Stellungnahme 03/2013 zur Zweckbindung, angenommen am 2. April 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (zuletzt besucht am 27.05.2020).

64 WP203, Seite 15, Hervorhebung durch den Autor.

„Personenbezogene Daten müssen für **eindeutige Zwecke** erhoben werden. Die Erhebungszwecke müssen **nicht nur in den Köpfen** der für die Datenerhebung verantwortlichen Personen verankert sein. Sie müssen auch explizit gemacht werden. Mit anderen Worten, sie müssen **klar offengelegt, erläutert oder in verständlicher Form ausgedrückt werden**.

Beachten Sie, dass die Anforderung, die Zwecke eindeutig anzugeben, eng mit der Unterrichtung der betroffenen Personen über die Zwecke der Verarbeitung zusammenhängt (siehe Art. 13 Absatz 1 Buchstabe c und 14 Absatz 1 Buchstabe c DSGVO).

Auf der Grundlage der Voraussetzung, dass ein bestimmter Zweck eindeutig genannt wird, können Legitimität und Rechtmäßigkeit erörtert werden.

1.1.1.2 Legitimität und Rechtmäßigkeit

Während Art. 5 Absatz 1 Buchstabe a DSGVO nur von der *Rechtmäßigkeit* spricht, ist das eng damit verbundene Erfordernis der *Legitimität* in Art. 5 Absatz 1 Buchstabe b DSGVO genannt. Da beide Bestimmungen Anforderungen an die Zwecke der Verarbeitung enthalten, werden sie hier gemeinsam erörtert.

Art. 5 Absatz 1 Buchstabe b DSGVO besagt:

> Personenbezogene Daten müssen für *festgelegte, eindeutige* und **legitime Zwecke** erhoben werden und [...]

Die Datenschutz-Grundverordnung enthält keine Definition der *Legitimität*, aber die *Artikel-29-Datenschutzgruppe* liefert die folgenden Informationen:[66]

> Das Erfordernis der ***Legitimität*** bedeutet, dass die Ziele „**im Einklang mit dem Gesetz" im weitesten Sinne** stehen müssen. Dies umfasst **alle Formen des geschriebenen Rechts und des Gewohnheitsrechts**, **primäre und sekundäre Rechtsvorschriften**, **kommunale Erlasse**, gerichtliche **Präzedenzfälle**, **Verfassungsgrundsätze**, **Grundrechte**, **andere Rechtsgrundsätze sowie** die **Rechtsprechung**, da dieses „Recht" von den zuständigen Gerichten ausgelegt und berücksichtigt wird.

Die Legitimität ist also eine sehr **umfassende Anforderung**. Dies wird noch deutlicher, wenn man bedenkt, dass bestimmte Rechtsvorschriften wie die *Verordnung*[67] *über klinische Prüfungen* auch ***ethische Anforderungen*** enthalten. Aber auch dort, wo die Ethik nicht gesetzlich vorgeschrieben ist, besteht die Gefahr, dass eindeutig unethische Zwecke auch als unrechtmäßig angesehen werden. Dies kann zum Beispiel der Fall sein, wenn die Verarbeitung unter Missachtung einer Ablehnung durch eine Forschungsethikkommission erfolgt.

Im Gegensatz zur *Legitimität* ist die ***Rechtmäßigkeit*** in der Datenschutz-Grundverordnung tatsächlich definiert. **Art. 6 Absatz 1** DSGVO lautet:

> Die Verarbeitung ist nur **rechtmäßig**, wenn mindestens eine der folgenden Bedingungen erfüllt ist: [...]

---

65 WP203, Seite 17, Hervorhebung durch den Autor.

66 WP203, Seite 20, , Hervorhebung durch den Autor.

67 VERORDNUNG (EU) Nr. 536/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG, https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf (zuletzt besucht am 27/05/2020).

In der durch [...] dargestellten Auslassung werden sechs mögliche *Rechtsgrundlagen* aufgeführt. Sie können als Kategorien von Zwecken angesehen werden. Diese werden im folgenden Abschnitt „Verwandte Artikel und Erwägungsgründe“ ausführlicher beschrieben.

1.1.1.3 Verarbeitung nach Treu und Glauben

Beim gesamten Datenschutz und somit auch bei der DSGVO geht es um die Verarbeitung nach Treu und Glauben gegenüber den betroffenen Personen. In der DSGVO wird dargelegt, was *„Verarbeitung nach Treu und Glauben“* eigentlich konkret bedeutet.

Die ausdrückliche Erwähnung als Grundsatz kann also als „Ausweichklausel“ für den Fall betrachtet werden, dass eine konkrete Anforderung in Bezug auf Treu und Glauben nicht ausdrücklich in der Datenschutz-Grundverordnung genannt wurde. Selbst in diesem Fall würde der Grundsatz der *Verarbeitung nach Treu und Glauben* jede „Lücke“ in der DSGVO verhindern.

Während sich die gesamte Datenschutz-Grundverordnung um die Verarbeitung nach Treu und Glauben dreht, enthält der folgende Abschnitt unten einige Beispiele, in denen die Verarbeitung nach Treu und Glauben besonders deutlich wird.

1.1.1.4 Transparenz

Transparenz ist ein wohlverstandenes Konzept und eine wichtige Voraussetzung für die Rechenschaftspflicht im Rahmen der Datenschutz-Grundverordnung. Das Hauptaugenmerk der Transparenz liegt darauf, die **betroffenen Personen** im Voraus[68] über das Vorhandensein der Verarbeitung und ihre wichtigsten Merkmale zu informieren. Weitere Informationen (z. B. die Daten über die betroffene Person) sind auf Anfrage erhältlich. Die betroffenen Personen müssen auch über bestimmte Ereignisse informiert werden, vor allem über Datenschutzverletzungen (wenn die betroffene Person einem hohen Risiko ausgesetzt ist). Die Transparenz wird auch dadurch unterstützt, dass die Verantwortlichen einen Datenschutzbeauftragten benennen, der als zentrale Anlaufstelle für die Anliegen der betroffenen Personen fungiert. In der Datenschutz-Grundverordnung werden die betroffenen Personen dazu ermächtigt, die wichtigsten Hüter ihrer eigenen Rechte und Freiheiten zu sein. Transparenz ist natürlich eine Voraussetzung dafür, dass Verstöße aufgedeckt werden und eingegriffen werden kann.

Die Aufsichtsbehörden sind, wie aus ihrem Namen hervorgeht, ebenfalls Hüter der Einhaltung der DSGVO, auch wenn ihre Beteiligung oft durch Beschwerden betroffener Personen ausgelöst wird[69]. Es gibt Transparenzanforderungen für Verantwortliche, die speziell auf aufsichtsführende Verantwortliche abzielen, einschließlich der Verzeichnisse über die Verarbeitung (siehe *Dokumentation der Verarbeitung* im Abschnitt „*Wichtigste Instrumente und Maßnahmen" in Teil II*) und der Datenschutz-Folgenabschätzung (siehe den gleichnamigen Abschnitt in „*Wichtigste Instrumente und Maßnahmen“,* Teil II dieser Leitlinien). Die Tatsache, dass die Verantwortlichen den Aufsichtsbehörden gegenüber rechenschaftspflichtig[70] sind und Untersuchungen und Audits[71] vor Ort[72] zulassen müssen, trägt ebenfalls zur Transparenz bei.

---

68 „Im Voraus“ bedeutet hier, dass die betroffenen Personen über die Verarbeitung informiert sein sollten, bevor sie stattfindet. Dies bedeutet nicht, dass eine bestimmte Methode der Informationsbereitstellung vorgeschrieben ist oder dass dynamische Möglichkeiten der Bereitstellung der erforderlichen Informationen ausgeschlossen sind.

69 Siehe Art. 57 Absatz 1 Buchstabe f DSGVO.

70 Siehe Art. 58 Absatz 1 Buchstabe a DSGVO.

71 Siehe Art. 58 Absatz 1 Buchstabe f DSGVO.

72 Siehe Art. 58 Absatz 1 Buchstabe b DSGVO.

1.1.2 Verwandte Artikel und Erwägungsgründe

1.1.2.1 Rechtmäßigkeit

Die Definition der Rechtmäßigkeit findet sich in Art. 6 Absatz 1 DSGVO. Sie lautet wie folgt:

> Die Verarbeitung ist **nur *rechtmäßig*, wenn** mindestens eine der folgenden Bedingungen erfüllt ist:
>
> (a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte *Zwecke* gegeben.
>
> (b) Die Verarbeitung ist für die **Einhaltung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.
>
> (c) Die Verarbeitung ist zur **Einhaltung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt.
>
> (d) Die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person **zu schützen.**
>
> (e) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die **im öffentlichen Interesse liegt** oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
>
> (f) Die Verarbeitung ist *zur* **Wahrung der berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, **sofern nicht die** Interessen **oder Grundrechte und Grundfreiheiten der betroffenen Person**, die den Schutz personenbezogener Daten erfordern, **überwiegen,** insbesondere wenn es sich bei der betroffenen Person um ein Kind handelt.
>
> Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Einhaltung ihrer Aufgaben vorgenommene Verarbeitung.

Während die Zwecke der Verarbeitung festgelegt und eindeutig (siehe Art. 5 Absatz 1 Buchstabe b) und daher auch hinreichend eng und spezifisch sein müssen, handelt es sich bei den oben genannten **Zwecken** eindeutig um **Kategorien von Zwecken**. (Wo das Wort Zweck ausdrücklich verwendet wurde, ist es daher kursiv geschrieben). Sie werden gemeinhin als ***Rechtsgrundlagen***[73] bezeichnet und sind durch ihre Stellung in Artikel 6 gekennzeichnet; so wäre beispielsweise die *Einwilligung die Rechtsgrundlage* von Art. 6 Absatz 1 Buchstabe a.

Die Datenschutz-Grundverordnung enthält zwei Artikel, die **weitere Anforderungen an die Rechtmäßigkeit** für zwei verschiedene Fälle festlegen: **sensible Daten** und Daten über **strafrechtliche Verurteilungen**. Im Einzelnen sind dies die Folgenden:

Art. 9 DSGVO besagt, dass die Verarbeitung besonderer Kategorien von Daten grundsätzlich verboten ist, und nennt 10 Ausnahmen von dieser Regel. Die Ausnahmen sind in ihrer Struktur vergleichbar mit den Rechtsgrundlagen des Art. 6. Der Artikel legt fest, dass Daten besonders sensibel sind, wenn sie Aufschluss geben über:

- rassische oder ethnische Herkunft,
- politische Meinungen,

73 Der Begriff *Rechtsgrundlage wird* in der Datenschutz-Grundverordnung ausführlich verwendet und hier als bevorzugter Begriff empfohlen. In der Literatur wird auch der Begriff *lawful basis* verwendet.

- religiöse oder philosophische Überzeugungen,
- Mitgliedschaft in einer Gewerkschaft,

oder es sich um Daten folgender Kategorien handelt:

- genetische Daten,
- biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person,
- Daten zur Gesundheit oder
- Daten über das Sexualleben oder die sexuelle Ausrichtung einer natürlichen Person.

Für diese Daten gelten strengere Anforderungen, damit ihre Verarbeitung als rechtmäßig angesehen werden kann. So erfordert die Verarbeitung solcher sensibler Daten anstelle der einfachen Einwilligung gemäß Art. 6 Absatz 1 Buchstabe a eine anspruchsvollere Stufe der Einwilligung, die als ***ausdrückliche Einwilligung*** bezeichnet wird (siehe Art. 9 Absatz 2 Buchstabe a DSGVO).

Wie Art. 9 für besonders sensible Daten gilt, schränkt **Artikel 10 DSGVO** die Verarbeitung von „Daten über **strafrechtliche Verurteilungen und Straftaten** oder damit zusammenhängende Sicherungsmaßregeln" weiter ein. Insbesondere muss die Verarbeitung, um rechtmäßig zu sein, entweder „nur unter behördlicher **Aufsicht erfolgen** oder, wenn [sie] nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist, angemessene Garantien für die Rechte und Freiheiten der betroffenen Personen vorsehen".

Es gibt mehrere Artikel und Erwägungsgründe in der DSGVO, die das **Konzept der Einwilligung** (Art. 6 Absatz 1 Buchstabe a DSGVO) näher erläutern. Die wichtigsten sind die Folgenden:

- **Art. 4 Absatz 11**, der **die Einwilligung definiert**;
- **Art. 7**, der die **Bedingungen für die Einwilligung** auflistet; und
- **Art. 8**, der die **Bedingungen für die Einwilligung des Kindes in die Dienste der Informationsgesellschaft** regelt**.**

In Anbetracht der Tatsache, dass die Einwilligung ein komplexes Konzept ist, hat der **Europäische Datenschutzausschuss** maßgebliche ***Leitlinien*** *05/2020* ***zur Einwilligung*** *gemäß Verordnung 2016/679*[74] herausgegeben.

Neben der *Einwilligung ist* auch das Konzept des ***berechtigten Interesses des Verantwortlichen*** (Art. 6 Absatz 1 Buchstabe f DSGVO) nur schwer vollständig zu verstehen. Entscheidend ist hier die Einschränkung „**sofern nicht die** Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen". Dies bedeutet, dass die berechtigten Interessen des Verantwortlichen mit den Interessen der betroffenen Personen abgewogen werden müssen. Um festzustellen, ob dies der Fall ist, muss der Verantwortliche eine so genannte ***Abwägungsprüfung durchführen***. Wie dies zu tun ist, wird in Teil II dieser Leitlinien unter „Wichtigste Instrumente und Maßnahmen" beschrieben. Sie stützt sich in erster Linie auf die maßgebliche *Stellungnahme 06/2014* der *Artikel-29-Datenschutzgruppe zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß*

74 EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.0, angenommen am 4. Mai 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (zuletzt besucht am 22.05.2020).

Artikel 7 der Richtlinie 95/46/EG[75]. Diese Stellungnahme basiert zwar auf der Datenschutzrichtlinie, die der DSGVO vorausging, ist aber generell auf die Auslegung von Art. 6 Absatz 1 Buchstabe f DSGVO anwendbar. Sie wird als **weiterführende Lektüre** zu diesem Thema empfohlen.

1.1.2.2 Verarbeitung nach Treu und Glauben

Bei der gesamten DSGVO geht es wohl um Verarbeitung nach Treu und Glauben. Im Folgenden werden einige Artikel der Datenschutz-Grundverordnung genannt, die dies besonders gut veranschaulichen.

Ein Bereich, in dem Verarbeitung nach Treu und Glauben offensichtlich ist, betrifft die Anforderungen an die Transparenz. Hier besagt **Art. 12 Absatz 1**, dass der Verantwortliche „der betroffenen Person Informationen in **präziser**, transparenter, **verständlicher** und **leicht zugänglicher** Form in einer **klaren und einfachen Sprache** zu übermitteln hat; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten." Dies verbietet offensichtlich die unlautere Praxis, die erforderlichen Informationen in einer Form bereitzustellen, die für die betroffenen Personen unzugänglich ist.

Ebenso kann die **Einwilligung** nicht stillschweigend erfolgen, sondern erfordert vielmehr eine ausdrückliche „Erklärung oder eine sonstige **eindeutige bestätigende Handlung"** (siehe **Art. 4 Absatz 11** DSGVO). In demselben Artikel heißt es weiter, dass die Einwilligung **freiwillig**, **für den bestimmten Fall**, **in informierter Weise** und **unmissverständlich abgegeben werden** muss". Darüber hinaus muss eine betroffene Person in der Lage sein, ihre Einwilligung **jederzeit** und ohne Angabe von Gründen genauso **einfach zu widerrufen, wie sie erteilt wurde**. Diese strengen Anforderungen an die Einwilligung verbieten direkt viele manipulative Praktiken, einschließlich des „Nudging"[76] von betroffenen Personen.

Mehrere **Rechte der betroffenen Person** können direkt mit Verarbeitung nach Treu und Glauben in Verbindung gebracht werden. Dazu gehören:

- Das **Recht auf Berichtigung** (Art. 16 DSGVO), um zu verhindern, dass betroffene Personen aufgrund unrichtiger Daten negative Folgen erleiden;
- Das **Recht auf Einschränkung der Verarbeitung** (Art. 18 DSGVO), das die Verantwortlichen daran hindert, Daten weiter zu verwenden, die als unrichtig gemeldet wurden oder sich auf eine Verarbeitung beziehen, der die betroffene Person widersprochen hat;
- Das **Recht auf Datenübertragbarkeit** (Art. 20 DSGVO), das verhindert, dass Nutzer, die ihre Beziehung zu dem Verantwortlichen ändern, in eine „Lock-in"-Situation geraten und einen möglichen Verlust (z. B. von Investitionen[77]) erleiden;
- Das **Widerspruchsrecht** (Art. 21 DSGVO), bei dem im Falle einer Rechtsgrundlage nach Art. 6 Absatz 1 Buchstabe f DSGVO die betroffenen Personen **ihre besondere Situation** darlegen können, in der ihre Interessen gegenüber den berechtigten Interessen des Verantwortlichen überwiegen;

---

75 Artikel 29 Datenschutzgruppe, 844/14/EN, WP217, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, angenommen am 9. April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (zuletzt besucht am 22.05.2020).

76 Siehe zum Beispiel Weinmann, M., Schneider, C. & Brocke, J.v. Digital Nudging. Bus Inf Syst Eng 58, 433-436 (2016). https://doi.org/10.1007/s12599-016-0453-1 (zuletzt besucht am 22.05.2020).

77 Ein Paradebeispiel für einen möglichen Investitionsverlust ist die Sammlung von persönlichen Fotos.

- Das **Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht** (Art. 22 DSGVO), die auch das **Recht auf ein menschliches Eingreifen seitens des** Verantwortlichen vorsieht (siehe Absatz 3).

