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.

ALLGEMEINE EINFÜHRUNG IN DEN DATENSCHUTZ

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 Datenschutz verstehen: die EU-Verordnung in Kurzform

Bud P. Bruegger (ULD)

Danksagung: Der Autor dankt Jörg Pohle, Harald Zwingelberg, Martin Rost, Iñigo de Miguel Beriain und Josh Bruegger für ihre Ratschläge, Anregungen und Rückmeldungen zu Entwürfen.

1.1 Der Datenschutz in der Gesetzgebung

Im Folgenden wird versucht, eine knappe Einführung in die Grundsätze des Datenschutzes aus europäischer Sicht zu geben. Der Schutz personenbezogener Daten in Europa ist ein **Grundrecht**, wie in Artikel 8 der *Charta der Grundrechte der Europäischen Union* festgelegt[1]. Er wurde durch *die Datenschutz-Grundverordnung* (**DSGVO**)[2] operationalisiert.

1.2 Zweck dieser Einführung

Die Datenschutz-Grundverordnung umfasst etwa 99 Artikel, die wiederum in der Regel in mehrere Absätze unterteilt sind, die wiederum mehrere Punkte enthalten können. Darüber hinaus gibt es 173 Erwägungsgründe, die bei der Auslegung der Artikel helfen. Von den elf Kapiteln der Datenschutz-Grundverordnung sind die ersten vier für jeden, der personenbezogene Daten verarbeiten will, unmittelbar relevant. Ohne die Erwägungsgründe umfassen sie insgesamt 43 Artikel, die in der offiziellen PDF-Fassung 28 Seiten Rechtstext füllen[3]. Es ist daher nicht verwunderlich, dass viele Personen, die die DSGVO einhalten müssen, sich aber mit dem Lesen und Auslegen von Rechtstexten nicht auskennen, die Lernkurve als ziemlich steil empfinden.

Die vorliegende Einführung versucht, diese Schwierigkeit zu mildern. Sie gibt nicht nur einen Überblick über den wichtigsten Inhalt, sondern versucht auch, die Datenschutz-Grundverordnung als ein einheitliches System darzustellen. Sie beschränkt sich nicht darauf, *die Anforderungen* aufzuzählen, sondern schlägt einen Weg vor, um zu verstehen, *warum* jede Anforderung vorhanden und inwieweit sie ein notwendiger Bestandteil des gesamten Systems ist. Es ist zu hoffen, dass dieser Ansatz nicht nur dazu beiträgt, einen guten Überblick zu erhalten, sondern darüber hinaus ein tieferes Verständnis ermöglicht. Dies soll Praktikern helfen, wenn sie abstrakte Anforderungen in konkrete Maßnahmen umsetzen oder entscheiden müssen, auf welcher Ebene die Maßnahmen ausreichenden Schutz und Sicherheit bieten.

1 Die Charta der Grundrechte wurde am 7. Dezember 2000 ratifiziert.

2 Die Datenschutz-Grundverordnung trat am 25. Mai 2018 in Kraft.

3 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (zuletzt besucht am 7.5.2020)

1.3 Das Problem, das der Datenschutz angeht

Um die DSGVO als System darzustellen, wird davon ausgegangen, dass sich der Datenschutz mit einem einzigen Problem befasst. Offensichtlich ist diese Annahme weder Teil des Gesetzes, noch wurde die DSGVO systematisch geschaffen, um ein einzelnes, erklärtes Problem zu lösen. Das Grundproblem, das hier postuliert wird, findet möglicherweise nicht einmal einen allgemeinen Konsensus. Dennoch ist das postulierte Grundproblem geeignet, die DSGVO systematisch als einheitliches System zu erklären. Dies ist der einzige Zweck, den dieses Basisproblem in dieser Einführung hat. Es mag durchaus alternative Grundprobleme und Wege zur systematischen Erklärung der DSGVO geben.