Ein weiteres Indiz für eine Verarbeitung nach Treu und Glauben ist, dass der Verantwortliche die Sichtweise der betroffenen Personen berücksichtigen muss. Dies geht beispielsweise aus Erwägungsgrund 50 der Datenschutz-Grundverordnung hervor, in dem gefordert wird, die berechtigten Erwartungen der betroffenen Personen zu berücksichtigen, wenn es um die Feststellung geht, ob ein Zweck gemäß Artikel 6 Absatz 4 vereinbar ist. Dies wird auch in der Datenschutz-Folgenabschätzung (Artikel 35 DSGVO) deutlich, bei der die Verantwortlichen gegebenenfalls die Meinung der betroffenen Personen oder ihrer Vertreter einholen müssen (Artikel 35 Absatz 9 DSGVO).

1.1.2.3 Transparenz

In mehreren Artikeln der Datenschutz-Grundverordnung wird der Grundsatz der *Transparenz* näher erläutert. Dazu gehören die Folgenden:

- **In den Artikeln 12 bis 14** wird detailliert beschrieben, welche **Informationen die** Verantwortlichen den betroffenen Personen **im Voraus zur** Verfügung stellen müssen.
- **Art. 15** beschreibt die Informationen, die den betroffenen Personen auf Anfrage erteilt werden müssen, einschließlich des vollständigen Zugangs zu ihren Daten.
- **Art. 34** beschreibt, wie betroffene Personen über Datenschutzverletzungen informiert werden müssen, wenn diese wahrscheinlich zu einem hohen Risiko führen.
- **Art. 38 Absatz 4** benennt den *Datenschutzbeauftragten* des Verantwortlichen als Anlaufstelle für betroffene Personen.
- **Art. 12** und **19** beschreiben die Informationen, die die Verantwortlichen betroffenen Personen geben müssen, die eines ihrer Rechte ausüben.
- **Art. 30** ***Verzeichnisse über die Verarbeitung*** und **35** ***Datenschutz-Folgenabschätzung*** beschreiben die Informationen, die den Aufsichtsbehörden vorgelegt werden müssen. (Letzteres nur, wenn die Verarbeitung wahrscheinlich zu einem hohen Risiko führt).
- **Art. 58 Absatz 1** legt fest, wie die Verantwortlichen gegenüber den Aufsichtsbehörden transparent sein müssen, indem sie Rede und Antwort stehen (Buchstabe a), Inspektionen und Audits zulassen (Buchstabe b) und Zugang zu ihren Räumlichkeiten gewähren (Buchstabe f).
- **Art. 33** beschreibt die Meldung von Verstößen an die Aufsichtsbehörden.

In Anbetracht der Bedeutung der Transparenz in der Datenschutz-Grundverordnung hat der ***Europäische Datenschutzausschuss*** in seinen **Leitlinien zur Transparenz** im Rahmen der Verordnung (EU) 2016/679 (wp260rev.01)[78] eine maßgebliche Auslegung der damit verbundenen Pflichten vorgelegt. Diese werden zur weiteren Lektüre empfohlen.

78 EDSA, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (wp260rev.01), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (zuletzt besucht am 22.05.2020).

1.1.3 Damit verbundene technische und organisatorische Maßnahmen

Im Folgenden werden Beispiele für Maßnahmen zur Umsetzung verschiedener Aspekte des Grundsatzes angeführt.

1.1.3.1 Legitimität und Rechtmäßigkeit

- Zumindest dort, wo die Überprüfung und der Nachweis der **Legitimität formale Schritte** erfordert, können diese als organisatorische Maßnahmen zur Unterstützung der Legitimität angesehen werden. Ein Paradebeispiel sind die **Beantragung und Genehmigung** bestimmter medizinischer Forschungen durch die zuständige **Forschungsethikkommission**.
- Eine Voraussetzung für die Bewertung der Legitimität und der Rechtmäßigkeit ist die **Angabe ausdrücklicher Ziele**. Dies kann an sich schon als Maßnahme betrachtet werden, insbesondere wenn sie mit **Überlegungen einhergeht**, wie die Spezifikation **so eindeutig** und **eng wie möglich** gestaltet werden kann. In diesem Fall kann auch eine solche Analyse als Teil dieser Maßnahme angesehen werden.
- Die wichtigste Maßnahme zur Unterstützung der Rechtmäßigkeit besteht darin, eine oder mehrere **Rechtsgrundlagen** gemäß **Art. 6 Absatz 1** DSGVO zu identifizieren. In vielen Fällen stützt sich eine Verarbeitungstätigkeit auf mehrere Rechtsgrundlagen. Ein von der *Data Privacy Vocabulary Community Group* des W3C[79] veröffentlichter Anwendungsfall liefert ein leicht zugängliches Beispiel.
- Wenn Art. **6 Absatz 1 Buchstabe a** DSGVO, d. h. die *Einwilligung,* als Rechtsgrundlage gewählt wurde, ist eine **Analyse**, die rechtfertigt, dass die strengen **Anforderungen** der DSGVO **an eine (freiwilllig und in Kenntnis der Sachlage erteilte) Einwilligung** erfüllt sind, eine wichtige Maßnahme. Dabei kann beispielsweise geprüft werden, ob die als Grundlage für die Einwilligung bereitgestellten Informationen für die betroffenen Personen tatsächlich verständlich sind und ob der Widerruf der Einwilligung tatsächlich so einfach ist wie die Erteilung der Einwilligung.
    - Wenn **Kinder** oder andere **schutzbedürftige Personen** betroffen sind, sollte diese Analyse außerdem einen besonderen Schwerpunkt auf Garantien gemäß Art. 7 DSGVO legen.
- Wenn Art. **6 Absatz 1 Buchstabe f** DSGVO, d. h. die *legitige Einwilligung des Verantwortlichen,* als Rechtsgrundlage gewählt wurde, umfassen die Maßnahmen eine genaue Spezifizierung der berechtigten Interessen sowie eine ***Abwägungsprüfung*** (siehe gleichnamigen Abschnitt in „Wichtigste Instrumente und Maßnahmen“ in Teil II dieser Leitlinien), um sicherzustellen, dass diese tatsächlich die Interessen, Rechte und Freiheiten der betroffenen Personen überwiegen.
- Beabsichtigt der Verantwortliche, bestimmte Daten über den ursprünglichen Zweck hinaus für **vereinbare Zwecke weiterzuverarbeiten** (siehe Art. 5 Absatz 1 Buchstabe b DSGVO), ist die Analyse auf der Grundlage der Kriterien von Art. 6 Absatz 4, um nachzuweisen, dass diese zusätzlichen Zwecke tatsächlich vereinbar sind, eine Maßnahme, die die Rechtmäßigkeit einer solchen Verarbeitung belegt.
- Wenn besondere Datenkategorien (d. h. sensible Daten) oder Daten über strafrechtliche Verurteilungen verarbeitet werden, müssen zusätzliche Maßnahmen zu

79 Brügger, Schlehahn & Zwingelberg, Data Privacy Vocabulary Community Group, Data Protection Aspects of Online Shopping – A Use Case, https://www.w3.org/community/dpvcg/2019/12/12/data-protection-aspects-of-online-shopping-a-use-case/ (zuletzt besucht am 25/05/2020).

den Maßnahmen nach Art. 6 Absatz 1 DSGVO ergriffen werden. Insbesondere im ersten Fall muss die Voraussetzung des Art. 9 Absatz 2 DSGVO, warum eine Ausnahme vom Verbot der Verarbeitung sensibler Daten gilt, begründet und dokumentiert werden. Im letzteren Fall müssen die Bedingungen, die die Verarbeitung gemäß Art. 10 DSGVO zulassen, umgesetzt und dokumentiert werden.

1.1.3.2 Verarbeitung nach Treu und Glauben

- Wie oben dargelegt, können alle Anforderungen der Datenschutz-Grundverordnung als eine Frage der Verarbeitung nach Treu und Glauben betrachtet werden; einige Rechte der betroffenen Person wurden jedoch als besonders relevant dargestellt. Die wichtigsten Maßnahmen zur Förderung der Verarbeitung nach Treu und Glauben sind daher eine angemessene **Umsetzung der Rechte der betroffenen Personen**.

1.1.3.3 Transparenz

- Die Umsetzung der Anforderungen der Art. 12 bis 14 DSGVO zur Bereitstellung angemessener und leicht verständlicher **Informationen für die betroffenen Personen** ist eine wichtige Maßnahme zur Förderung der Transparenz.
- Gleiches gilt für Dokumente, die zur Unterrichtung der Aufsichtsbehörden erstellt werden, insbesondere das ***Verzeichnis von Verarbeitungstätigkeiten*** (gemäß Art. 30 DSGVO) und eine ***Datenschutz-Folgenabschätzung*** (gemäß Art. 35 DSGVO). Eine weitere Maßnahme ist die teilweise Veröffentlichung dieser Folgenabschätzung.
- Jede Analyse, die die Wirksamkeit und Zugänglichkeit der bereitgestellten Informationen bewertet – möglicherweise im Hinblick auf besondere Kategorien betroffener Personen wie Kinder – kann als Maßnahme an sich betrachtet werden.
- Die Ernennung eines Datenschutzbeauftragten kann zum Teil als Maßnahme zur Erhöhung der Transparenz sowohl gegenüber den betroffenen Personen als auch gegenüber der Aufsichtsbehörde gesehen werden.

1.2 Zweckbindung

Bud P. Bruegger (ULD)

Danksagung: Die Autoren sind dankbar für den Beitrag von Iñigo de Miguel Beriain (UPV/EHU), der eine Analyse dieses Grundsatzes als Beitrag zu der hier vorgestellten Beschreibung verfasst hat.

Im Folgenden wird der Grundsatz der *Zweckbindung* erörtert, der in Art. 5 Absatz 1 Buchstabe b DSGVO definiert ist.

***Zweckbindung* auf einen Blick:**

Daten, die **für bestimmte „ursprüngliche" Zwecke erhoben** wurden, dürfen **nur**

weiterverarbeitet werden:

- für diese **ursprünglichen Zwecke** oder für
- **vereinbare Zwecke**.

Für den allgemeinen Fall gibt die Datenschutz-Grundverordnung **Kriterien vor**, anhand derer die **Vereinbarkeit** der Zwecke **bestimmt werden kann** (siehe Art. 6 Absatz 4). Darüber hinaus werden einige Zwecke von der Datenschutz-Grundverordnung **vorab als vereinbar anerkannt** (siehe Art. 5 Absatz 1 Buchstabe b), sofern geeignete Garantien ergriffen werden (siehe Art. 89). Dies sind:

- im **öffentlichen Interesse liegende Archivzwecke,**
- **wissenschaftliche oder historische Forschungszwecke** und
- **statistische Zwecke**.

1.2.1 Beschreibung

In *„Datenschutz verstehen: Die EU-Verordnung in Kurzform"* wurde die *Zweckbindung* dadurch begründet, dass die Nutzung der erlangten Macht ausschließlich auf die erklärten und rechtmäßigen Zwecke beschränkt werden soll. (Siehe *1.6.4 Einschränkung der Macht der Verantwortlichen, die Macht ausschließlich zur Erreichung der erklärten rechtmäßigen Zwecke zu nutzen*).

In der Datenschutz-Grundverordnung wird dieser Grundsatz wie folgt definiert:

Definition laut Art. 5 Absatz 1 Buchstabe b DSGVO:

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und **dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden**; [...] („*Zweckbindung*")

Es sei darauf hingewiesen, dass die erste Hälfte dieses Satzes bereits unter dem vorhergehenden Grundsatz erörtert wurde. Insbesondere das Erfordernis, dass die Zwecke ***festgelegt* und *eindeutig*** sein müssen, war eine **Voraussetzung dafür, dass man** von ***Rechtmäßigkeit*** sprechen konnte; das Erfordernis „legitim" bezieht sich auf die Zwecke und wurde daher zusammen mit der *Rechtmäßigkeit* erörtert.

Was hier ausführlicher erörtert wird, ist der Kern dieses Grundsatzes, nämlich die **Beschränkung auf eine mit den Zwecken vereinbare Verarbeitung**. Diese Anforderung bezieht sich auf die Durchführung der Verarbeitungstätigkeit, nicht auf die Zwecke.

1.2.1.1 Nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden

Der wesentliche Teil dieses Grundsatzes ist also in dem Halbsatz „nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden" enthalten. Im Folgenden wird dieser Satz näher analysiert.

Der Satz spricht von der Vereinbarkeit mit den **Zwecken**. Aus der ersten Hälfte des Satzes geht hervor, dass es sich dabei um die Zwecke handelt**, die eindeutig festgelegt wurden**[80] (siehe Abschnitt 1.1.1.1 oben). Der Teil von Art. 5 Absatz 1 Buchstabe b, der durch [...] dargestellt wurde und weiter unten erörtert wird, verwendet ebenfalls den Begriff der „Vereinbarkeit mit den ***ursprünglichen Zwecken“***. Die *ursprünglichen Zwecke* scheinen also die gleichen zu sein wie die (bei der Konzipierung der Verarbeitungstätigkeit) angegebenen.

Art. 5 Absatz 1 Buchstabe b drückt somit aus, dass die Verarbeitung mit den folgenden Bestimmungen vereinbar sein muss:

- den **ursprünglichen Ziele selbst** oder
- **anderen Zwecke**, die mit diesen ursprünglichen Zwecken **vereinbar** sind.

Ersteres ergibt sich aus der Überlegung, dass Zwecke immer mit sich selbst vereinbar sind.

Der Wortlaut von Art. 5 Absatz 1 Buchstabe b spricht von „weiterverarbeitet“. Dies könnte zwar zeitlich verstanden werden, d. h. im Sinne von „nachdem die ursprünglichen Zwecke erreicht wurden“, doch scheint der zeitliche Aspekt für diesen Grundsatz irrelevant zu sein. Stattdessen hat „weiter“ die Bedeutung von „darüber hinaus“ ohne zeitliche Bedeutung und bezieht sich lediglich auf die Zwecke.

Die Situation wird visualisiert in Abbildung 1:

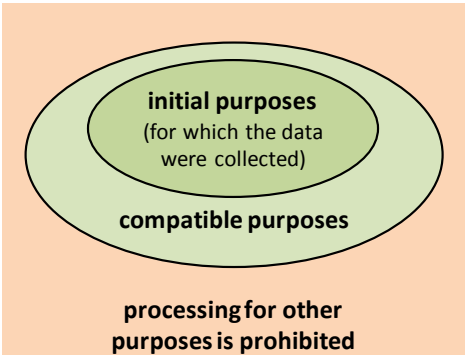

Abbildung 1: Die Verarbeitung ist für die ursprünglichen und vereinbaren Zwecke zulässig.

Es ist wichtig zu wissen, dass für die Weiterverarbeitung zu vereinbaren Zwecken keine zusätzliche Rechtsgrundlage erforderlich ist. Dies wird in Erwägungsgrund 50 der Datenschutz-Grundverordnung (2 .Satz) ausdrücklich festgestellt. Unter Bezugnahme auf die Weiterverarbeitung zu als vereinbar geltenden Zwecken heißt es dort:

> n diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten.

1.2.1.2 Verwendung für unvereinbare Zwecke

Dies wirft die Frage auf, wie es dazu kommen kann, dass personenbezogene Daten für unvereinbare Zwecke verarbeitet werden, und welche Folgen dies hat.

Um dies zu vermeiden, ist es wichtig zu verstehen, wie die Verarbeitung ablaufen kann. Die folgenden drei Beispiele veranschaulichen das Problem ohne Anspruch auf Vollständigkeit:

- **Funktionserweiterung:** Es ist üblich, dass sich die Verarbeitungstätigkeiten im Laufe der Zeit weiterentwickeln. Es ist auch üblich, dass sie dann neue Funktionen oder „Merkmale“ erhalten, die einer zusätzlichen oder geänderten Verarbeitung entsprechen. In Fällen, in denen der Verantwortliche diese Entwicklung nicht

80 Dies sind auch die Zwecke, die den betroffenen Personen gemäß Art. 13 und 14 DSGVO mitgeteilt werden.

ausreichend kontrolliert, kann die Verarbeitung unbemerkt über den ursprünglichen oder vereinbaren Zweck hinausgehen.

- **Fehlende Trennung**: Nehmen wir an, ein Verantwortlicher betreibt mehrere unabhängige Verarbeitungstätigkeiten, die unterschiedliche Zwecke verfolgen. Wenn der Verantwortliche keine angemessenen Maßnahmen ergreift, um die verschiedenen Verarbeitungstätigkeiten zu trennen, ist es leicht möglich, dass Daten, die für eine Reihe von Zwecken erhoben wurden, für andere Zwecke verwendet werden. Dies wird veranschaulicht in Abbildung 2.

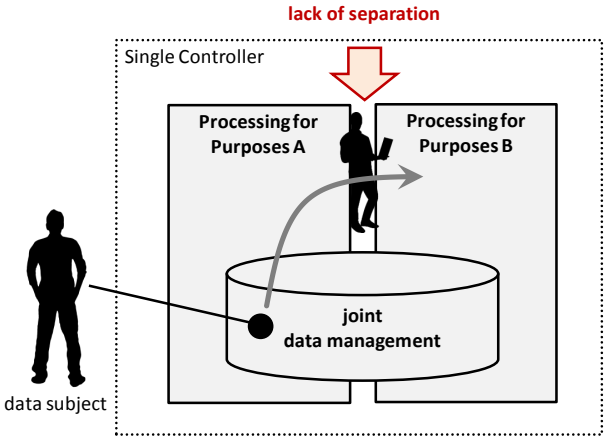

Abbildung 2: Eine fehlende Trennung führt zur Verwendung von Daten für unvereinbare Zwecke.

- **Empfänger, die ihre eigenen Zwecke verfolgen**: Empfänger sind Personen oder Organisationen, an die personenbezogene Daten weitergegeben werden (siehe Definition in Art. 4 Absatz 9 DSGVO). Empfänger können zum Beispiel sein:
    - **Mitarbeiter**, die auf Anweisung des Verantwortlichen *rechtmäßig* auf Daten zugreifen, um vereinbare Zwecke der Verarbeitung zu erfüllen, oder
    - **externe Angreifer**, die sich durch eine Sicherheitsverletzung unrechtmäßig Zugang zu den Daten verschaffen[81].

  Im letzteren Fall ist es offensichtlich, dass der Empfänger die personenbezogenen Daten für andere Zwecke verwendet. Es sind genau diese Zwecke, die den Angriff wahrscheinlich überhaupt erst motiviert haben. Aber auch Arbeitnehmer können andere Interessen an den Daten haben als die Verfolgung der angegebenen Zwecke ihres Arbeitgebers. Ein Paradebeispiel dafür ist, wenn der Mitarbeiter die betroffene Person bereits kennt und Informationen erfährt, die ihm sonst nicht zugänglich wären.

Mit dem aus diesen Beispielen gewonnenen Verständnis, wie Daten für andere Zwecke verwendet werden können, muss die Frage nach den möglichen Folgen gestellt werden.

In allen Fällen werden die Grundsätze der *Rechtmäßigkeit* und *Legitimität* **wahrscheinlich verletzt**. Nach diesen Grundsätzen ist die Verarbeitung verboten, es sei denn, sie ist durch eine nachgewiesene Rechtmäßigkeit und Legitimität der Zwecke gerechtfertigt. Dies ist natürlich nicht der Fall, wenn die Verarbeitung zu unvereinbaren und damit ungerechtfertigten Zwecken erfolgt.

Die Verwendung von Daten außerhalb und über die gerechtfertigten Zwecke hinaus **ermöglicht es den Verantwortlichen** auch, **Macht zu erlangen**. Dies kann beispielsweise der Fall sein, wenn Verantwortliche die Datensätze von Personen über verschiedene

81 Die Verantwortlichen sind nicht für die Handlungen von Angreifern verantwortlich, sondern lediglich dafür, Angriffe durch angemessene Sicherheitsmaßnahmen zu verhindern.

Verarbeitungstätigkeiten hinweg kombinieren, Daten aufbewahren und akkumulieren, wenn sie für die Zwecke nicht mehr erforderlich sind, und möglicherweise sogar Daten aus anderen Quellen erwerben, um mehr Macht über die betroffenen Personen zu erlangen. Eine solche angehäufte Macht übersteigt offensichtlich den Machtgewinn, der durch eine nachgewiesene Rechtmäßigkeit und Legitimität der ursprünglichen Zwecke gerechtfertigt war.

Es liegt auf der Hand, dass über die bloße Verletzung von Datenschutzgrundsätzen hinaus je nach den Zwecken, für die die Daten (miss)verwendet werden, den **betroffenen Personen** auch **materieller oder immaterieller Schaden** entstehen kann. So kann beispielsweise die Kenntnis bestimmter Gesundheitsdaten Beziehungen erheblich beeinträchtigen, wenn sie für Bekannte zugänglich sind, oder Beschäftigungsmöglichkeiten verhindern, wenn sie für potenzielle Arbeitgeber zugänglich sind. Wenn sie zu kriminellen Zwecken verwendet werden, können einige Arten von Daten die Grundlage für Erpressung sein.

1.2.1.3 Wann sind die Zwecke vereinbar?

Im Folgenden wird erörtert, wie festgestellt werden kann, ob potenzielle zusätzliche Zwecke als vereinbar angesehen werden. Dies stützt sich in erster Linie auf Art. 6 Absatz 4 DSGVO.

In Fällen, in denen als **Rechtsgrundlage für** die Verarbeitung eine ***Einwilligung*** (siehe Art. 6 Absatz 1 Buchstabe a DSGVO) für die Verarbeitung gewählt wurde, **gilt eine** weitere Verarbeitung für andere **Zwecke** als die zuvor genehmigten, vereinbaren Zwecke (siehe unten) **als unvereinbar**[82]. Dies liegt daran, dass die Einwilligung immer nur für bestimmte Zwecke[83] gilt. Eine „Ausweitung" der Verarbeitungszwecke über die angegebenen Zwecke hinaus, in die eine betroffene Person eingewilligt hat, wäre eindeutig unfair und intransparent.

Art. 6 Absatz 4 sieht dann die folgenden **Kriterien** vor, die von den Verantwortlichen anzuwenden sind, um festzustellen, ob ein zusätzlicher Zweck vereinbar ist (im Vergleich zur DSGVO leicht umformuliert):

(a) jegliche **Verbindung zwischen** den **ursprünglichen Zwecken** und den in Frage kommenden **zusätzlichen Zwecken;**

(b) der **Kontext, in dem** die personenbezogenen **Daten erhoben wurden**, insbesondere die **Beziehung** zwischen den **betroffenen Personen** und dem **Verantwortlichen**;

(c) die **Art der personenbezogenen Daten**, insbesondere ob es sich um **besondere Kategorien von** (d. h. sensiblen) personenbezogenen **Daten handelt** oder ob personenbezogene Daten im Zusammenhang mit **strafrechtlichen Verurteilungen** und **Straftaten** verarbeitet werden;

(d) die **möglichen Folgen** der beabsichtigten Weiterverarbeitung **für die betroffenen Personen**;

(e) das **Vorhandensein geeigneter Garantien**, zu denen auch die **Pseudonymisierung** gehören kann.

Weitere Hinweise und Beispiele für die Anwendung dieser Kriterien sind bei der *Artikel-29-Datenschutzgruppe* erhältlich[84]. Diese Stellungnahme bezieht sich zwar auf die

82 Beachten Sie, dass Art. 6 Absatz 4 DSGVO über vereinbare Zwecke ausdrücklich ausschließt, dass er anwendbar ist, wenn die Rechtsgrundlage die Einwilligung ist.

83 Insbesondere werden diese Zwecke in dem Dialog angegeben, in dem um Einwilligung gebeten wird, und die Angabe ist ein wichtiger Aspekt der Einwilligung in Kenntnis der Sachlage.

84 rtikel-29-Datenschutzgruppe, 00569/13/EN, WP203, Stellungnahme 03/2013 zur Zweckbindung, angenommen am 2. April 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (zuletzt besucht am 28.05.2020).

Datenschutzrichtlinie (d. h. den Vorläufer der DSGVO), aber viele Aspekte sind auch heute noch gültig.

Um die Feststellung zu vereinfachen, ob zusätzliche Zwecke vereinbar sind, werden in der **Datenschutz-Grundverordnung einige** der häufigsten zusätzlichen **Zwecke**, die bei der Weiterverarbeitung verfolgt werden, **vorab genehmigt**. Art. 5 Absatz 1 Buchstabe b umfasst die folgenden Zwecke:

> [Die Weiterverarbeitung zu **im öffentlichen Interesse liegenden** Archivzwecken, zu **wissenschaftlichen oder historischen Forschungszwecken** oder zu **statistischen** Zwecken gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken.

Der erwähnte Art. 89 Absatz 1 verlangt das Vorhandensein zusätzlicher Garantien.

Hier schreibt der erwähnte Art. 89 DSGVO vor, dass die Weiterverarbeitung zu diesen vorab genehmigten Zwecken nur zulässig ist, wenn angemessene Garantien vorhanden sind.

1.2.2 Verwandte Artikel und Erwägungsgründe

Das **Wesen** des Grundsatzes der Zweckbindung ist in **Art. 5 Absatz 1 Buchstabe b** DSGVO beschrieben und enthält auch die Auflistung der **vorab genehmigten vereinbaren Zwecke**.

Art. 5 Absatz 1 Buchstabe e DSGVO enthält weitere Einzelheiten über die mögliche **Speicherfrist** von Daten im Zusammenhang mit der Weiterverarbeitung **zu den vorab genehmigten, als vereinbar geltenden Zwecken**.

Erwägungsgrund 50 der Datenschutz-Grundverordnung enthält Leitlinien für die Auslegung der Weiterverarbeitung zu als vereinbar geltenden Zwecken. Von besonderem Interesse ist der zweite Satz, der besagt, dass **keine andere gesonderte Rechtsgrundlage erforderlich ist als diejenige für die Erhebung der personenbezogenen Daten**.

Art. 89 DSGVO schreibt vor, dass die Verantwortlichen bei der Weiterverarbeitung zu **im Voraus genehmigten, als vereinbar geltenden Zwecken angemessene Garantien** vorsehen müssen. Er eröffnet auch die Möglichkeit, dass in diesem Zusammenhang das Unionsrecht oder das Recht der Mitgliedstaaten **Ausnahmen von bestimmten Rechten der betroffenen Person** vorsehen kann.

1.2.3 Damit verbundene technische und organisatorische Maßnahmen

Im Folgenden finden Sie Beispiele für technische und organisatorische Maßnahmen zur Unterstützung der *Zweckbindung*:

- Eine genaue und klare Spezifizierung der ursprünglichen und potenziell als vereinbar geltenden Zwecke ist eine Voraussetzung für jegliche Überlegungen zur Trennung der Zwecke.
- Datenschutz als einen Prozess zu verstehen, der **regelmäßige Überprüfungen** während des gesamten Lebenszyklus der Verarbeitungstätigkeit umfasst, ist wichtig, um zu vermeiden, dass Daten zu unvereinbaren Zwecken verarbeitet werden, z. B. aufgrund einer **schleichenden Ausweitung der Funktionen**. Beachten Sie, dass eine regelmäßige Überprüfung im Zusammenhang mit dem *Datenschutz durch Technikgeschaltung* (Artikel 25 Absatz 1 DSGVO), der *Datenschutz-Folgenabschätzung* (Artikel 35 Absatz 11 DSGVO) und der *Sicherheit* (Artikel 32 Absatz 1 Buchstabe d DSGVO) vorgeschrieben ist.
- Die **Überprüfung der Vereinbarkeit der Zwecke** nach Art. 6 Absatz 4 kann als eine organisatorische Maßnahme zur Unterstützung der Zweckbindung angesehen werden.

- Eine weitere organisatorische Maßnahme ist die **Analyse**, inwieweit **befugte Mitarbeiter** personenbezogene Daten **für andere Zwecke** nutzen können. Eine solche Analyse zielt darauf ab, mögliche **Motivationen**, **Interessenkonflikte** (z. B. Personal, das Daten von Verwandten und Bekannten verarbeitet) und Maßnahmen zur **Verhinderung**[85] **oder Entschärfung** solcher Situationen zu ermitteln (z. B. die Möglichkeit, dass ein Mitarbeiter einen Interessenkonflikt für einen zugewiesenen Fall signalisieren und diesen an einen anderen Mitarbeiter ohne Interessenkonflikt weitergeben kann).
- Eine weitere Maßnahme ist die Analyse der **Beweggründe**, die **externe Angreifer** haben könnten, um die Daten für andere Zwecke zu erhalten. Dies ist ein wichtiger Teil der Risikobewertung und eine Voraussetzung für die Einführung geeigneter Garantien zur Unterstützung der Zweckbindung.
- Alle organisatorischen oder technischen Maßnahmen zur **Trennung verschiedener Verarbeitungstätigkeiten**, die von demselben Verantwortlichen durchgeführt werden, unterstützen unmittelbar die Zweckbindung.
- Jede Maßnahme (z. B. Verschlüsselung) zur Wahrung **der Vertraulichkeit** verhindert, dass Unbefugte die Daten für unrechtmäßige Zwecke nutzen können.
- Jede Maßnahme, die sicherstellt, dass **befugtes Personal nur auf Anweisung und nach Weisung** des Verantwortlichen handelt (siehe Art. 29 und 32 Absatz 4 DSGVO) stellt sicher, dass die Verarbeitung nicht über das hinausgeht, was zur Erreichung der angegebenen Zwecke erforderlich ist.
- Eine sekundäre Maßnahme, die den Schaden nach einer Sicherheitsverletzung mindert, ist die **Pseudonymisierung**. Die drastisch eingeschränkte Möglichkeit, betroffene Personen zu identifizieren und mit anderen Datensätzen zu verknüpfen, kann in vielen Fällen die Verwendung der durchgesickerten Daten für andere Zwecke wirksam verhindern.

1.3 Datenminimierung

B*ud P. Bruegger (ULD)*

Danksagung: Der Autor dankt Andrès Chomczyk Penedo (VUB), der eine Analyse dieses Grundsatzes als Beitrag zu der hier vorgestellten Beschreibung verfasst hat.

Im Folgenden wird der Grundsatz der *Datenminimierung* erörtert, der in Art. 5 Absatz 1 Buchstabe c DSGVO definiert ist.

***Datenminimierung* auf einen Blick:**

Die Datenminimierung beschränkt die erhobenen und verwendeten Daten auf diejenigen, die dem Zweck **angemessen** und **erheblich** sowie auf **das für die Zwecke der**

85 Ein weiteres Beispiel zur Vermeidung von Interessenkonflikten ist, wenn ein großes Unternehmen die Datenverarbeitung in Büros durchführt, die weit von den betroffenen Personen entfernt sind, um die Wahrscheinlichkeit zu verringern, dass Mitarbeiter Daten von Bekannten verarbeiten.

Verarbeitung notwendige Maß beschränkt sind. Die Beschränkung auf das notwendige Maß hat zwei Aspekte:

- Datenmenge (oder genauer gesagt, Informationsgehalt) und
- Dauer der Speicherung.

Folglich sollten so wenig Daten wie nötig für einen so kurzen Zeitraum wie möglich verarbeitet werden (einschließlich der Speicherung), ohne dass der angegebene Zweck verfehlt wird.

1.3.1 Beschreibung

In „*Datenschutz verstehen: Die EU-Verordnung in Kurzform*“ wurde die *Datenminimierung* mit dem Ziel begründet, den Machtgewinn des Verantwortlichen auf das Minimum zu beschränken, das zur Einhaltung der erklärten, rechtmäßigen Zwecke erforderlich ist. Insbesondere ging es um die Minimierung des Informationsgehalts der verarbeiteten personenbezogenen Daten. Dies ergänzt die Minimierung des Grades der Assoziation, den die Daten mit der betroffenen Person haben, und die Begrenzung des Zugangs zur Macht. Siehe *Minimierung der Befugnisse auf das für die Einhaltung der erklärten Zwecke erforderliche Maß* für weitere Einzelheiten.

In der Datenschutz-Grundverordnung wird dieser Grundsatz wie folgt definiert:

Definition laut Art. 5 Absatz 1 Buchstabe c DSGVO:

Personenbezogene Daten müssen **dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein** („*Datenminimierung*“);

Dies ist natürlich nur möglich, wenn diese Zwecke festgelegt und ausdrücklich genannt werden (wie laut Art. 5 Absatz 1 Buchstabe b DSGVO gefordert).

1.3.1.1 Angemessen, erheblich und beschränkt

Angemessen und ***erheblich*** sind leicht zu verstehen: Daten, die unangemessen, d. h. für die Zwecke ungeeignet sind, dürfen nicht erhoben oder verarbeitet werden; die Daten müssen auch erheblich sein, d. h. den Zwecken dienen.

Um den Aspekt der ***Beschränkung*** zu verstehen, ist eine genauere Betrachtung dessen erforderlich, was *Daten* eigentlich bedeuten. Insbesondere ist intuitiv klar, dass es hier nicht nur um die Anzahl der Datenelemente geht, sondern um den eigentlichen **Informationsgehalt** der Daten. Im Folgenden soll dies in Bezug auf die Zwecke verdeutlicht werden:

- **Auswahl**: Wenn eine Reihe möglicher Datenelemente in Betracht gezogen wird, sind diejenigen **auszuwählen,** die für die Zwecke erforderlich sind. Wenn die Daten bereits gespeichert sind, kann die Auswahl auch als **Löschung** unnötiger Datenelemente verstanden werden. Ansonsten handelt es sich um Daten, die tatsächlich erhoben werden.
- **Auflösung**: Wenn Daten in mehreren möglichen Auflösungen verfügbar sind, **sollten Sie die Auflösung** auf das für den Zweck erforderliche Minimum beschränken. Zum Beispiel:
    - **Werte**: drücken Sie **Werte** auf der **gröbsten Skala** aus, die den Zweck noch unterstützt:

        - Verwenden Sie beispielsweise eine **Alterskategorie** (40–59 Jahre alt, Auflösung von 20 Jahren) **anstelle** eines **Geburtsdatums** (Auflösung von einem Tag)
    - **Orte**: Drücken Sie **Orte in der** gröbsten geografischen Unterteilung aus:
        - z. B. **Verwaltungseinheiten** wie Postleitzahlengebiete oder Provinzen oder **Gitterzellen** anstelle von exakten Koordinaten (mit metergenauer Auflösung)
    - **Zeitreihen**: Stellen sie **Zeitreihen** von Daten mit der gröbsten Abtastrate dar, die noch für den Zweck geeignet ist:
        - Dies kann eine Neuabtastung der von einem bestimmten Sensor erhaltenen Daten erfordern
    - **Fingerabdrücke**: Wenn Sie Datensätze **nur** auf **Gleichheit** vergleichen müssen, sollten Sie nur einen „**Fingerabdruck“** der Daten verarbeiten:
        - So kann zum Beispiel ein „kryptographischer Hash-Wert“ (auch „Digest“ genannt) der Daten ausreichen, um Änderungen[86] zu erkennen
- **Grad der Aggregation**: Wählen Sie nach Möglichkeit eine angemessene **Aggregationsebene**. Bei den meisten Datenwerten, mit denen wir zu tun haben, handelt es sich um eine Form der Aggregation, auch wenn dies nicht immer offensichtlich ist, da sie möglicherweise „unsichtbar“ durch einen Sensor oder eine Datenerfassungsmethode erfolgt. Die Aggregation ist eine Möglichkeit, **mehrere Datenelemente durch ein einziges zu ersetzen**. Paradebeispiele kommen aus der Statistik und umfassen den Durchschnitt, den Median, das Minimum und das Maximum. Im Zusammenhang mit dem Datenschutz müssen zwei Arten der Aggregation unterschieden werden:
    - **Einzelne Person**: Aggregation von Datenelementen, die sich auf eine **einzelne Person** beziehen:
        - Nimmt man z. B. das Durchschnittseinkommen einer Person über ein Jahr, so verringert sich der Informationsgehalt über diese Person.
    - **Mehrere Personen**: Aggregation von Datenelementen, die sich auf eine **Vielzahl von Personen** beziehen:
        - Nimmt man beispielsweise das durchschnittliche Jahreseinkommen über eine Gruppe von Personen, so verringert sich auch der Gesamtinformationsgehalt (Datenminimierung). Darüber hinaus wird dadurch auch der Grad der Assoziation zwischen einem Datenelement und einer bestimmten Person abgeschwächt. Diese Art der Aggregation ist daher auch für die Speicherbegrenzung relevant (siehe Abschnitt 1.5)

1.3.1.2 Zeitlicher Aspekt

Die Datenminimierung hat natürlich auch einen **zeitlichen Aspekt**. Vor allem bedeutet „Beschränkung auf das für die Zwecke erforderliche Maß“ auch, dass es nicht mehr gerechtfertigt ist, Daten zu speichern, wenn die Zwecke bereits erfüllt sind. Die Daten müssen daher **gelöscht werden, sobald sie nicht mehr erforderlich sind**.