Es besteht kein allgemeiner Konsensus darüber, welches Problem der Datenschutz eigentlich angeht[4]. Die These einer „einflussreichen Minderheit“[5] lautet, dass es beim Datenschutz um Macht[6] geht. In dieser Einleitung wird diese These aufgegriffen, um das Grundproblem darzustellen. Das Grundproblem des Datenschutzes besteht demnach darin, die Macht zu begrenzen, die Organisationen durch die Verarbeitung personenbezogener Daten[7] über Personen erlangen. Die bekannte Aussage „*Wissen ist Macht“* drückt genau diesen Gedanken aus. Der Besitz von Informationen über eine Person verschafft ihr nämlich Macht über diese Person.

In der Praxis kann die Verarbeitung solcher personenbezogenen Daten das Verhalten einer Person an sich beeinflussen (z. B. durch *abschreckende Wirkung*[8]), sie kann helfen, das Verhalten einer Person vorherzusagen, sie kann es leichter machen, eine Person zu einem bestimmten Verhalten zu bewegen (z. B. durch gezielte Werbung), oder sie kann im Extremfall sogar ermöglichen, eine Person zu einem bestimmten Verhalten zu zwingen (z. B. durch Erpressung). Der Datenskandal rund um Facebook-Cambridge-Analytica zeigt, wie weit die auf personenbezogenen Daten basierende Macht reichen kann, wenn sie die Grundwerte der Demokratie bedroht. Die Nutzung personenbezogener Daten durch totalitäre Überwachungsstaaten, um Macht über ihre Bürger auszuüben, ist vielleicht die ultimative Veranschaulichung des Problems.

Es war schon immer möglich, durch personenbezogene Daten Macht über Personen zu erlangen. In der Vergangenheit haben jedoch die begrenzten technischen Möglichkeiten in der Regel eingeschränkt, wer Zugang zu dieser Macht hatte[9] und wie viele Informationen tatsächlich erhoben und verarbeitet werden konnten. Mit dem Aufkommen der elektronischen Datenverarbeitung hat sich die Situation drastisch geändert. Das Speichern, Auffinden, Kombinieren und Analysieren von Daten ist immer kostengünstiger und für jeden zugänglich geworden. Das Aufkommen persönlicher Geräte und allgegenwärtiger Sensoren hat die Erfassung personenbezogener Daten drastisch vereinfacht. Der Datenschutz ist die Antwort auf das zunehmende Risiko für den Einzelnen, das mit dieser Situation einhergeht.

---

4 Siehe S. 104–105 in Pohle, Jörg. (2018). Datenschutz und Technikgestaltung : Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung, Berlin, Deutschland: Humboldt-Universität zu Berlin, DOI http://dx.doi.org/10.18452/19136, https://edoc.hu-berlin.de/handle/18452/19886 (zuletzt besucht am 11.03.2020),.

5 Persönliche Kommunikation mit Jörg Pohle.

6 Siehe zum Beispiel Austin, Lisa M., Enough About Me: W:hy Privacy is About Power, Not Consent (or Harm) (1. Januar 2014). Erscheint demnächst in Austin Sarat, Hrsg., A World Without Privacy? What Can/Should Law Do.. Verfügbar bei SSRN: https://ssrn.com/abstract=2524512.

7 Beachten Sie, dass die Verarbeitung personenbezogener Daten für private Zwecke in einem Haushalt vom Datenschutz ausgenommen ist (siehe Artikel 2 Absatz 2 Buchstabe b DSGVO).

8 Eine abschreckende Wirkung liegt vor, wenn die rechtmäßige Ausübung eines Rechts oder einer Freiheit durch die Datenverarbeitung, z. B. durch Videoüberwachung, behindert oder erschwert wird.

9 Der Zugang war z. B. durch hohe Kosten eingeschränkt.

So wie Datenschutzgesetze als Mittel zur Beseitigung von Machtungleichgewichten zwischen Einzelpersonen und Organisationen im Zusammenhang mit der Datenverarbeitung angesehen werden können, können Kartellgesetze als Mittel zur Beseitigung von Machtungleichgewichten auf dem Markt betrachtet werden[10].