86 Weitere Informationen über kryptografische Prüfsummen finden Sie z. B. unter https://en.wikipedia.org/wiki/Cryptographic_hash_function (zuletzt besucht am 15.5.2020).

In der Praxis kann dies sogar noch **vielfältiger** sein: Von den Zwecken (Plural) können einige früher erfüllt werden als andere. Auch kann nach der „Hauptverarbeitung“[87] eine „Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“[88] erfolgen. Um dies zu modellieren, unterscheiden wir mehrere **Phasen der Verarbeitung**. Die folgende Abbildung versucht, diese Situation zu veranschaulichen.

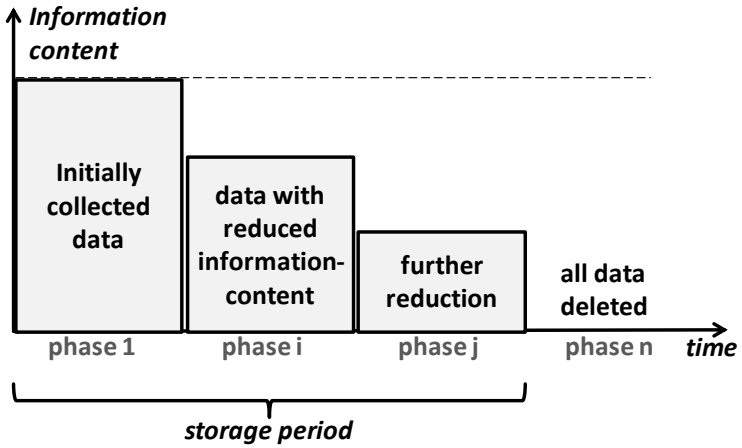

Abbildung 3: Reduktion des Informationsgehalts in mehreren Schritten.

Die Abbildung zeigt insbesondere ein Beispiel mit vier Phasen. Es ist eine beliebige Anzahl von Phasen möglich. Da jede Phase mit einer Teilmenge von Zwecken verbunden ist, sind am Ende jeder Phase, wenn die jeweiligen Zwecke erfüllt sind, bestimmte Daten nicht mehr erforderlich. Folglich können am **Ende jeder Phase** bestimmte Daten **entweder gelöscht** (Auswahl) oder ihr **Informationsgehalt reduziert werden** (Verringerung der Auflösung oder Erhöhung des Aggregationsgrades). Es liegt auf der Hand, dass ein solcher diversifizierter Ansatz die Datenmenge weiter minimiert als ein einphasiger Ansatz, bei dem der gesamte Informationsgehalt erhalten bleibt, bis alle Zwecke erfüllt sind.

1.3.2 Verwandte Artikel und Erwägungsgründe

Neben der Definition der *Datenminimierung* in Art. 5 Absatz 1 Buchstabe c, legt der zweite Teil von Art. 5 Absatz 1 Buchstabe e DSGVO „Speicherbegrenzung“ ausdrücklich fest, dass:

> [P]ersonenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden;

Dies bezieht sich auf die Weiterverarbeitung zu als vereinbar geltenden Zwecken nach Einhaltung der ursprünglichen Zwecke gemäß Art. 5 Absatz 1 Buchstabe b DSGVO[89].

87 Der Begriff "Hauptverarbeitung" wird hier zur Unterscheidung von "Weiterverarbeitung" verwendet.
88 Die Formulierung wurde direkt aus Art. 5 Absatz 1 Buchstabe b DSGVO übernommen.
89 Namentlich Art. 5 Absatz 1 Buchstabe b enthält die folgende Aussage: „Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke

Da dieser die Speicherung personenbezogener Daten betrifft, wird er hier als relevant für die Datenminimierung betrachtet, da die Aussage „auf das für die Zwecke erforderliche Maß beschränkt“ nicht nur auf die Datenmenge beschränkt ist, sondern eindeutig auch den zeitlichen Aspekt der Daten betrifft. Außerdem bezieht sich die Datenminimierung auf alle Aspekte der Verarbeitung (z. B. *Erhebung* und *Offenlegung*) und somit auch auf die *Speicherung*.

Aus diesen Gründen wird der zweite Teil von Art. 5 Absatz 1 Buchstabe e DSGVO betrachtet, um eine Orientierungshilfe für die Auslegung des Grundsatzes der Datenminimierung im Zusammenhang mit der Weiterverarbeitung für als vereinbar geltende Zwecke nach Einhaltung der ursprünglichen Zwecke zu geben.

Darüber hinaus unterstreicht die Datenschutz-Grundverordnung die Bedeutung dieses Grundsatzes in verschiedenen Zusammenhängen:

In Art. 25 Absatz 1 DSGVO über den ***Datenschutz durch Technikgestaltung*** wird betont, dass die ***Datenminimierung*** **in jeder Phase des Lebenszyklus** einer Verarbeitungstätigkeit **berücksichtigt werden** muss. Dazu gehört zum Beispiel die Analyse- und Konzeptionsphase einer Verarbeitungstätigkeit, in der die Zwecke der Verarbeitung festgelegt werden: Je genauer und enger die Zwecke festgelegt werden, desto klarer wird, welche Daten tatsächlich notwendig sind, und desto mehr Daten können als unnötig erkannt werden. In ähnlicher Weise können in einer späteren Phase des Lebenszyklus Maßnahmen ergriffen werden, um eine effektive Löschung oder Reduzierung des Informationsgehalts zu erreichen.

Art. 89 Absatz 1 und Erwägungsgrund 156 DSGVO betonen die **Bedeutung der *Datenminimierung*** für den Fall, dass die Daten nach Einhaltung der ursprünglichen Zwecke für „als vereinbar geltende Zwecke“ weiterverarbeitet werden[90]. Insbesondere „im öffentlichen Interesse liegende Archivzwecke, **wissenschaftliche** oder **historische Forschungszwecke** oder **statistische Zwecke gelten** gemäß Artikel 89 Absatz 1 nicht als mit den ursprünglichen Zwecken unvereinbar“[91]. Art. 89 Absatz 1 DSGVO (2. Satz) schreibt ausdrücklich vor, dass für diese Weiterverarbeitung „technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird“.

1.3.3 Damit verbundene technische und organisatorische Maßnahmen

Im Folgenden werden Beispiele für technische oder organisatorische Maßnahmen zur Unterstützung der Datenminimierung aufgeführt. Sie erheben keinen Anspruch auf Vollständigkeit, sondern dienen vielmehr der Konkretisierung des Grundsatzes:

- **Wissen, welche Daten für die Zwecke erforderlich sind**: Zu wissen, welche Daten tatsächlich erforderlich sind, ist nur mit einer genauen und engen Definition der Zwecke möglich. Herauszufinden, was wirklich benötigt wird, ist eine Maßnahme zur Unterstützung der Datenminimierung, die typischerweise während der Konzeptions- oder Entwurfsphase einer Verarbeitungstätigkeit durchgeführt wird.
- **Erfassen nur der notwendigen Daten**: In der Entwurfsphase und bei der Auswahl, Implementierung und/oder Konfiguration von Software ist die Datenerfassung, z. B.

---

oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als mit den ursprünglichen Zwecken unvereinbar“.

90 Siehe Art. 5 Absatz 1 Buchstabe b DSGVO.

91 Wortlaut entnommen aus Art. 5 Absatz 1 Buchstabe b DSGVO.

durch Eingabeformulare oder Dialoge, so zu gestalten, dass nur die notwendigen Daten in der erforderlichen Detailtiefe erfasst werden.

- **Löschen von Daten und Reduzierung des Informationsgehalts zwischen den Verarbeitungsphasen**[92]: Planen und implementieren Sie die Funktionalität, unnötige Daten am Ende von Verarbeitungsphasen zu löschen oder ihren Informationsgehalt anderweitig zu reduzieren.
- **Schutz gegen die Überschreitung des maximalen Speicherzeitraums**: Als zweite Verteidigungslinie sollten Sie eine *maximale Speicherfrist* festlegen[93] und ein Verfahren einführen, das Sie über das Vorhandensein von Daten informiert, die diese Dauer überschritten haben. Diese Maßnahme schützt vor Fehlern bei der Löschung, z. B. durch einen Softwarefehler, der in bestimmten Fällen auftritt, einen Systemabsturz während des Löschvorgangs oder die Wiederherstellung von Daten aus einem Backup nach einem Systemabsturz, obwohl die Daten zuvor bereits gelöscht worden waren.

1.4 Richtigkeit

Bud P. Bruegger (ULD)

Danksagung: Der Autor dankt Frédéric Tronnier (GUF), der eine Analyse dieses Grundsatzes als Beitrag zu der hier vorgestellten Beschreibung verfasst hat.

Im Folgenden wird der Grundsatz der *Richtigkeit* erörtert, der in Art. 5 Absatz 1 Buchstabe d DSGVO definiert ist.

***Richtigkeit* auf einen Blick:**

Die Richtigkeit der Daten betrifft sowohl die **sachliche Richtigkeit** als auch die **Aktualität**. Es ist verboten, unrichtige Daten zu verwenden, die für den Zweck ungeeignet sind oder negative Folgen für die betroffenen Personen haben. Die wichtigste Maßnahme zur Umsetzung dieses Grundsatzes besteht darin, das **Recht der** betroffenen Personen **auf Berichtigung** angemessen zu unterstützen.

1.4.1 Beschreibung

In „*Datenschutz verstehen: Die EU-Verordnung in Kurzform"* wurde die *Richtigkeit* (zusammen mit der Integrität) mit der Tatsache begründet, dass die Richtigkeit der Daten notwendig ist, um für die erklärten Zwecke geeignet zu sein. Eine Verarbeitung, die nicht

92 Beachten Sie, dass sich diese Aussage auf die Gesamtheit der von dem Verantwortlichen gespeicherten Daten bezieht. Außerdem wird hier davon ausgegangen, dass die Daten nur einmal von/über die betroffenen Personen erhoben werden und dass keine spätere Datenerhebung (z. B. bei Bedarf) stattfindet. Die Erklärung schließt nicht aus, dass verschiedene Phasen oder Verarbeitungsschritte nur eine Teilmenge der Gesamtdaten verwenden.

93 Hierbei könnte es sich direkt um „den Zeitraum, für den die personenbezogenen Daten gespeichert werden" im Sinne von Art. 13 Absatz 2 Buchstabe a handeln oder, wenn die Speicherfrist von Kriterien abhängt, den maximalen Zeitraum, in dem erwartet werden kann, dass diese Bedingungen erfüllt sind.

zweckdienlich ist, kann keinen Machtzuwachs gegenüber einer betroffenen Person rechtfertigen. Siehe *Verbot einer nicht zweckdienlihen Verarbeitung* für weitere Einzelheiten.

Neben der Zweckmäßigkeit kann die Verarbeitung unrichtiger Daten auch negative Folgen für die betroffenen Personen haben. Diese können von einem erhöhten Aufwand, der zur Ausübung ihrer Rechte erforderlich ist, über die Verneinung von Rechten und Möglichkeiten bis hin zu negativen finanziellen oder rechtlichen Folgen reichen. Eine Verarbeitung, die mit solchen Mängeln behaftet ist, ist wohl nicht zweckmäßig, würde aber zusätzlich gegen den Grundsatz der *Verarbeitung nach Treu und Glauben* verstoßen (siehe ***¡Error! No se encuentra el origen de la referencia.*** oben).

In der Datenschutz-Grundverordnung wird dieser Grundsatz wie folgt definiert:

Definition laut Art. 5 Absatz 1 Buchstabe d DSGVO:

Personenbezogene Daten müssen **sachlich richtig** und erforderlichenfalls auf dem **neuesten Stand** sein; es sind **alle angemessenen Maßnahmen** zu treffen, damit **personenbezogene Daten, die im Hinblick auf die** Zwecke ihrer Verarbeitung **unrichtig sind,** unverzüglich **gelöscht oder berichtigt werden** („*Richtigkeit*“);

Im Folgenden werden verschiedene Aspekte der *Richtigkeit* näher erläutert:

1.4.1.1 Wie lässt sich die Richtigkeit beurteilen?

Der Begriff der Richtigkeit muss objektiv sein. Es muss zweifelsfrei überprüfbar sein, ob die Daten richtig sind oder nicht, und verschiedene Prüfer müssen zu derselben Einschätzung kommen. Dies ist nur möglich, wenn die Daten **nachprüfbare Tatsachen** darstellen. Dies ist zum Beispiel nicht der Fall bei Daten, die eine Äußerung oder Meinung einer Person darstellen.

Die Überprüfung der Richtigkeit von Daten beinhaltet daher in der Regel die Überprüfung der den Daten zugrunde liegenden Fakten. Um beispielsweise zu überprüfen, ob eine Mobiltelefonnummer tatsächlich zu einer Person gehört, könnte eine Testnachricht mit einem Zufallscode über einen anderen Kanal gesendet und wieder empfangen werden.

In einigen Fällen kann es die betroffene Person sein, die dem Verantwortlichen die erforderlichen Nachweise für Fakten vorlegt, die eine Überprüfung ermöglichen. So kann eine betroffene Person beispielsweise eine von einer vertrauenswürdigen Behörde ausgestellte Wohnsitzbescheinigung vorlegen, um die Überprüfung einer Wohnsitzadresse zu unterstützen.

1.4.1.2 Was bedeutet „auf dem neuesten Stand“?

Bei der Beurteilung des neusten Stands von Daten sind die Zwecke der Verarbeitung zu berücksichtigen. So kann ein Verkäufer beispielsweise die Lieferadresse einer betroffenen Person speichern, obwohl diese inzwischen umgezogen ist. Wenn der Zweck der Verarbeitung darin besteht, der betroffenen Person tatsächlich Waren zu liefern, ist die Adresse offensichtlich nicht mehr auf den neuesten Stand und die Daten sind für den Zweck ungeeignet. Besteht der Zweck der Verarbeitung jedoch in der Rechnungsstellung für bereits gelieferte Waren, so ist die alte Adresse als aktuell zu betrachten.

1.4.1.3 Wie wird die Unrichtigkeit von Daten entdeckt?

Unrichtige (einschließlich veralteter) Daten müssen von dem Verantwortlichen unverzüglich berichtigt oder gelöscht werden. Aber wie wird die Unrichtigkeit der Daten eigentlich entdeckt und welche Verantwortung tragen die Verantwortlichen?

Der wahrscheinlich wichtigste Mechanismus für Verantwortliche, um Unrichtigkeiten in ihren Daten aufzudecken, ist die **Benachrichtigung durch die betroffene Person**[94]. Insbesondere muss die betroffene Person über die Verarbeitung informiert sein (siehe Artikel 13 und 14 DSGVO) und Zugang zu den von dem Verantwortlichen verwendeten Daten haben (siehe Artikel 15 DSGVO). Auf dieser Grundlage kann sie die Richtigkeit ihrer Daten überprüfen und gegebenenfalls ihr **Recht** auf **Berichtigung** ihrer Daten geltend machen (siehe Art. 16 DSGVO). In diesem Fall erfüllt der Verantwortliche die Verpflichtung zur Überprüfung der Richtigkeit der Daten, indem er das Recht auf Berichtigung in angemessener Weise unterstützt.

Wenn Daten direkt bei den betroffenen Personen erhoben werden, kann der Verantwortliche in den meisten Fällen davon ausgehen, dass die erhaltenen Daten (zumindest zum Zeitpunkt der Erhebung) richtig sind. Die Situation kann anders sein, wenn die Daten von einer anderen Quelle erhoben werden. In diesem Fall ist der Verantwortliche verpflichtet, die Richtigkeit der erhaltenen Daten zu überprüfen, zumindest im Hinblick auf ihre Eignung für die erklärten Zwecke der Verarbeitung und auf etwaige negative Folgen, die Unrichtigkeiten für die betroffenen Personen haben können.

Bei einigen Datenelementen reicht die Tatsache, dass sie direkt bei den betroffenen Personen erhoben wurden, möglicherweise nicht aus, damit ein Verantwortlicher von der Richtigkeit ausgehen kann. Dies ist insbesondere dann der Fall, wenn eine möglicherweise unzutreffende Angabe zu Vorteilen für die betroffene Person führt. In diesen Fällen muss der Verantwortliche unter Umständen im Vorfeld eine Überprüfung der Daten als integralen Bestandteil der Datenerhebung vornehmen. Dies ist beispielsweise möglich, indem die betroffenen Personen aufgefordert werden, die behaupteten Tatsachen von einer vertrauenswürdigen Stelle bestätigen zu lassen.

1.4.2 Verwandte Artikel und Erwägungsgründe

Der Artikel der Datenschutz-Grundverordnung, der am engsten mit dem Grundsatz der *Richtigkeit* verbunden ist, ist das ***Recht auf Berichtigung***. Seine Bedeutung wurde bereits in Abschnitt 1.4.1.3 erörtert. Angemessene **Informationen**, die das Bewusstsein der betroffenen Personen für die Verarbeitung schärfen (**Artikel 13 und 14 DSGVO**), und das **Recht auf Auskunft über** die Daten, die sich im Besitz des Verantwortlichen befinden (**Artikel 15**), können als notwendig angesehen werden, um das Recht auf Berichtigung zu ermöglichen.

Wenn ein Verantwortlicher einem Antrag auf Berichtigung nicht sofort nachkommen kann (gemäß Artikel 16 DSGVO), sondern eine angemessene Zeit benötigt, um die Richtigkeit der fraglichen Daten zu überprüfen, kann es erforderlich sein, **die Verarbeitung** der Daten **einzuschränken** (siehe **Artikel 18 Absatz 1 Buchstabe a DSGVO)**. Nach der Überprüfung der Richtigkeit und der erfolgten Berichtigung muss der Verantwortliche die **betroffene Person** gemäß **Art. 12 Absatz 3** DSGVO informieren. Stellt der Verantwortliche fest, dass die Daten tatsächlich richtig sind und nicht berichtigt werden müssen, muss er **die betroffene Person** gemäß **Art. 12 Absatz 4** DSGVO informieren. Wurde die Verarbeitung eingeschränkt, so kann die betroffene Person **der Aufhebung der Einschränkung** auch ohne

94 Andere Mechanismen sind zum Beispiel Konsistenzprüfungen, übermäßige Varianz oder ein Mangel an erwarteter Korrelation.

Berichtigung **zustimmen** (siehe **Art. 18 Absatz 2** DSGVO). Liegt eine solche Einwilligung nicht vor, kann der Verantwortliche **die Daten** entweder **löschen** (siehe **Art. 5 Absatz 1 Buchstabe d DSGVO**) oder seinen Datenschutzbeauftragten beauftragen, **die Aufsichtsbehörde** in dieser Angelegenheit zu **konsultieren** (siehe **Art. 39 Absatz 1 Buchstabe e DSGVO**).

Falls der Verantwortliche die Daten an **Empfänger** weitergegeben hat, **müssen** diese **ebenfalls** auf die Unrichtigkeit hingewiesen werden (gemäß **Artikel 19** DSGVO). Insbesondere sind die Verantwortlichen verpflichtet, die Empfänger über die vorgenommenen Berichtigungen zu informieren. In Anbetracht der Tatsache, dass die Überprüfung der Richtigkeit von den Zwecken der Verarbeitung abhängen kann (siehe 1.4.1.2 oben), kann es sinnvoll und zeitnaher sein, die Empfänger bereits freiwillig über den Antrag auf Berichtigung zu informieren. Ein solcher erweiterter Ansatz deckt dann auch den Fall ab, dass die Daten für den Verantwortlichen richtig sind, aber bei einem der Empfänger berichtigt werden müssen.

Betroffene Personen haben auch das **Recht, über solche Meldungen informiert zu werden** (siehe **Artikel 19** Satz 2 DSGVO). Diese Informationen umfassen die Nennung der einzelnen Empfänger[95].

1.4.3 Damit verbundene technische und organisatorische Maßnahmen

Jede organisatorische oder technische Maßnahme zur Unterstützung der Aufdeckung von Unrichtigkeiten oder zur rechtzeitigen Berichtigung (oder Löschung) von Daten unterstützt den Grundsatz der *Richtigkeit*. Um zu verstehen, wann die Richtigkeit besonders wichtig ist und strengere Maßnahmen erforderlich sind, ist eine Analyse erforderlich, wie sich Unrichtigkeiten auf die Zweckmäßigkeit beziehen und wie sie sich nachteilig auf die betroffenen Personen auswirken können.

Beispiele für mögliche Maßnahmen zur Unterstützung der Richtigkeit sind:

- Eine organisatorische Maßnahme zum Zeitpunkt der Konzeption ist die Analyse des minimalen Richtigkeitsgrades, der erforderlich ist, um für den Zweck geeignet zu sein.
- Eine organisatorische Maßnahme zum Zeitpunkt der Konzeption ist die Analyse der möglichen negativen Auswirkungen, die unrichtige Daten auf die Betroffenen haben können.
- Eine Maßnahme zum Zeitpunkt der Konzeption ist die Analyse der Richtigkeit von Daten, die aus anderen Quellen als den betroffenen Personen selbst stammen.
- Eine weitere ist die Analyse, ob bestimmte Datenelemente im Vorfeld überprüft werden müssen (siehe 1.4.1.3 oben).
- Eine weitere zeitlich begrenzte Maßnahme ist die Formulierung von Anforderungen zur Unterstützung des Rechts auf Information (Art. 13 oder 14 DSGVO), des Rechts auf Auskunft (Art. 15 DSGVO) und vor allem des Rechts auf Berichtigung (Art. 16 DSGVO).
- Das Gleiche gilt für die Durchführung von Benachrichtigungen der Empfänger (Art. 19 DSGVO) über Unrichtigkeit und Berichtigung.
- Zum Zeitpunkt der Durchführung der Verarbeitungstätigkeit ist die Benennung von Personal für eventuelle manuelle Eingriffe, die zur Überprüfung der Richtigkeit oder

95 Dies ist interessant, da es laut Art. 13 Absatz 1 Buchstabe e und Art. 14 Absatz 1 Buchstabe e genügt, über Kategorien von Empfängern zu informieren.

zur Vornahme von Berichtigungen erforderlich sind, eine mögliche organisatorische Maßnahme.

- Das Gleiche gilt für die Vorbereitung des Datenschutzbeauftragten auf die wirksame Bearbeitung von Berichtigungsanträgen.

1.5 Speicherbegrenzung

Bud P. Bruegger (ULD)

Im Folgenden wird der Grundsatz der *Speicherbegrenzung gemäß* Artikel. 5 Absatz 1 Buchstabe e DSGVO definiert ist.

***Speicherbegrenzung* auf einen Blick:**

Bei der Speicherbegrenzung (auch wenn der Name dies nicht impliziert) geht es um den Grad der **Identifizierung** der betroffenen Person durch die Daten, d. h. darum, wie einfach die betroffene Person mit den Daten in Verbindung gebracht werden kann. Die in der Datenschutz-Grundverordnung vorgesehenen Identifizierungsgrade sind ***direkt identifizierende Daten,*** die *Kennungen* enthalten, ***pseudonyme Daten*** und ***anonyme Daten***. Daten sind mit dem geringstmöglichen Identifizierungsgrad zu erheben, und Pseudonymisierung und Anonymisierung sind zu verwenden, um die Identifizierung im Laufe der Zeit so schnell wie möglich weiter zu reduzieren.

1.5.1 Beschreibung

In „*Datenschutz verstehen: Die EU-Verordnung in Kurzform“* wurde die *Speicherbegrenzungg* damit begründet, den Machtgewinn des Verantwortlichen auf das zur Einhaltung der erklärten rechtmäßigen Zwecke erforderliche Mindestmaß zu beschränken. Insbesondere ging es um die Minimierung des Ausmaßes, in dem die personenbezogenen Daten mit der betroffenen Person in Verbindung gebracht werden. Dies ergänzt die Minimierung des Informationsgehalts und die Begrenzung des Zugriffs auf die Macht. Siehe *Minimierung der Befugnisse auf das zur Einhaltung der erklärten Zwecke erforderliche Maß.*

In der Datenschutz-Grundverordnung wird dieser Grundsatz wie folgt definiert:

Definition laut Art. 5 Absatz 1 Buchstabe e DSGVO:

Personenbezogene Daten müssen in einer Form gespeichert werden, die **die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke,** für die sie verarbeitet werden, **erforderlich ist**; [...]

(„*Speicherbegrenzung“*);

Das Hauptkonzept dieses Grundsatzes bezieht sich eindeutig auf die ***Identifizierung***, d. h. die Zuordnung der personenbezogenen Daten zu der betroffenen Person. Im weiteren Verlauf dieses Abschnitts wird daher hauptsächlich analysiert, was Identifizierung eigentlich bedeutet.

Beachten Sie, dass im obigen Definitionsfeld der ausgelassene Teil, der durch [...] dargestellt wird, unter dem Grundsatz der *Datenminimierung* diskutiert wurde (siehe 1.3.2 *Verwandte Artikel und Erwägungsgründe* in *Datenmnimierung*). Dabei geht es um die **zeitliche Begrenzung der Speicherung**, die wohl ein Aspekt des allgemeinen **Konzepts der Begrenzung von** Daten ist, das im Grundsatz der *Datenminimierung zum* Ausdruck kommt.

Unter diesem Gesichtspunkt ist die Bezeichnung *Speicherbegrenzung* irreführend, da sie nur den zeitlichen Aspekt der Datenminimierung impliziert, nicht aber die Identifizierung im Ganzen. Die Bezeichnung „*Minimierung des Identifikationspotenzials"* ist vielleicht klarer.

1.5.1.1 Identifizierung der betroffenen Personen

Um besser zu verstehen, was mit Identifizierung gemeint ist, verweisen wir auf Art. 4 Absatz 1 DSGVO. Der zweite Halbsatz[96] lautet wie folgt:

> [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;

Zum besseren Verständnis wird dieser Satz in die beiden folgenden Teile aufgeteilt:

Direkte Identifizierung mittels Zuordnung zu einer Kennung:

> [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;

Indirekte Identifizierung mittels Zuordnung zu einem oder mehreren Merkmalen, die für die Identität einer natürlichen Person spezifisch sind:

> [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;

Die **Beispiele für Kennungen** sind[97]:

- ein Name,
- eine Kennnummer,
- Standortdaten,
- eine Online-Kennung.

96 Ein Teil eines Satzes, der durch ein Semikolon vom Rest getrennt ist, wird hier als „Halbsatz" bezeichnet.

97 In Erwägungsgrund 30 der Datenschutz-Grundverordnung werden zusätzlich Beispiele für „Online-Kennungen" genannt: IP-Adressen, Cookie-Kennungen oder andere Kennungen wie Funkfrequenzkennzeichnungen.

Besonders zu beachten sind *Standortdaten*, die gemeinhin nicht als Kennungen angesehen werden, die eine direkte Identifizierung ermöglichen, auch wenn ihr hochgradig identifizierender Charakter tatsächlich intuitiv ist.

Die Beispiele für **Merkmale, die sich auf die Identität einer natürlichen Person beziehen,** betreffen die folgenden Aspekte:

- physisch,
- physiologisch,
- genetisch,
- psychisch,
- wirtschaftlich,
- kulturell,
- sozial.

Diese Unterscheidung zwischen direkter und indirekter Identifizierung ermöglicht es nun, den Begriff der *Form, die die Identifizierung der betroffenen Personen ermöglicht,* zu diversifizieren.

1.5.1.2 Arten von Daten, die in der DSGVO unterschieden werden

Die Datenschutz-Grundverordnung unterscheidet zwischen drei Arten von Daten, die in unterschiedlichem Maße mit den betroffenen Personen in Verbindung gebracht werden können:

(i) **direkt identifizierende personenbezogene Daten**[98],

(ii) **pseudonymisierte personenbezogene Daten**, und

(iii) **anonyme Daten**.

(i) Direkt identifizierende personenbezogene Daten: Erstere müssen natürlich **Kennungen** enthalten, da sie eine direkte Identifizierung der betroffenen Personen ermöglichen. Die meisten personenbezogenen Datensätze enthalten jedoch nicht nur Kennungen. Die anderen Daten müssen dann alle als **Merkmale** betrachtet werden**, die für die Identität einer natürlichen Person spezifisch sind**, da sie alle verschiedene Aspekte beschreiben, die mit der Identität der betroffenen Person verbunden sind.

(ii) Pseudonymisierte personenbezogene Daten: Art. 4 Absatz 5 DSGVO definiert das damit verbundene Konzept der „Pseudonymisierung". Sein Wortlaut kann wie folgt angepasst werden, um pseudonyme personenbezogene Daten zu definieren:

> Pseudonymisierte personenbezogene Daten sind personenbezogene Daten, die **ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können**.

Dies ist wie folgt zu interpretieren:

- Pseudonymisierte personenbezogene Daten **ermöglichen keine direkte Identifizierung**.

98 Der Begriff „*direkt identifizierende personenbezogene Daten"* wird in der Datenschutz-Grundverordnung nicht verwendet, sondern vom Verfasser geklont.

- Sie **düfren** daher **keine Kennungen enthalten**.
- **Zusätzliche Daten** sind in diesem Zusammenhang Daten, die es ermöglichen, **Merkmale, die für die Identität einer natürlichen Person spezifisch sind, mit Kennungen zu verknüpfen.**

(iii) Anonyme Daten: Anonyme Informationen sind in Erwägungsgrund 26 der DSGVO (fünfter Satz) definiert. Da *Informationen* und *Daten* synonym verwendet werden, kann der Wortlaut wie folgt angepasst werden:

Anonyme Daten sind entweder

- Daten, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen oder
- Anonymisierung der personenbezogenen Daten in der Weise, dass die betroffene Person nicht oder nicht mehr identifizierbar ist.

Beachten Sie, dass „identifizierbar“ hier sowohl die direkte als auch die indirekte Identifizierung umfasst. Selbst mit zusätzlichen Informationen ist es nicht möglich, anonyme Daten einer bestimmten betroffenen Person zuzuordnen.

Beachten Sie, dass die DSGVO gemäß Erwägungsgrund 26 (Satz 6) nicht für anonyme Daten gilt. Dies ist auch klar, da sie nicht mit der Definition von personenbezogenen Daten übereinstimmen (siehe Art. 4 Absatz 1 und Erwägungsgrund 26 DSGVO).

Nachdem diese Arten von Daten unterschieden wurden, kann die Formulierung „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“ nun genauer verstanden werden, wobei auch der zeitliche Aspekt des Grundsatzes berücksichtigt wird.

1.5.1.3 Zeitlicher Aspekt

Art. 5 Absatz 1 Buchstabe e spricht eindeutig den zeitlichen Aspekt an, indem er vorschreibt, dass eine Speicherform, die eine Identifizierung ermöglicht, **nicht länger** zulässig ist, als es für die Zwecke erforderlich ist. Dieser zeitliche Aspekt wird hier in differenzierter Weise erörtert. Die folgenden zwei Kriterien definieren diese Diversifizierung:

- **Die Identifizierung** kann entweder **direkt** oder **indirekt erfolgen**.
- **Die Identifizierung** kann **für jedermann** oder für **einen begrenzten Personenkreis zugänglich** sein**.**

Auf der Grundlage dieser Unterscheidungen lassen sich vier verschiedene Fälle unterscheiden. Diese sind in Abbildung 4 als „Phasen“ dargestellt. Es ist möglich, von einer Phase zu einer beliebigen späteren Phase überzugehen. Dies kann entweder sequenziell oder durch Auslassen von Zwischenphasen geschehen. In jeder Phase wird der Grad der Identifizierung der Daten mit der betroffenen Person verringert. Der Grundsatz der *Speicherbegrenzung* besagt, dass zu jedem Zeitpunkt nur **der minimale Grad der Identifizierung verwendet werden darf, der zur Einhaltung der Zwecke erforderlich ist**.

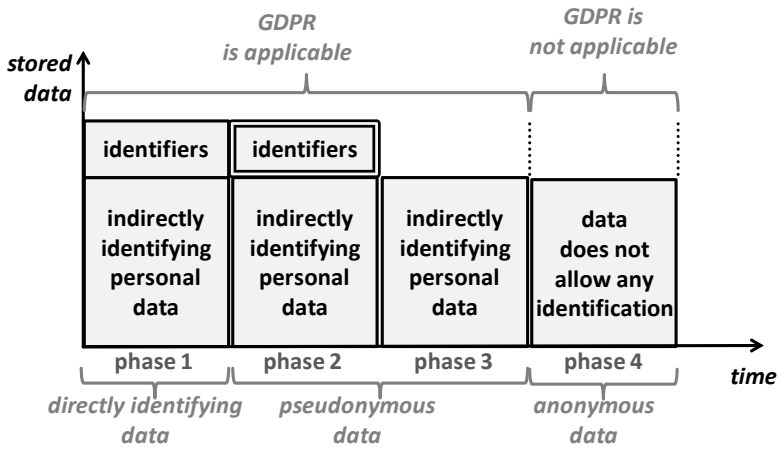

Abbildung 4: Daten mit unterschiedlichen Assoziationsgraden zur betroffenen Person.

Es ist zu beachten, dass der Grundsatz der *Speicherbegrenzung* in seiner reinen Form dargestellt wird: Lediglich der Grad der Verknüpfung mit der betroffenen Person wird zwischen aufeinanderfolgenden Phasen reduziert. In der Praxis wird die Speicherbegrenzung in der Regel mit der *Datenminimierung* kombiniert. In einem kombinierten Szenario würde auch die Höhe der in der Abbildung gezeigten Kästchen reduziert werden.

Die Phasen der Abbildung werden im Folgenden näher beschrieben:

Phase 1 zeigt die Daten, die sowohl **Kennungen** als auch **spezifische Merkmale für die Identität einer natürlichen Person** enthalten. Letztere werden der Einfachheit halber als *indirekt identifizierende personenbezogene Daten* bezeichnet. Die Kennungen dienen der direkten Identifizierung. Sie sind für **jeden zugänglich, dem die Daten offengelegt werden**.

Phase 2 zeigt eine Art der Verarbeitung, die „**Pseudonymisierung**“[99] genannt wird. Hier werden die **Kennungen** zwar weiterhin gespeichert, aber **getrennt aufbewahrt** und so **geschützt**, dass der **Zugriff nur** unter **genau festgelegten Bedingungen,** mit **vordefinierten Verfahren** und zu **genau festgelegten Zwecken** möglich ist, wobei der Zugriff auf eine **im Voraus festgelegte Gruppe befugter Personen**[100] beschränkt ist. Diese Beschränkungen werden durch einen doppelten Rahmen um die Kennungen dargestellt. Der **Zugang zur direkten Identifizierung** wird somit **streng kontrolliert** und ist nur wenigen bestimmten Personen zugänglich.