1.4 Wie ist die Grundstruktur der Datenschutz-Grundverordnung?

Grundsätzlich ist es nicht wünschenswert, durch die Verarbeitung von Daten Macht über Personen zu erlangen, da dies die Rechte und Freiheiten von Personen beeinträchtigen kann. Die Verarbeitung personenbezogener Daten gänzlich zu verbieten, wäre jedoch übertrieben. Insbesondere könnten dadurch andere Grundrechte und -freiheiten wie beispielsweise die unternehmerische Freiheit beeinträchtigt werden[11]. Aus diesem Grund müssen die Datenschutzvorschriften ein Gleichgewicht zwischen all diesen Rechten herstellen.

Daher verwendet die Datenschutz-Grundverordnung die folgende Grundstruktur:

- Die Verarbeitung ist nur zu bestimmten **Zwecken** erlaubt;
- und dann nur unter bestimmten Bedingungen, wie die Verarbeitung **durchgeführt wird**.

Dies wird in der Folge näher erläutert.

In diesem Zusammenhang bestimmt die **Durchführung der Verarbeitung** unter anderem, welche Daten erhoben werden, welche personellen und technischen Ressourcen (Computerhardware und -infrastruktur) die Daten auf welche Weise (Software und Verfahren) und für wie lange verarbeiten und an wen die Daten weitergegeben werden.

1.5 Für welche Zwecke ist die Verarbeitung zulässig?

Grundsätzlich verbietet die DSGVO die Verarbeitung personenbezogener Daten, es sei denn, sie erfolgt zu **legitimen und rechtmäßigen Zwecken**[12].

Ein **Zweck** beschreibt ein konkretes Ziel, das durch die Verarbeitung erreicht werden soll.

Rechtmäßig bedeutet die Einhaltung des Wortlauts des Gesetzes (nicht nur der DSGVO), des Geistes des Gesetzes (z. B. ohne Ausnutzung von Gesetzeslücken), der Werte der Gesellschaft (wie sie beispielsweise in der Europäischen Charta der Grundrechte zum Ausdruck kommen) und der ethischen Grundsätze. In bestimmten Forschungsbereichen kann die Einhaltung der ethischen Grundsätze in formellen Verfahren wie der Genehmigung durch eine Forschungsethikkommission überprüft werden.

Die Rechtmäßigkeit ist in Artikel 6 der Datenschutz-Grundverordnung definiert. Damit eine Verarbeitung rechtmäßig ist, muss ihr Zweck in eine der sechs vorgesehenen Kategorien fallen, die als *Rechtsgrundlage* bezeichnet werden[13]. Die Verantwortlichen dürfen personenbezogene Daten nur verarbeiten, wenn sie eine gültige Rechtsgrundlage vorweisen können.

---

10 Reiner Rehak, Was schützt eigentlich der Datenschutz?, Vortrag auf dem 35. Chaos Communication Congress (35C3), Leipzig, Deutschland, 28.12.18, Folie 18, https://mirror.netcologne.de/CCC/congress/2018/slides-pdf/35c3-9733-was_schutzt_eigentlich_der_datenschutz.pdf (zuletzt besucht am 24.04.2020).

11 Siehe Artikel 16 der Europäischen Charta der Grundrechte.

12 Siehe Artikel 5 Absatz 1 Buchstaben a und b der Datenschutz-Grundverordnung.

13 Siehe Artikel 6 Absatz 1 der Datenschutz-Grundverordnung.

Bezogen auf das Problem des Datenschutzes bedeutet dies, dass die Erlangung von Macht über Einzelpersonen nur dann zulässig ist, wenn sie legitimen Zwecken dient, wie sie in der Datenschutz-Grundverordnung vorgesehen sind.

1.6 Was sind die Bedingungen für die Durchführung der Verarbeitung?

Die Verarbeitung personenbezogener Daten zu rechtmäßigen und legitimen Zwecken ist somit zulässig, allerdings nur unter bestimmten Bedingungen. Im Folgenden werden diese Bedingungen ausführlicher beschrieben.

Der Grundgedanke dieser Bedingungen besteht darin, die **Macht** der Organisation, die personenbezogene Daten verarbeitet (die sogenannten ***Verantwortlichen***), gegenüber den Betroffenen (den sogenannten ***betroffenen Personen)*** zu begrenzen und auszugleichen.