Eine indirekte Identifizierung unter Verwendung zusätzlicher Informationen ist auf der Grundlage der indirekt identifizierenden personenbezogenen Daten weiterhin möglich. Sie erfordert jedoch zusätzliche Informationen. Der Verantwortliche ergreift Maßnahmen, um zu verhindern, dass die Personen, die während der Verarbeitung auf diese Daten zugreifen, Zugang zu diesen zusätzlichen Informationen erhalten. Dies bedeutet, dass **für den größten Teil der Verarbeitungen** (und eine wichtige Untergruppe von Zwecken) und die Mehrzahl der Beschäftigten eine **Identifizierung nicht mehr möglich ist**.

Phase 3 zeigt die Situation, in der die **Zwecke nicht mehr die Möglichkeit der direkten Identifizierung** der betroffenen Personen **erfordern**, auch nicht in Ausnahmefällen. In diesem Fall können die *Kennungen*, die eine direkte Identifizierung ermöglichen, vollständig gelöscht werden. Folglich ist **der Verantwortliche selbst** (einschließlich aller Mitarbeiter) bei Vorhandensein angemessener Garantien **nicht mehr in der Lage, die betroffenen Personen zu identifizieren**. Dadurch wird der Grad der Identifizierung im Vergleich zu Phase 2 weiter verringert.

99 Siehe Artikel 4 Absatz 5 der Datenschutz-Grundverordnung.
100 Siehe Erwägungsgrund 29 DSGVO, Satz 2.

Phase 4 zeigt, dass nur **anonyme Daten** verwendet werden. Die Abbildung impliziert, dass diese das Ergebnis einer Anonymisierung der Daten aus Phase 3 (oder früheren Phasen) sind. Anonyme Daten können per Definition[101] nicht einer betroffenen Person zugeordnet werden, auch nicht mithilfe von Zusatzinformationen. Bei diesen Daten handelt es sich daher nicht mehr um personenbezogene Daten, die somit nicht unter die DSGVO fallen (und eine erfolgreiche Anonymisierung hat daher die gleiche Wirkung wie eine Löschung). **Anonyme Daten schließen also die Möglichkeit der Identifizierung vollständig aus**.

Einige Leser kennen vielleicht das Konzept der „***Unverknüpfbarkeit***“[102], das eng mit dem der Speicherbegrenzung verbunden ist. Dies wird deutlich, wenn man bedenkt, dass die direkte Identifizierung als eine Kennung angesehen werden kann, die eine Verbindung zur betroffenen Person herstellt, und dass die Verwendung zusätzlicher Informationen für die indirekte Identifizierung die Verknüpfung von Datensätzen erfordert, die zu derselben Person in den beiden Datensätzen gehören.

1.5.2 Verwandte Artikel und Erwägungsgründe

Wie gezeigt wurde, sind mehrere Begriffe, die außerhalb von Artikel 5 DSGVO definiert sind, für das Verständnis des Grundsatzes der Speicherbegrenzung von Bedeutung. Dies sind insbesondere die folgenden:

- *Direkte* und *indirekte Identifizierung* im Sinne von Art. 4 Absatz 1 DSGVO,
- *Pseudonymisierung*, die in Art. 4 Absatz 5 DSGVO, und
- *anonyme Daten*, die in Erwägungsgrund 26 der DSGVO definiert sind.

In Art. 11 Absatz 1 der DSGVO heißt es:

> Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren

Dies gibt Aufschluss über die Bedeutung des Grundsatzes der Speicherbegrenzung im Vergleich zu anderen Konzepten in der Datenschutz-Grundverordnung: Die Speicherbegrenzung hat einen klaren Vorrang vor anderen Pflichten der Datenschutz-Grundverordnung in dem Sinne, dass ein Verantwortlicher Kennungen nicht zu dem alleinigen Zweck erheben oder speichern darf, diesen Pflichten nachzukommen.

In Artikel 11 Absatz 2 DSGVO[103] wird dies dann ausdrücklich in Bezug auf die Pflichten aus den Rechten der betroffenen Person in den Artikeln 15 bis 20 festgelegt:

> Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

101 Siehe Erwägungsgrund 26 der Datenschutz-Grundverordnung.

102 Deutsche Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, 17. April 2020, Das Standard-Datenschutzmodell, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b_EN.pdf (zuletzt besucht am 28.05.2020).

103 Siehe auch Art. 12 Absatz 2 DSGVO, in dem dieser Fall weiter erörtert wird.

Darüber hinaus unterstreicht die Datenschutz-Grundverordnung die Bedeutung der Pseudonymisierung in verschiedenen Zusammenhängen:

Art. 89 Absatz 1 unterstreicht die **Bedeutung der *Pseudonymisierung*** für den Fall, dass die Daten nach Einhaltung der ursprünglichen Zwecke für „als vereinbar geltende Zwecke“[104] weiterverarbeitet werden. Insbesondere „im öffentlichen Interesse liegende Archivzwecke, **wissenschaftliche** oder **historische Forschungszwecke** oder **statistische Zwecke gelten** gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken“[105]. Art. 89 Abs. 1 DSGVO (Satz 2) schreibt ausdrücklich vor, dass für diese Weiterverarbeitung „technische und organisatorische Maßnahmen vorhanden sein müssen“ und nennt als einziges Beispiel für solche Maßnahmen die Pseudonymisierung (Satz 3). Weiter heißt es (Satz 4): „In allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt“. Dies scheint eine direkte Anwendung des Grundsatzes der Speicherbegrenzung zu sein.

Art. 6 Absatz 4 Buchstabe e unterstreicht ferner die Rolle der Pseudonymisierung, wenn ein Verantwortlicher feststellt, ob ein zusätzlicher Zweck mit den Zwecken, für die die Daten erhoben wurden, vereinbar ist.

Art. 25 Absatz 1 nennt die Pseudonymisierung als einziges Beispiel für eine Maßnahme, die im Rahmen des Datenschutzes durch Technikgestaltung umgesetzt werden kann.

Auch Art. 32 Absatz 1 Buchstabe a führt die Pseudonymisierung zusammen mit der Verschlüsselung als Maßnahme zur Unterstützung der Sicherheit auf. Dies unterstreicht zwar die Bedeutung der Pseudonymisierung und damit der Speicherbegrenzung, es ist jedoch fraglich, ob die Pseudonymisierung tatsächlich eines der gemeinsamen Schutzziele der IT-Sicherheit, nämlich *Vertraulichkeit*, *Integrität* und *Verfügbarkeit,* unterstützt.

1.5.3 Damit verbundene technische und organisatorische Maßnahmen

Im Folgenden werden einige Beispiele für konkrete Maßnahmen genannt, die das Prinzip der Speicherbegrenzung unterstützen:

- Eine organisatorische Maßnahme ist es, bei der Konzeption einer Verarbeitungstätigkeit **zu prüfen, ob** direkt **identifizierende Daten** zur Einhaltung der angegebenen Zwecke **überhaupt erhoben werden müssen**.
- **Pseudonymisierung** und **Anonymisierung** von Daten zwischen den Verarbeitungsschritten sind vorrangige technische Maßnahmen. Sie erfordern die Überprüfung, ob die verbleibenden Zwecke nach Abschluss des Verarbeitungsschritts noch den gleichen Grad der Identifizierung der betroffenen Personen erfordern.
- Bei der Planung der Ausgabe von Authentifizierungsdaten an die betroffenen Personen ist als organisatorische Maßnahme zu prüfen, ob es ausreicht, **pseudonyme Daten auszugeben**. Beispielsweise kann die Ausgabe eines zufälligen Einmal-Passworts während der Datenerhebung ausreichen, um später das Recht auf Widerruf der Einwilligung zu unterstützen.
- Wenn eine Website so gestaltet wird, dass **keine Cookies** außerhalb der Bereiche **gesetzt werden, die** eine Authentifizierung erfordern, **wird eine Möglichkeit zur Identifizierung der betroffenen Personen** über mehrere Sitzungen hinweg **vermieden** und kann als Maßnahme zur Unterstützung der Speicherbegrenzung betrachtet werden. (Siehe Setzen von Cookies und Verfassen einer Cookie-Richtlinie).

104 Siehe Art. 5 Absatz 1 Buchstabe b DSGVO.
105 Wortlaut entnommen aus Art. 5 Absatz 1 Buchstabe b DSGVO.

Konkret kann dies über eine geeignete Konfiguration der Webanwendung (wie ein Content-Management-System und seine Plugins) oder des Webservers erfolgen.

- Der Betrieb eines internetbasierten Dienstes, der **es den** Nutzern **ermöglicht**, sich über ein **anonymisierendes Overlay-Netz wie TOR** zu verbinden[106], vermeidet die Identifizierung der betroffenen Personen über ihre (Netz-)IP-Adresse und ist somit eine Maßnahme zur Unterstützung der Speicherbegrenzung.
- Ausstattung eines **WLAN-fähigen Nutzergeräts** mit einer **MAC-Adressen-Randomisierung**[107], um zu verhindern, dass die betroffene Person eindeutige Kennungen sendet.

1.6 Integrität und Vertraulichkeit

Bud P. Bruegger (ULD)

Danksagung: Der Autor dankt Frédéric Tronnier (GUF), der eine Analyse dieses Grundsatzes als Beitrag zu der hier vorgestellten Beschreibung verfasst hat.

Im Folgenden wird der Grundsatz der *Integrität und Vertraulichkeit* erörtert, der in Art. 5 Absatz 1 Buchstabe f DSGVO definiert ist.

***Integrität und Vertraulichkeit* auf einen Blick:**

Der Grundsatz bezieht sich auf die klassischen Schutzziele der **IT-Sicherheit**, nämlich ***Vertraulichkeit***, ***Integrität*** und ***Verfügbarkeit*** (CIA). ***Belastbarkeit*** kann als ein Aspekt der Verfügbarkeit betrachtet werden. Das Hauptaugenmerk liegt auf dem Schutz von *Werten* gegen *Risiken*, die durch *unerwünschte Ereignisse* verursacht werden. Im Gegensatz zur IT-Sicherheit handelt es sich bei diesen **Vermögenswerten und Risiken** nicht um die des Verantwortlichen (einer Organisation), sondern um die **der betroffenen Personen**. Unter diesem Gesichtspunkt wird auch klar, warum die *Datenübertragbarkeit* im Rahmen dieses Grundsatzes zur *Verfügbarkeit* gehört: Sie schützt die betroffenen Personen vor dem Verlust eines Vermögenswerts (repräsentiert durch die Daten), wenn sie den Verantwortlichen (meist den Anbieter) wechseln.

1.6.1 Beschreibung

In „*Datenschutz verstehen: Die EU-Verordnung in Kurzform“* wurde die *Integrität* (zusammen mit der Richtigkeit) mit der Tatsache begründet, dass die Richtigkeit der Daten notwendig ist, um für die erklärten Zwecke geeignet zu sein. Eine nicht zweckdienliche Verarbeitung kann keinen Machtzuwachs gegenüber einer betroffenen Person rechtfertigen. Siehe *Verbot einer nicht zweckdienlihen Verarbeitung,* für weitere Einzelheiten. Die *Vertraulichkeit hingegen* wurde durch die Begrenzung des Zugangs zur Macht begründet. Siehe *1.6.5.3 Begrenzung des Zugangs zur Macht im* Detail. Die *Verfügbarkeit*

106 Siehe zum Beispiel https://en.wikipedia.org/wiki/Tor_(anonymity_network) (letzter Zugriff am 18.05.2020).
107 Siehe zum Beispiel https://en.wikipedia.org/wiki/MAC_spoofing#MAC_Address_Randomization_in_WiFi (letzter Zugriff am 18.05.2020).

wurde durch den Schutz des Vermögens der betroffenen Person begründet. Siehe *1.6.6 Schutz des Vermögens der betroffenen Person für weitere Einzelheiten*.

In der Datenschutz-Grundverordnung wird dieser Grundsatz wie folgt definiert:

Definition laut Art. 5 Absatz 1 Buchstabe f DSGVO:

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die **eine angemessene Sicherheit** der personenbezogenen Daten **gewährleistet**, einschließlich Schutz vor **unbefugter** oder **unrechtmäßiger Verarbeitung** und vor **unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische oder organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

1.6.1.1 Struktur von Art. 5 Absatz 1 Buchstabe f und Sicherheitsrisiken

Wie aus dem Wortlaut von Art. 5 Absatz 1 Buchstabe f hervorgeht, spricht die DSGVO von **unerwünschten Ereignissen**, nämlich:

- unbefugte oder unrechtmäßige Verarbeitung und
- unbeabsichtigter Verlust, unbeabsichtiguge Zerstörung oder unbeabsichtigte Schädigung.

Es ist klar, dass diese Ereignisse nicht Teil der geplanten Verarbeitung sind; idealerweise sollten sie gänzlich verhindert werden. Da dies im Sicherheitsbereich nie mit 100-prozentiger Sicherheit möglich ist, besteht eine **Restwahrscheinlichkeit, dass solche Ereignisse eintreten**.

Es ist auch klar, dass das Eintreten solcher Ereignisse **unerwünschte Folgen** hat.

Leser, die mit der IT-Sicherheit vertraut sind, werden erkannt haben, dass in dieser Diskussion die Elemente der *Risikodefinition* eingeführt wurden. Dies wird im Folgenden deutlich gemacht:

Sicherheitsrisiko = Wahrscheinlichkeit eines unerwünschten Ereignisses * Schwere der unerwünschten Folgen

Dies ist ein „individuelles“ Risiko, und das Gesamtrisiko ist dann die Summe aller anwendbaren individuellen Risiken.

Aufmerksame Leser werden bemerkt haben, dass die hier verwendete Terminologie etwas von der in der IT-Sicherheit[108] üblichen abweicht. Insbesondere wurde der Begriff „Sicherheitsrisiko“ und nicht nur „Risiko“ verwendet, und in ähnlicher Weise wurde „Schwere der unerwünschten Folgen“ anstelle von „Schädigung“ verwendet. Die Motivation für diese Begriffswahl wird im Folgenden erläutert:

1.6.1.2 Hauptunterschied zu anderen Risiken in der DSGVO und zu Risiken in der IT-Sicherheit

Die Datenschutz-Grundverordnung bezieht sich auf mindestens zwei grundlegend verschiedene Arten von Risiken (ohne diese Unterscheidung jedoch explizit zu machen). Im Folgenden werden daher zwei verschiedene Begriffe eingeführt, um diese Unterscheidung

108 Siehe zum Beispiel https://en.wikipedia.org/wiki/IT_risk#Measuring_IT_risk (zuletzt besucht am 19.05.2020).

deutlich zu machen. Es handelt sich dabei um das *Sicherheitsrisiko* und das *Datenschutzrisiko*.

In der Datenschutz-Grundverordnung ist das ***Sicherheitsrisiko*** sowohl in Artikel 5 Absatz 1 Buchstabe f als auch in Artikel 32 implizit enthalten. Wie aus dem vorangegangenen Unterabschnitt hervorgeht, ergibt sich seine Definition aus dem Vorhandensein **unerwünschter Ereignisse**, die **nicht Teil der geplanten Verarbeitungsvorgänge** sind.

Im Gegensatz dazu berücksichtigt die Datenschutz-Grundverordnung eindeutig auch Risiken, die sich aus der Datenverarbeitung selbst ergeben – wenn keine unerwünschten Ereignisse eintreten – d. h. bei einer ungestörten Verarbeitung wie geplant. Wir bezeichnen diese Art von Risiko als *Datenschutzrisiko.* Es ist vorhanden, selbst wenn die Sicherheit perfekt wäre und alle möglichen unerwünschten Ereignisse mit 100%iger Sicherheit verhindert werden könnten.

Daher ist es wichtig zu verstehen, dass *Sicherheitsrisiken* nur eine Teilmenge der Risiken sind, die die Verantwortlichen durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen eindämmen müssen.

Nachdem wir die Sicherheitsrisiken von den Datenschutzrisiken unterschieden haben, wollen wir die Sicherheitsrisiken der DSGVO mit denen der IT-Sicherheit vergleichen. Die im Kasten im vorherigen Unterabschnitt bereitgestellte Definition weist dieselbe Struktur auf. Kann man daher daraus schließen, dass die *Sicherheitsrisiken* in der DSGVO dieselben sind wie die Risiken in der IT-Sicherheit?

Dies spricht für die Wahl des zweiten Begriffs, nämlich *Schwere der unerwünschten Folgen* anstelle von *Schaden* oder *Schädigung*.

In der **IT-Sicherheit** ist der ***Schaden*** eine Quantifizierung der unerwünschten Folgen im Vergleich zum **Auftrag und den Werten der Organisation**, die die Verarbeitungstätigkeit durchführt. Die Quantifizierung erfolgt häufig in Form eines **Geldwerts**, wie es **sich für** eine Organisation gehört, deren Aufgabe es ist, **Gewinne** zu erzielen.

In krassem Gegensatz dazu steht die **Schwere der unerwünschten Folgen,** die mit dem Grundsatz der Integrität und Vertraulichkeit **in der DSGVO verbunden sind.** Diese Maßnahme **bezieht sich auf** die **Rechte und Freiheiten natürlicher Personen**, wie sie in der Europäischen Charta der Grundrechte niedergelegt sind. Die unerwünschte Wirkung kann also darin bestehen, dass die freie Ausübung der Rechte und Freiheiten behindert oder vereitelt wird[109]. Solche Auswirkungen können in der Regel nicht in Geldwerten gemessen werden. Sie sind in der Regel auch nicht quantifizierbar und können nur auf einer Ordinalskala (z. B. *niedrig*, *mittel* und *hoch*) ausgedrückt werden.

Der **Unterschied** zwischen **IT-Sicherheit** und **Sicherheit nach Art. 5 Absatz 1 Buchstabe f** DSGVO ist die **Bewertung der unerwünschten Folgen**, auch wenn die unerwünschten Ereignisse dieselben sein können. In vielen Fällen kann ein Ereignis, das nur geringfügige Folgen für die Aufgabe der Organisation des Verantwortlichen hat, einen schwerwiegenden Eingriff in die Rechte und Freiheiten einer betroffenen Person darstellen (und umgekehrt).

1.6.1.3 Die in Art. 5 Absatz 1 Buchstabe f integrierten Schutzziele

In der DSGVO wird dieser Grundsatz in Art. 5 Absatz 1 Buchstabe f ausschließlich als ***Integrität*** *und* ***Vertraulichkeit*** bezeichnet. Dies sind zwei der drei bekannten Schutzziele der IT-Sicherheit. Das dritte ist die ***Verfügbarkeit***. Diese Dreifaltigkeit der Schutzziele wird oft einfach mit dem Akronym *CIA* bezeichnet.

---

109 Felix Bieker, Benjamin Bremert, Identifizierung von Risiken für die Grundrechte von Individuen, in : ZD, 2020, S. 7 ff. (in Deutsch, Zusammenfassung in Englisch).

Die Bezeichnung des Grundsatzes in der Datenschutz-Grundverordnung scheint zwar zu suggerieren, dass die Verfügbarkeit ausgeschlossen ist, aber sowohl der genaue Wortlaut von Art. 5 Absatz 1 Buchstabe f als auch Art. 32 „*Sicherheit der Verarbeitung“* legen etwas anderes nahe. Im Einzelnen:

- Die Formulierung „Schutz vor unbeabsichtigtem Verlust“ kann eindeutig mit der *Verfügbarkeit in* Verbindung gebracht werden und
- Art. 32 Absatz 1 Buchstabe b verpflichtet die Verantwortlichen, die ständige „*Vertraulichkeit*, *Integrität*, *Verfügbarkeit* und ***Belastbarkeit*** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen“.

Belastbarkeit wird hier als viertes Schutzziel genannt. Sie wird auch eindeutig als Ziel der IT-Sicherheit akzeptiert und oft als ein Aspekt der *Verfügbarkeit* behandelt.

Zusammenfassend lässt sich sagen, dass Art. 5 Absatz 1 Buchstabe f DSGVO auf das gesamte Spektrum der Schutzziele verweist, die aus der IT-Sicherheit bekannt sind. Sie werden hier alle erörtert, ohne sich auf die beiden zu beschränken, die im Namen des Grundsatzes enthalten sind.

Eine ausführliche Erörterung finden Sie in den Veröffentlichungen der ENISA zu diesem Thema[110, 111]. Im Folgenden wird nur eine kurze Beschreibung der einzelnen Schutzziele gegeben.

1.6.1.4 Integrität

Die *Integrität* bezieht sich auf den Aspekt von Art. 5 Absatz 1 Buchstabe f, der den Schutz personenbezogener Daten „vor unbeabsichtigter Schädigun“", z. B. aufgrund eines Übertragungsfehlers, vorschreibt. Er zielt also darauf ab, jede Art von Ereignis zu verhindern, das die Daten in einer Weise „beschädigen“ könnte, die sie für die Zwecke der Verarbeitung ungeeignet macht.

1.6.1.5 Vertraulichkeit

Die *Vertraulichkeit* bezieht sich auf den Aspekt von Artikel. 5 Absatz 1 Buchstabe f, der den Schutz personenbezogener Daten „vor unbefugter oder unrechtmäßiger Verarbeitung“ fordert. Es ist wichtig anzumerken, dass in der Datenschutz-Grundverordnung die *Verarbeitung* auch die *Offenlegung* von Daten umfasst (siehe Artikel 4 Absatz 2 der Datenschutz-Grundverordnung). Die Vertraulichkeit erfordert also, dass personenbezogene Daten im Ruhezustand, bei der Übermittlung und bei der Verwendung vor unerwünschter Offenlegung geschützt werden[112]. Darüber hinaus muss sichergestellt werden, dass keine unbefugte Person in die Verarbeitung eingreifen kann, indem sie beispielsweise Entscheidungen, die eine Person betreffen, eingibt, personenbezogene Daten ändert oder löscht oder andere Vorgänge auslöst, die befugtem Personal vorbehalten sind, das nach genauen Anweisungen des Verantwortlichen arbeitet.

---

110 ENISA, Guidelines for SMEs on the security of personal data processing, 27. Januar 2017, https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing (zuletzt besucht am 19.05.2020).

111 ENISA, Handbook on Security of Personal Data Processing, 29. Januar 2018, https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing (zuletzt besucht am 19.05.2020).

112 Art. 32 Absatz 2 DSGVO verwendet den Ausdruck „übermittelt, gespeichert oder auf andere Weise verarbeitet".

1.6.1.6 Verfügbarkeit, Belastbarkeit und Übertragbarkeit

Die Verfügbarkeit bezieht sich auf den Aspekt von Art. 5 Absatz 1 Buchstabe f, der den Schutz personenbezogener Daten „vor unbeabsichtigtem Verlust oder unbeabsichtigter Zerstörung“, z. B. durch den Ausfall einer Speicherkomponente, fordert.

Die Belastbarkeit wird in Art. 32 Absatz 1 Buchstabe c definiert als „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“. Es handelt sich also eindeutig um einen Aspekt der Verfügbarkeit und steht im Zusammenhang mit der bekannten Maßnahme der Wiederherstellung im Katastrophenfall.

Ein weiterer Aspekt der *Verfügbarkeit* ist wohl die *Übertragbarkeit* von Daten, wie sie in Artikel 20 DSGVO definiert ist. Während unter Verfügbarkeit in der Regel verstanden wird, dass betroffene Personen davor geschützt werden, ihre Daten zu verlieren, während sie von einem bestimmten Verantwortlichen verarbeitet werden, schützt die *Datenübertragbarkeit* betroffene Personen vor dem Verlust, wenn sie von einem Verantwortlichen (z. B. in der Rolle eines Dienstleisters) zu einem anderen wechseln. Die Übertragbarkeit setzt voraus, dass die betroffenen Personen ihre Daten in einem maschinenlesbaren Format erhalten können (siehe Art. 20 Absatz 1 DSGVO) und gegebenenfalls deren direkte Übermittlung von einem Verantwortlichen an einen anderen (siehe Art. 20 Absatz 2 DSGVO).

1.6.2 Verwandte Artikel und Erwägungsgründe

Während Art. 5 Absatz 1 Buchstabe f DSGVO abstrakt besagt, dass „geeignete technische oder organisatorische Maßnahmen“ zu ergreifen sind, um die oben genannten Sicherheitsziele zu erreichen, enthält **Art. 32 DSGVO weitere Details.**

In Artikel 32 Absatz 1 heißt es, dass die Verantwortlichen bei der Entscheidung über geeignete Maßnahmen „den Stand der **Technik** und die **Impmenentierungskosten“** sowie „die Art, den Umfang, die **Umstände** und die Zwecke **der Verarbeitung“** berücksichtigen mussen. Insbesondere der Kontext der Verarbeitung ist hier von Bedeutung, da man argumentieren kann, dass die aktuelle **Bedrohungslage** ein Aspekt davon ist. Wie erwartet, muss der Verantwortliche auch „**die Risiken für die Rechte und Freiheiten natürlicher Personen**“ berücksichtigen.

Das erforderliche Schutzniveau hängt also eindeutig von der Schwere der möglichen unerwünschten Folgen ab, denen die betroffenen Personen ausgesetzt sind, sowie von einem Bedrohungsmodell, das die Wahrscheinlichkeit unerwünschter Ereignisse abschätzt. Sicherheit ist also nur ein Mittel, kein Ziel an sich. Das Sicherheitsniveau ist ausreichend, wenn die Risiken für die betroffenen Personen auf ein akzeptables Maß reduziert werden. Die Auswahl der Maßnahmen hängt sowohl davon ab, was der Markt zu bieten hat, als auch davon, wie kosteneffizient diese Maßnahmen sind.

Art. 32 Absatz 1 Buchstabe d der Datenschutz-Grundverordnung besagt, dass **Sicherheit ein Verfahren ist** und kein einmal erreichtes Ziel. Insbesondere verlangt die DSGVO „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“.

Art. 32 Absatz 2 DSGVO enthält **zusätzliche Details zu den Schutzzielen**, indem er „Vernichtung, Verlust, Veränderung oder unbefugte Offenletung beziehungsweise unbefugten Zugang – ob unbeabsichtigt oder unrechtmäßig – zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurde“ aufzählt.

Artikel 32 Absatz 3 DSGVO schlägt vor, dass „die Einhaltung **genehmigter Verhaltensregeln** oder eines **genehmigten Zertifizierungsverfahrens** als Faktor herangezogen werden kann, um **die Einhaltung**“ des Grundsatzes der *Integrität und Vertraulichkeit* **nachzuweisen**.

Art. 32 Absatz 4 DSGVO stellt klar, dass ein wichtiges Element der Sicherheit darin besteht, **sicherzustellen, dass unterstellte natürlich Personen nur auf Anweisung des Verantwortlichen handeln**. Dies ist notwendig, um eine klare Verantwortung und Rechenschaftspflicht festzulegen. Es ist auch notwendig, um die Anforderung von Art. 5 Absatz 1 Buchstabe f zum „Schutz vor unbefugter oder unrechtmäßiger Verarbeitung“ zu erfüllen.

Aus **Art. 25** DSGVO folgt, dass alle von der DSGVO gestellten Anforderungen, einschließlich der Sicherheit, **während des gesamten Lebenszyklus** der Verarbeitungstätigkeit berücksichtigt werden müssen. Die Datenschutz-Grundverordnung verlangt also auch **Sicherheit durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**. Die Sicherheit muss also auch zu Beginn des Lebenszyklus berücksichtigt werden, z. B. durch entsprechende Anforderungen bei einer Ausschreibung, und am Ende des Lebenszyklus, z. B. bei der Migration zu einem neuen Verarbeitungssystem und der Demontage des alten Systems.

Art. 30 Absatz 1 Buchstabe g DSGVO verlangt, dass die technischen und organisatorischen **Maßnahmen** in den an die Aufsichtsbehörden gerichteten ***Verzeichnissen von Verarbeitungstätigkeiten*** ausdrücklich aufgeführt werden.

1.6.3 Damit verbundene technische und organisatorische Maßnahmen

Die folgenden Beispiele für technische und organisatorische Maßnahmen sollen den Begriff der Sicherheit in der DSGVO weiter konkretisieren.

1.6.3.1 Maßnahmen zur Förderung der Integrität

- Eine der klassischen technischen Maßnahmen zur Unterstützung der Integrität ist die **transaktionale Verarbeitung**. Sie ist vor allem aus Datenbankverwaltungssystemen bekannt, kann aber auch in anderen Bereichen[113] eingesetzt werden. Transaktionen sind wichtig, wenn eine Operation, die das System von einem konsistenten Zustand in einen anderen bringt, aus mehreren Verarbeitungsschritten besteht (d. h. nicht „atomar“ ist). Eine Transaktion stellt dann sicher, dass entweder alle diese Schritte oder keiner davon ausgeführt werden, selbst wenn das System zwischendurch abstürzt. Sie garantiert also, dass das System immer in einem konsistenten Zustand bleibt.
- Unstimmigkeiten können aufgrund von Übertragungsfehlern in verrauschten Kommunikationsleitungen entstehen. Die technische Maßnahme der **Vorwärtsfehlerkorrektur**[114], die in moderne Kommunikationsprotokolle eingebaut ist, unterstützt daher die Integrität der Daten während der Übertragung.
- Eine gängige technische Maßnahme zur Erkennung unerwünschter Änderungen in Datensätzen sind **Prüfsummen** (auch Hash oder Digest genannt). Insbesondere wird eine Prüfsumme eines Datensatzes berechnet, wenn bekannt ist, dass er sich in einem konsistenten Zustand befindet. Zu späteren Zeitpunkten kann die Prüfsumme des

113 Beispiele für die transaktionale Verarbeitung außerhalb von DBMS finden Sie unter https://en.wikipedia.org/wiki/Tuxedo_(software) und https://docs.oracle.com/cd/E13222_01/wls/docs81/jta/trxejb.html (beide zuletzt besucht am 20.05.2020).

114 Siehe zum Beispiel https://en.wikipedia.org/wiki/Forward_error_correction (zuletzt besucht am 20.05.2020).

Datensatzes neu berechnet und mit der ursprünglichen verglichen werden, um Änderungen und Verfälschungen zu erkennen.

- Integrität ist ein wichtiges Thema bei der Verteilung von Software – insbesondere, wenn Software automatisch über ein Netz heruntergeladen wird. Automatische Aktualisierungen von Betriebssystemen sind ein gutes Beispiel dafür. Um die Integrität der Software zu unterstützen, werden häufig technische Maßnahmen wie die **Authentifizierung der Quellen** im Netz und die **digitale Signatur der Software** eingesetzt. Die digitale Signatur wird häufig auch für Datendateien verwendet.

1.6.3.2 Maßnahmen zur Förderung der Vertraulichkeit

- Eine organisatorische Maßnahme zur Unterstützung der Vertraulichkeit während der Konzeptionsphase ist eine **Analyse** der **Folgen, die** unerwünschte Offenlegungen gegenüber verschiedenen Parteien **für die betroffenen Personen** haben können. Dies ist vergleichbar mit der IT-Sicherheit, bei der die kritischen Vermögenswerte der Organisation, die besonders geschützt werden müssen, ermittelt werden.
- Die Vertraulichkeit schreibt vor, dass der Verantwortliche Maßnahmen zum Schutz vor unbefugter Verarbeitung ergreift (siehe Art. 5 Absatz 1 Buchstabe f DSGVO). Wie in Art. 29 und 32 Absatz 4 DSGVO hervorgehoben wird, gehört dazu, dass Mitarbeiter personenbezogene Daten nur auf Anweisung des Verantwortlichen verarbeiten. Es gibt eine Vielzahl von organisatorischen Maßnahmen, die diese Anforderung unterstützen, darunter die Folgenden:
    - **Überprüfung** neuer Mitarbeiter, um sicherzustellen, dass sie über die erforderlichen Fähigkeiten verfügen, um die Anweisungen der Verantwortlichen auszuführen;
    - Rechtlich bedeutet, dass „gewährleistet ist, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen“; (Die Formulierung wurde Art. 28 Absatz 3 Buchstabe b entnommen, der sich auf Personen bezieht, die für Auftragsverarbeiter arbeiten, aber ebenso auf Personen anwendbar ist, die für den Verantwortlichen arbeiten).
    - In diesem Sinne sind auch die **Verträge mit möglichen Auftragsverarbeitern** (siehe Art. 28 Absatz 3 DSGVO), die Vertraulichkeitsanforderungen enthalten, als Maßnahmen zu betrachten.
    - **Schulung** der Mitarbeiter in der Ausführung von Anweisungen;
    - **Interne Anlaufstellen** für Mitarbeiter, die klären wollen, wie Anweisungen auszuführen sind;
    - Handbücher, die die Anweisungen beschreiben (**Prozesshandbücher**);
    - **Beaufsichtigung** und **Qualitätskontrolle**.
- Was für die Anweisungen an das Personal gilt, gilt auch für die **Anweisungen an die technischen Mittel**, d. h. die Software. Die Umsetzung von Maßnahmen zum Schutz vor unbefugter Verarbeitung bedeutet, dass die Verantwortlichen sicherstellen müssen, dass die Software tatsächlich ihren Anweisungen entspricht. Zu diesem Zweck gibt es mehrere Maßnahmen, darunter die Folgenden:

- **Spezifizierung präziser Anforderungen** als Grundlage für Ausschreibungen oder die individuelle Entwicklung von Software;
- Formale **Abnahmeprüfung** durch den Verantwortlichen;
- **Analyse neuer** Softwareversionen, um sicherzustellen, dass die geänderte Funktionalität immer noch den Anweisungen des Verantwortlichen entspricht und dass sich keine zusätzliche Funktionalität eingeschlichen hat (**function creep**), die einer nicht vom Verantwortlichen genehmigten Vearbeitung entspricht.

- Eine wichtige technische Maßnahme ist die **Zugangskontrolle**, die sicherstellt, dass nur befugtes Personal zu den Systemen und Daten für die genehmigten Zwecke Zugang hat. Die Zugangskontrolle kann eine Vielzahl von Maßnahmen umfassen, darunter die Folgenden:
  - Ausstellung von **Authentifizierungsnachweisen**.
  - Konfiguration der **Zugriffsrechte** und -bedingungen.
  - Verwaltung des **Lebenszyklus von Berechtigungsnachweisen** und **Zugriffsrechten**, einschließlich Ablauf und Erneuerung, Widerruf (z. B. beim Ausscheiden von Mitarbeitern), Gewährung und Entzug vorübergehender Zugriffsrechte (z. B. bei Krankheit von Mitarbeitern).
  - Regelmäßige **Audits** der allgemeinen Wirksamkeit des Zugangskontrollsystems.
- Es gibt eine Fülle von technischen Maßnahmen, die verhindern sollen, dass (interne oder externe) Unbefugte auf Daten zugreifen können. In der Regel werden sie als **Schutz der Daten im Ruhezustand, bei der Übertragung und bei der Nutzung bezeichnet.** Für die ersten beiden Aspekte ist in der Regel eine **Verschlüsselung** erforderlich.
- Es gibt eine Fülle von Maßnahmen, um zu verhindern, dass Unbefugte Zugang zu Systemen und Netzen erhalten. Beispiele hierfür sind die folgenden:
  - **Härtung** von Betriebssystemen;
  - Rechtzeitige Anwendung von **sicherheitskritischen Patches und Updates;**
  - **Firewalls**;
  - Installation von Anti-Malware-Software;
  - Betrieb von **Systemen zur Erkennung von Eindringlingen**;
- Bei der **Entwicklung von Software** stehen zahlreiche Maßnahmen zur Verfügung, um den unbefugten Zugriff auf Software und Systeme zu verhindern. Dazu gehören die Bereinigung von Eingaben, Maßnahmen zur Verhinderung bekannter Angriffsarten wie Cross-Site-Scripting, Methoden zur Vermeidung von Pufferüberläufen, Speicherrandomisierung usw.
- Einige Maßnahmen sind nicht in der Lage, unbefugte Verarbeitungen direkt zu verhindern, sondern dienen der **Abschreckung**, indem sie dazu beitragen, solche Handlungen **aufzudecken**, die **Verantwortlichkeiten** eindeutig **zu bestimmen** und die **Personen**, die unbefugt gehandelt haben, **zur Rechenschaft zu ziehen**. Solche Maßnahmen umfassen in der Regel die **Protokollierung** oder die Erstellung von **Prüfpfaden**.