Im Überblick wird dies auf folgende Weise erreicht:

- Rechenschaftspflicht des Verantwortlichen
- Befähigung der betroffenen Personen
- Machtgleichgewicht durch eine Aufsichtsbehörde
- die Einschränkung, dass die Verantwortlichen die erlangte Macht ausschließlich zur Erreichung der erklärten rechtmäßigen Zwecke nutzen dürfen
- Beschränkung der erlangten Macht auf das zur Erfüllung der rechtmäßigen Zwecke erforderliche Mindestmaß
- Schutz der Investitionen und des Vermögens der betroffenen Personen
- Verbot von Verarbeitungen, die nicht mit dem Zweck vereinbar sind

Die einzelnen Aufzählungspunkte werden in den folgenden Abschnitten näher erläutert.

1.6.1 Verantwortliche sind voll rechenschaftspflichtig

Eine erste Maßnahme zur Begrenzung der Macht der Verantwortlichen besteht darin, sie in vollem Umfang für die gesamte Verarbeitungstätigkeit verantwortlich zu machen. Dies ist einer der wichtigsten Grundsätze der Datenschutz-Grundverordnung (siehe Art. 5 Absatz 2). Er geht über die bloße Verpflichtung der Verantwortlichen hinaus, ihre Verarbeitung (gegenüber den betroffenen Personen und den Aufsichtsbehörden) **transparent**[14] zu machen. Vielmehr sind die Verantwortlichen verpflichtet, die **Einhaltung der** Datenschutz-Grundverordnung tatsächlich **nachzuweisen**. Dadurch wird die Verarbeitung klar für die Aufsicht geöffnet. Außerdem wird die „Beweislast“ eindeutig zugewiesen: Nicht die betroffenen Personen oder die Aufsichtsbehörden müssen einen Verstoß gegen die DSGVO nachweisen; Intransparenz, die eine Nichteinhaltung bedeutet, ist an sich schon ein Verstoß.

Um dies in der Praxis zu erreichen, stellt die Datenschutz-Grundverordnung in einem ersten Schritt sicher, dass die volle **Verantwortung** eindeutig bei dem/den (gemeinsamen) Verantwortlichen liegt, der/die die Zwecke und Mittel der Verarbeitung bestimmt/bestimmen[15]. Dies geschieht beispielsweise dadurch, dass die Verantwortlichen verpflichtet werden, ihre **Mitarbeiter** zu kontrollieren[16], und dass Verträge[17] mit möglichen

14 Beachten Sie, dass Transparenz auch ein Grundsatz der Datenschutz-Grundverordnung ist, siehe Art. 5 Abs. 1 Buchstabe a.
15 Siehe Art. 4 Absatz 7 DSGVO.
16 Siehe Art. 29 und 32 Absatz 4 DSGVO.
17 Siehe Art. 28 Absatz 3 DSGVO.

externen Rechenzentren (sogenannten ***Auftragsverarbeitern***) abgeschlossen werden, die eine Kontrolle bis hin zum Recht auf Vor-Ort-Prüfungen durch den Verantwortlichen gewährleisten.[18]

Sobald die Verantwortung geklärt ist, sind die Verantwortlichen verpflichtet, die Verarbeitung völlig **transparent zu gestalten**. Dazu gehört, dass sie die **betroffenen Personen** proaktiv über die Existenz und die wichtigsten Merkmale der Verarbeitung **informieren**[19] und auf Anfrage weitere Informationen bereitstellen[20]. Für den letztgenannten Zweck müssen die Verantwortlichen in der Regel auch einen *Datenschutzbeauftragten* benennen[21], dessen Kontaktdaten Teil der vorgeschriebenen Informationen sind[22] und der als Kontaktstelle für die betroffenen Personen dient[23].

Darüber hinaus müssen die Verantwortlichen sowohl die zuständige **Aufsichtsbehörde**[24] als auch (bei wahrscheinlich hohem Risiko) die betroffenen Personen über Datenschutzverletzungen informieren[25]. Darüber hinaus müssen die Verantwortlichen für die Aufsichtsbehörden Verzeichnisse über alle Verarbeitungstätigkeiten, die personenbezogene Daten[26] betreffen, führen und in der Lage sein, eine *Datenschutz-Folgenabschätzung* für Verarbeitungstätigkeiten vorzulegen, die wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führen[27]. Letztere ist ein wichtiges Instrument, um die Einhaltung der DSGVO *nachzuweisen*.