- Eine wichtige Maßnahme im Zusammenhang mit dem **Ende der Lebensdauer** von Speicherkomponenten ist die vollständige und **sichere Vernichtung** aller Daten vor der **Entsorgung**.

1.6.3.3 Maßnahmen zur Förderung von Verfügbarkeit und Belastbarkeit

- Eine organisatorische Maßnahme zur Konzeptionsphase ist die Analyse der Auswirkungen eines unbeabsichtigten Verlusts auf die betroffenen Personen. Dadurch sollen die Werte ermittelt werden, die durch Verfügbarkeitsmaßnahmen geschützt werden müssen.
- Eine weitere Maßnahme zur Konzeptionsphase betrifft die Datenübertragbarkeit und untersucht die Verfügbarkeit geeigneter standardisierter maschinenlesbarer Formate und Möglichkeiten zur automatischen Übertragung der Daten an einen anderen Verantwortlichen (siehe Art. 20 Absatz 2 DSGVO).
- Eine sehr verbreitete Art von Maßnahmen zur Förderung der Verfügbarkeit ist die **Redundanz der Speicherung**. Bekannte Beispiele sind die folgenden:
    - RAID-Speicher;
    - Backups;
    - Fernspeicherung zur Unterstützung der Notfallwiederherstellung.
- Neben der Datenspeicherung kann **Redundanz** auch **in Verarbeitungssystemen** wichtig sein. Zu den entsprechenden Maßnahmen gehören die Folgenden:
    - Master/Slave-Konfigurationen mit Ausfallsicherung;
    - Serverfarmen und Cloud-Konfigurationen;
    - Virtualisierungsbasierte Prozessmigrationsstrategien.

1.7 Rechenschaftspflicht

Bud P. Bruegger (ULD)

Danksagung: Der Autor dankt Johann Čas und Walter Peissl (beide OEAW), die eine Analyse dieses Grundsatzes als Beitrag zu der hier vorgelegten Beschreibung verfasst haben, für ihren Beitrag.

Im Folgenden wird der Grundsatz der *Rechenschaftspflicht* erörtert, wie er in Art. 5 Absatz 2 DSGVO definiert ist.

***Rechenschaftspflicht* auf einen Blick:**

Die Rechenschaftspflicht besteht aus zwei Anforderungen an die Verantwortlichen:

- **Einhaltung der** Grundsätze der Datenschutz-Grundverordnung;
- **Nachweis der Einhaltung.**

Die Einhaltung wird durch ***technische und organisatorische Maßnahmen*** erreicht, die im Vergleich zu den Risiken für die Rechte und Freiheiten der betroffenen Personen angemessen sind, dem Stand der Technik entsprechen und kostengünstig sind. In jeder

Beschreibung der Grundsätze wurden Beispiele für solche technischen und organisatorischen Maßnahmen genannt. Für eine systematische Anwendung dieser Maßnahmen können die Verantwortlichen ***Datenschutzrichtlinien*** erstellen. ***Genehmigte Verhaltensregeln***, sofern vorhanden, sind ähnlich, werden aber im Voraus genehmigt und betreffen in der Regel einen ganzen Sektor. Die Einhaltung der Grundsätze ist kein Zustand, der einmal erreicht wird, sondern **ein kontinuierliches Verfahren**, das sich über den gesamten Lebenszyklus einer Verarbeitungstätigkeit erstreckt.

Der Nachweis der Einhaltung der Vorschriften wird in erster Linie durch **Dokumentation** erbracht (siehe den Abschnitt *Dokumentation der Verarbeitung* in „Wichtigste Instrumente und Maßnahmen"). Die Dokumentation sollte ebenso kontinuierlich erfolgen wie der Prozess der Einhaltung. Jede durchgeführte Maßnahme, einschließlich datenschutzrelevanter Überlegungen und Entscheidungen, sollte dokumentiert werden. Die Datenschutz-Grundverordnung verlangt zwei formale Dokumente als Teil des Nachweises der Einhaltung der Vorschriften gegenüber den *Aufsichtsbehörden*: das ***Verzeichnis der Verarbeitungen*** (siehe *Dokumentation der Verarbeitungen* für Details) und, wenn die Risiken wahrscheinlich hoch sind, eine ***Datenschutz-Folgenabschätzung*** (siehe den gleichnamigen Abschnitt in „*Wichtigste Instrumente und Maßnahmen" in Teil II* für Details). Eine *Zertifizierung* kann den Nachweis der Einhaltung der Vorschriften unterstützen.

1.7.1 Beschreibung

In „*Datenschutz verstehen: Die EU-Verordnung in Kurzform" wurde die* uneingeschränkte *Rechenschaftspflicht* der Verantwortlichen als erste von mehreren Maßnahmen genannt, die die Datenschutz-Grundverordnung ergreift, um die von dem Verantwortlichen durch die Verarbeitung gewonnene Macht zu begrenzen und sie mit der Macht der betroffenen Personen in Einklang zu bringen. Siehe *1.6.1 Die Verantwortlichen sind in vollem Umfang rechenschaftspflichtig* für Details.

In der Datenschutz-Grundverordnung wird dieser Grundsatz wie folgt definiert:

Definition laut Art. 5 Absatz 2 DSGVO:

Der **Verantwortliche** ist **für die Einhaltung** des Absatzes 1 verantwortlich und **muss dessen Einhaltung nachweisen können** („Rechenschaftspflicht").

Absatz 1 bezieht sich auf die Grundsätze, die in den sechs vorangegangenen Abschnitten erörtert wurden, nämlich

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz;
- Zweckbindung;
- Datenminimierung;
- Richtigkeit;
- Speicherbegrenzung; und
- Integrität und Vertraulichkeit.

Anders ausgedrückt ist ein **Verantwortlicher** für laut Artikel 5 Absatz 2 für zwei Dinge voll **verantwortlich:**

- **Einhaltung** dieser sechs Grundsätze,
- **Nachweis der Einhaltung der Vorschriften**.

Die Rechenschaftspflicht ist also kein neuer Grundsatz, den die Verantwortlichen einhalten müssen, sondern sie gibt den Verantwortlichen vor**, wie die sechs Grundsätze anzuwenden sind**.

Beachten Sie, dass die Verpflichtung, die Einhaltung der Vorschriften nachzuweisen, einen großen Schritt über die bloße Verpflichtung zur Einhaltung hinaus darstellt. Insbesondere liegt die „Beweislast" bei dem Verantwortlichen; ein Verantwortlicher, der nicht in der Lage oder nicht willens ist, die Einhaltung nachzuweisen, verstößt gegen die Datenschutz-Grundverordnung.

1.7.1.1 Was bedeutet es, die Vorschriften einzuhalten?

Während Art. 5 Absatz 2 nur von der Einhaltung der sechs Grundsätze spricht, muss dies eigentlich auf die **gesamte Datenschutz-Grundverordnung** ausgedehnt werden. Dies ist dadurch begründet, dass alle anderen Artikel dazu dienen, die Grundsätze zu präzisieren oder genauer zu beschreiben, wie sie umgesetzt werden müssen.

In der Datenschutz-Grundverordnung ist durchgängig festgelegt, wie die Einhaltung der Vorschriften erreicht werden soll, nämlich durch die Umsetzung **technischer oder organisatorischer Maßnahmen**. In Art. 24, der die Pflichten des Verantwortlichen beschreibt, heißt es im ersten Absatz ausdrücklich, dass die Verantwortlichen auf diese Weise die DSGVO einhalten (und ihre Einhaltung nachweisen); Art. 25 Absatz 1 besagt, dass Datenschutz durch Technikgestaltung darauf hinausläuft, solche Maßnahmen während des gesamten Lebenszyklus der Verarbeitungstätigkeit zu ergreifen; in Art. 25 Absatz 2 wird ebenfalls die Verwendung solcher Maßnahmen durch datenschutzfreundliche Voreinstellungen betont; Art. 28 Absatz 1 besagt, dass auch die Auftragsverarbeiter solche Maßnahmen ergreifen müssen; Art. 32 besagt, dass auch die Einhaltung der Sicherheitsanforderungen durch die Durchführung solcher Maßnahmen erreicht wird; und Art. 89 Absatz 1 besagt, dass die für die „Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken" erforderlichen Garantien das Vorhandensein solcher Maßnahmen gewährleisten.

Da technische und organisatorische Maßnahmen für die Einhaltung der Vorschriften von so zentraler Bedeutung sind, wurde jeder der sechs oben genannten Grundsätze mit Beispielen für solche Maßnahmen abgeschlossen.

Die Einhaltung der Datenschutzanforderungen kann als Verfahren betrachtet werden. Nach dem Konzept des *„Datenschutzes durch Technikgestaltung"* (siehe Art. 25 Absatz 1 DSGVO) werden in jeder Lebenszyklusphase der Verarbeitungstätigkeit die Risiken für die Rechte und Freiheiten natürlicher Personen bewertet und geeignete Abhilfemaßnahmen ergriffen. Die DSGVO verwendet eine sehr weit gefasste Definition des Begriffs *„technische und organisatorische Maßnahmen"*. Er umfasst im Grunde alles, was ein Verantwortlicher tut, um die DSGVO einzuhalten. Daher kann sogar der oben erwähnte Bewertungsschritt als eine Maßnahme an sich betrachtet werden.

1.7.1.2 Was bedeutet es, die Einhaltung der Vorschriften nachzuweisen?

In Anbetracht der Tatsache, dass die Einhaltung der Vorschriften durch die Umsetzung geeigneter Maßnahmen erreicht wird, ist es nicht verwunderlich, dass der **Nachweis der Einhaltung diese Maßnahmen dokumentiert**.

Dies geht zum Beispiel aus Art. 30 Absatz 1 Buchstabe g hervor, der vorschreibt, die sicherheitsrelevanten Maßnahmen in den ***Verzeichnissen von Verarbeitungstätigkeiten*** aufzuführen. Es ist auch von zentraler Bedeutung in Art. 35 über die ***Datenschutz-Folgenabschätzung***, die wohl das wichtigste Instrument ist, das die Datenschutz-Grundverordnung für den Nachweis der Einhaltung der Vorschriften vorsieht. Insbesondere Art. 35 Absatz 7 Buchstabe d fordert die Verantwortlichen auf, die Maßnahmen zu erklären, die sie zum Schutz personenbezogener Daten ergriffen haben, und die Einhaltung der DSGVO nachzuweisen.

Eine **ausführlichere Erörterung** der ***Dokumentation der Verarbeitung*** im Allgemeinen und der *Datenschutz-Folgenabschätzungen* im Besonderen findet sich im Abschnitt „Wichtigste Instrumente und *Maßnahmen"* weiter unten. In diesen beiden Abschnitten wird auch die Bedeutung technischer und organisatorischer Maßnahmen hervorgehoben.

1.7.1.3 Größenvorteile bei der Einhaltung der Vorschriften und deren Nachweis

Wie oben dargelegt, wird die Einhaltung der Vorschriften durch die Umsetzung technischer und organisatorischer Maßnahmen erreicht. Aus den obigen Ausführungen ist ersichtlich, dass die Einhaltung der Vorschriften eine große Anzahl solcher Maßnahmen erfordern kann. Dies kann es erschweren, den tatsächlichen Schutz, den diese Maßnahmen bieten, und die einheitliche und konsequente Anwendung dieses Schutzes zu beurteilen.

Um diese Schwierigkeit abzumildern, bietet die Datenschutz-Grundverordnung einige Arten von „Abstraktionsmechanismen", die es ermöglichen, eine Reihe von zusammenhängenden Maßnahmen als eine einzige Einheit zu betrachten. Insbesondere sieht die DSGVO zwei solcher Mechanismen in Art. 24 vor, der die „Verantwortung des für die Verarbeitung Verantwortlichen" beschreibt:

- ***Datenschutzvorkehrungen*** (siehe Art. 24 Absatz 2 DSGVO), und
- ***genehmigte Verhaltensregeln*** (siehe Art. 24 Absatz 3 und 40).

Datenschutzvorkehrungen ist ein Mechanismus, um die Anwendung von Maßnahmen systematisch zu gestalten. Dadurch wird ein einheitlicher und konsistenter Satz von Maßnahmen in ähnlichen Situationen gewährleistet. Anstatt beispielsweise für jeden einzelnen von vielen sehr ähnlichen Servern beurteilen zu müssen, welche Sicherheitsmaßnahmen angemessen sind, kann eine einzige Richtlinie einmal geschrieben und auf alle Server angewendet werden. Insbesondere bei komplexen und umfangreichen Verarbeitungsvorgängen führt dies zu einer potenziell sehr bedeutenden Skaleneffizienz, die sogar mehrere unabhängige Verarbeitungsvorgänge desselben Verantwortlichen umfassen kann.

Der Mechanismus der ***genehmigten Verhaltensregeln*** dehnt diese Größenvorteile über einen einzelnen Verantwortlichen hinaus auf einen ganzen Verarbeitungssektor aus. Diese Verhaltensregeln werden von **Verbänden** und anderen Einrichtungen ausgearbeitet**, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten** (siehe Art. 40 Absatz 2 DSGVO). Beziehen sich Verhaltensregeln nicht auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, kann die zuständige *Aufsichtsbehörde* sie **genehmigen** (siehe Art. 40 Absatz 5 DSGVO) und anschließend registrieren und veröffentlichen (siehe Art. 40 Absatz 6 DSGVO). Bezieht sich ein Entwurf von Verhaltensregeln auf Verarbeitungstätigkeiten in

mehreren Mitgliedstaaten, wird ein ähnliches Verfahren angewandt, an dem der *Europäische Datenschutzausschuss* beteiligt ist (siehe Art. 40 Absatz 7 DSGVO). Verhaltensregeln bieten den Aufsichtsbehörden, die die Einhaltung der Datenschutz-Grundverordnung überwachen müssen, offensichtlich auch eine Größenvorteil.

Sowohl *genehmigte Verhaltensregeln* als auch *Zertifizierungen* (gemäß Artikel 42 DSGVO) können den Verantwortlichen beim Nachweis der Einhaltung der Vorschriften helfen (siehe Artikel 24 Absatz 3 DSGVO).

1.7.2 Verwandte Artikel und Erwägungsgründe

Bei der Rechenschaftspflicht geht es um die Einhaltung und den Nachweis der Einhaltung. Sie bezieht sich direkt auf die in Artikel. 5 Absatz 1 definierten sechs Datenschutzgrundsätze, erstreckt sich aber indirekt auf die gesamte DSGVO.

Art. 24 DSGVO regelt im Einzelnen, wie ein Verantwortlicher die Einhaltung der Vorschriften erreichen und nachweisen muss. Art. 25 Absatz 1 über den „Datenschutz durch Technikgestaltung“ verdeutlicht, dass die Einhaltung der Vorschriften (und folglich auch ihr Nachweis) als kontinuierliches Verfahren zu betrachten ist, das sich über alle Lebenszyklen einer Verarbeitungstätigkeit erstreckt. Die *Verhaltensregeln* und die *Zertifizierung*, die bei der Einhaltung der Vorschriften und ihrer Zertifizierung helfen können, werden in Art. 40 bzw. 42 DSGVO beschrieben.

Die Artikel, die für den Nachweis der Einhaltung der Vorschriften besonders wichtig sind, sind 30 *Verzeichnis von Verarbeitungstätigkeiten* und 35 *Datenschutz-Folgenabschätzungen*.

1.7.3 Damit verbundene technische und organisatorische Maßnahmen

Die für die *Rechenschaftspflicht* relevanten Maßnahmen betreffen eher die Art und Weise, wie die Einhaltung der Vorschriften erreicht und nachgewiesen werden kann, als das, was zur Einhaltung der Vorschriften getan werden muss.

Die folgenden „Meta“-Maßnahmen befassen sich mit der Frage, wie die **Einhaltung der Vorschriften erreicht werden kann**:

- ***Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*** (siehe Art. 25 DSGVO)
- Die ***Datenschutz-Folgenabschätzung*** (siehe Art. 35 DSGVO) in ihrer Funktion als kontinuierlicher Prozess, der den Verantwortlichen bei der Bewertung der Risiken und der Ermittlung geeigneter technischer und organisatorischer Maßnahmen zu deren Minderung anleitet
- Die Erstellung und Anwendung von ***Datenschutzvorkehrungen*** (siehe Art. 24 Absatz 2 DSGVO).
- Die Einhaltung der ***genehmigten Verhaltensregeln*** (siehe Art. 24 Absatz 3 DSGVO).
- Die Einhaltung der ***anerkannten Zertifizierungsmechanismen*** (siehe Art. 24 Absatz 3 DSGVO).

Die folgenden „Meta“-Maßnahmen befassen sich mit den Möglichkeiten, **die Einhaltung der Vorschriften zu dokumentieren**:

- Die ***Datenschutz-Folgenabschätzung*** (siehe Art. 35 DSGVO) in ihrer Funktion als Bericht. Wenn das Risiko wahrscheinlich nicht hoch ist und eine solche

Folgenabschätzung daher nicht erforderlich ist, sollte dokumentiert werden, wie diese Risikoeinschätzung ermittelt wurde (siehe Abschnitt „Datenschutz-Folgenabschätzung“ unter „Wichtigste Instrumente und Maßnahmen“ in Teil II dieser Leitlinien).

- Die ***Verzeichnisse von Verarbeitungstätigkeiten*** (siehe Art. 30 DSGVO).