1.6.2 Befähigung der betroffenen Personen

Da bei der Datenverarbeitung ein Machtungleichgewicht besteht, stärkt die Datenschutz-Grundverordnung die schwächere Partei, d. h. die betroffenen Personen. Dadurch werden die betroffenen Personen von machtlosen Beobachtern der Verarbeitung zu Beteiligten, die ihre Rechte und Freiheiten durch Intervention verteidigen können.

Die Datenschutz-Grundverordnung stärkt die Rechte der betroffenen Personen vor allem durch die so genannten ***Rechte der betroffenne Person***[28]. Dazu gehören die Folgenden[29]:

- Das *Recht auf Auskunft*[30] über die verarbeiteten Daten der betroffenen Person,
- das *Recht auf Berichtigung*[31], das es erlaubt, unrichtige personenbezogene Daten zu berichtigen und unvollständige Daten zu ergänzen,
- das *Recht auf Löschung*[32], das auch das *Recht auf Vergessenwerden* genannt wird,
- das *Recht auf Einschränkung der Verarbeitung*[33], das es den betroffenen Personen ermöglicht, unter bestimmten Umständen die Einstellung der Verarbeitung ihrer Daten zu verlangen[34].

---

18 Siehe Art. 28 Absatz 3 Buchstabe h DSGVO.
19 Siehe Art. 13 und 14 DSGVO.
20 Siehe zum Beispiel Art. 15 12 Absatz 3 und 19 DSGVO.
21 Siehe Art. 37 DSGVO.
22 Siehe Art. 13 Absatz 1 Buchstabe b und 14 Absatz 1 Buchstabe b DSGVO.
23 Siehe Art. 38 Absatz 4 DSGVO.
24 Siehe Art. 33 DSGVO.
25 Siehe Art. 34 DSGVO.
26 Siehe Art. 30 DSGVO.
27 Siehe Art. 35 DSGVO.
28 Siehe Kapitel 3 DSGVO, das die Artikel 12 bis 23 umfasst.
29 Beachten Sie, dass das Recht auf Datenübertragbarkeit im Abschnitt über den Schutz des Vermögens der betroffenen Person behandelt wird.
30 Siehe Art. 15 DSGVO.
31 Siehe Art. 16 DSGVO.
32 Siehe Art. 17 DSGVO.

- das *Widerspruchsrecht*[35], das es den betroffenen Personen ermöglicht, unter bestimmten Umständen die Einstellung der Verarbeitung ihrer Daten zu verlangen.
- das *Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden,* die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt[36], einschließlich des *Rechts auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen*[37].

Über diese Rechte hinaus haben die betroffenen Personen weitere Rechte:

- Das *Recht, die Einwilligung jederzeit zu widerrufen*[38], wenn die Rechtsgrundlage der Verarbeitung die Einwilligung ist [39].
- Das Recht, von dem Verantwortlichen darüber informiert zu werden, wie die Geltendmachung der Rechte der betroffenen Person an alle Empfänger weitergegeben wird[40].

1.6.3 Machtausgleich durch die Einrichtung von Aufsichtsbehörden

Obwohl die betroffenen Personen durch die oben genannten Rechte gestärkt werden, reichen ihre Mittel möglicherweise nicht aus, um sie durchzusetzen. Insbesondere können sie sich außerstande sehen, von ihrem *Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen Verantwortlichen oder einen Auftragsverarbeiter*[41] selbst Gebrauch zu machen. Aus diesem Grund räumt die Datenschutz-Grundverordnung den betroffenen Personen das ***Recht ein, eine Beschwerde bei einer Aufsichtsbehörde***[42] ***einzureichen***.

Mit anderen Worten: Die DSGVO gibt den betroffenen Personen einen Verbündeten an die Hand, dessen Macht mit der des Verantwortlichen vergleichbar sind oder darüber hinausgeht und somit ausreicht, um die Rechte der betroffenen Personen durchzusetzen.

Die Datenschutz-Grundverordnung räumt den Aufsichtsbehörden daher entsprechende Befugnisse ein[43]. Diese reichen von Untersuchungsbefugnissen[44] wie Audits vor Ort[45] bis hin zu Abhilfebefugnissen[46] wie die Verhängung von Geldbußn[47], die Anordnung der Aussetzung der Übermittlung von Daten an die Empfänger[48] und die Verhängung eines vollständigen Verbots der Verarbeitung[49].

---

33 Siehe Art. 18 DSGVO.
34 Diese Umstände sind in Art. 18 Absatz 1 DSGVO aufgeführt.
35 Siehe Art. 21 DSGVO.
36 Siehe Art. 22 DSGVO.
37 Siehe Art. 22 Absatz 3 DSGVO.
38 Siehe Art. 7 Absatz 3 DSGVO.
39 Siehe Art. 6 Absatz 1 Buchstabe a und 9 Absatz 2 Buchstabe a DSGVO.
40 Siehe Art. 19 DSGVO, zweiter Satz.
41 Siehe Art. 79 DSGVO.
42 Siehe Art. 77 DSGVO.
43 Siehe Art. 58 DSGVO.
44 Siehe Art. 58 Absatz 1 DSGVO.
45 Siehe Art. 58 Absatz 1 Buchstabe b und f DSGVO.
46 Siehe Art. 58 Absatz 2 DSGVO.
47 Siehe Art. 58 Absatz 2 Buchstabe i DSGVO.
48 Siehe Art. 58 Absatz 2 Buchstabe j DSGVO.
49 Siehe Art. 58 Absatz 2 Buchstabe f DSGVO.

1.6.4 Beschränkung der Verantwortlichen darauf, die Macht ausschließlich zur Erreichung der erklärten rechtmäßigen Zwecke zu nutzen

Durch den Nachweis, dass die Zwecke legitim und rechtmäßig sind, hat ein Verantwortlicher den mit der Verarbeitungstätigkeit verbundenen Machtzuwachs gerechtfertigt. Es liegt auf der Hand, dass die Nutzung dieser Macht für andere Zwecke nicht gerechtfertigt wäre. Mit anderen Worten, die Erlaubnis zur Verarbeitung ist auf die erklärten Zwecke, für die die Daten erhoben werden, beschränkt.

Die Datenschutz-Grundverordnung nennt diesen Grundsatz **„Zweckbindung“** (siehe Art. 5 Absatz 1 Buchstabe b).

Die technische und organisatorische Umsetzung dieses Grundsatzes erfolgt durch die **Trennung** verschiedener Verarbeitungstätigkeiten.

Als zweite Verteidigungslinie gilt: Selbst wenn Daten aus verschiedenen Verarbeitungstätigkeiten zusammenkommen, können Maßnahmen wie die Pseudonymisierung eine tatsächliche Kombination durch die Verknüpfung von Datensätzen, die sich auf dieselbe Person beziehen erschweren.

Beachten Sie, dass diese Regel auch die **Anhäufung von Macht** durch die Kombination von Daten aus verschiedenen Verarbeitungstätigkeiten verhindert. Eine solche Kombination würde typischerweise zu einem tieferen Einblick in das Leben der betroffenen Personen führen, der mehr Aspekte abdeckt, oder zu einer breiteren Abdeckung von Wissen, das eine größere Anzahl von betroffenen Personen umfasst. In beiden Fällen kann argumentiert werden, dass die kombinierte Macht größer ist als die Summe ihrer Teile.

1.6.5 Beschränkung der Macht auf das zur Erfüllung der erklärten Ziele erforderliche Maß

Während der Nachweis der Legitimität und Rechtmäßigkeit der Zwecke die Verarbeitung als solche gerechtfertigt hat, muss sie so durchgeführt werden, dass der Machtzuwachs auf das zur Erfüllung dieser Zwecke notwendige Mindestmaß beschränkt wird. Diese Minimierung der Macht betrifft die folgenden drei Aspekte:

- Informationsgehalt der personenbezogenen Daten
- Grad der Verknüpfung der Daten mit der betroffenen Person und
- Begrenzung der Empfänger, die Zugang zur Macht haben.

Diese werden im Folgenden ausführlicher beschrieben.

1.6.5.1 Minimierung des Informationsgehalts (d. h. der Macht)

Da Wissen Macht ist, bedeutet die Minimierung der Macht, dass die erhobenen personenbezogenen Daten auf ein Minimum beschränkt werden müssen. Nur die Daten, die nachweislich für die Erfüllung der erklärten Zwecke erforderlich sind, können rechtmäßig erhoben werden.

Die Datenschutz-Grundverordnung nennt diesen Grundsatz **„Datenminimierung“** (siehe Art. 5 Absatz 1 Buchstabe c). Konkret verlangt sie, dass die erhobenen Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt“ sind. Bei einer zeitlichen Betrachtung wird außerdem verlangt, dass die Daten nicht länger als für die Zwecke erforderlich gespeichert werden. Bei komplexeren Verarbeitungen mit mehreren Phasen sollte jede Phase nur die wirklich notwendigen Daten enthalten, wobei der Informationsgehalt zwischen den Phasen zu reduzieren ist.

1.6.5.2 Minimierung der Verbindung zur betroffenen Person

Die Leichtigkeit, mit der Macht über die betroffene Person ausgeübt werden kann, hängt davon ab, inwieweit die betroffene Person mit den Daten in Verbindung gebracht werden kann. Die Stärke der Verbindung zwischen Daten und der betroffenen Person sollte daher so gering wie möglich gehalten werden.

Die Datenschutz-Grundverordnung unterscheidet zwischen drei Arten von Daten mit unterschiedlichem Grad der Verknüpfung:

- Vollständig identifizierende Daten,
- pseudonymisierte Daten und
- anonymisierte Daten.

Ersteres erlaubt die „**direkte Identifizierung**“[50] der betroffenen Person durch die Zuordnung zu einer „**Kennung**“ wie einem Namen, zu einer Kennnummer, zu Standortdaten [oder] zu einer Online-Kennung“[51]; **pseudonymisierte Daten** erlauben die **Identifizierung nur durch die Verwendung „zusätzlicher Informationen“**[52]; und **anonyme Daten**, bei denen „**die betroffene Person nicht oder nicht mehr identifiziert werden kann**“[53].

Analog zur Datenminimierung sind die Daten so zu erheben, dass sie möglichst wenig mit der betroffenen Person in Verbindung gebracht werden. Im Hinblick auf den zeitlichen Aspekt gilt: „Personenbezogene Daten werden in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“[54]. Im Falle einer komplexeren Verarbeitung mit mehreren Phasen sollte jede Phase nur den minimalen Grad an Assoziation aufweisen, der wirklich notwendig ist, und zwischen den Phasen sollte eine Pseudonymisierung oder Anonymisierung verwendet werden.

Die Datenschutz-Grundverordnung nennt diesen Grundsatz **„Speicherbegrenzung“** (siehe Art. 5(1)(e)).

1.6.5.3 Beschränkung des Zugangs zur Macht

Die Macht liegt in den Händen von Personen und Organisationen. Wenn Wissen Macht ist, steht diese Macht nur denjenigen zur Verfügung, denen die personenbezogenen Daten offengelegt werden. In der Datenschutz-Grundverordnung werden diese Parteien als *Empfänger* bezeichnet[55]. Dabei kann es sich entweder um Mitarbeiter des Verantwortlichen oder des Auftragsverarbeiters, um beabsichtigte Drittempfänger oder um unbeabsichtigte Parteien wie Angreifer handeln.

Der Zugriff auf die Daten muss auf das beschränkt sein, was zur Erfüllung der erklärten Zwecke erforderlich ist. Die Datenschutz-Grundverordnung nennt diesen Grundsatz **„Vertraulichkeit“**[56].

Die Vertraulichkeit hat zwei Aspekte:

---

50 Dieser Begriff wird in Art. 4 Absatz 1 DSGVO.
51 Diese Formulierung stammt aus Art. 4 Absatz 1 DSGVO.
52 Beachten Sie, dass dieser Begriff in Art. 4 Absatz 5 DSGVO verwendet wird, der die Definition für *Pseudonymisierung* enthält.
53 Diese Formulierung ist dem 5. Satz von Erwägungsgrund 26 der Datenschutz-Grundverordnung entnommen.
54 Diese Formulierung stammt aus Art. 5 Absatz 1 Buchstabe e DSGVO.
55 Siehe Art. 4(9).
56 Siehe Art. 5 Absatz 1(f).

- Verhinderung des Zugriffs durch Unbefugte und
- Beschränkung des Zugriffs auf autorisierte Parteien.

Ersteres schützt weitgehend vor externen Angreifern mit Maßnahmen wie der Verschlüsselung von Daten im Ruhezustand oder von Kommunikationen mit Firewalls. Letzteres wird gewöhnlich als **Zugangskontrolle** bezeichnet. Sie stellt sicher, dass derjenige, der auf die Daten zugreift, tatsächlich berechtigt ist (Authentifizierung), beschränkt den Zugriff auf die Daten, die benötigt werden (Zugriffsrechte) und kann den Zugriff auf die Zeiten beschränken, in denen er notwendig ist.

1.6.6 Schutz des Vermögens der betroffenen Person

Bei vielen Arten von Verarbeitungstätigkeiten sind die vom Verantwortlichen gespeicherten personenbezogenen Daten auch für die betroffene Person von erheblichem Wert. Paradebeispiele sind Cloud-basierte Fotosammlungen, Office-Suiten und Dokumentenmanagementsysteme, aber auch medizinische Daten, die beim Arzt eines Patienten gespeichert sind. Wir bezeichnen solche Daten als *Vermögenswerte*.

Diese Vermögenswerte können für den Verantwortlichen von weitaus geringerem Wert sein, der somit möglicherweise zögert, erheblich in ihren Schutz zu investieren. Eine Möglichkeit, wie ein Verantwortlicher Macht über eine betroffene Person ausüben kann, besteht auch darin, den Zugang zu den Vermögenswerten der betroffenen Person von bestimmten Bedingungen abhängig zu machen.

Um eine solche Machtausübung zu verhindern, verpflichtet die Datenschutz-Grundverordnung die Verantwortlichen, die Vermögenswerte der betroffenen Personen zu schützen. Sie verlangt insbesondere, dass diese Vermögenswerte geschützt werden vor:

- uunbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung[57] und
- der Weigerung, der betroffenen Person die Nutzung der Vermögenswerte unabhängig von dem Verantwortlichen zu gestatten.

Die erste Art des Schutzes wird auch als **Verfügbarkeit** und **Belastbarkeit**[58] bezeichnet. Letzteres wird als **Datenübertragbarkeit** bezeichnet und ist eines der Rechte[59] der betroffenen Person.

1.6.7 Verbot von Verarbeitungen, die nicht für den Zweck geeignet sind

Die Erlangung von Macht durch eine Verarbeitung, die nicht geeignet ist, die erklärten Zwecke zu erfüllen, ist offensichtlich unrechtmäßig.

Die Datenschutz-Grundverordnung verwendet zwei Grundsätze zur Durchsetzung der Zweckmäßigkeit:

- **Integrität** (siehe Art. 5 Absatz 1 Buchstabe f) und
- **Genauigkeit** (siehe Art. 5 Absatz 1 Buchstabe d).

Erstere schreibt vor, dass die Daten vor unbeabsichtigter Schädigung oder nicht genehmigter Änderung zu schützen sind, Letztere dagegen, dass die Daten auf dem neuesten Stand und richtig sein müssen und dass sie anderenfalls unverzüglich zu löschen oder zu berichtigen sind.

---

57 Siehe Art. 5 Absatz 1(f) DSGVO.
58 Siehe Art. 32 Absatz 1 Buchstabe b und (c) DSGVO.
59 Siehe Art. 20 DSGVO.

1.7 Der Begriff des Risikos

Risiko ist ein wichtiger Begriff in der Datenschutz-Grundverordnung[60]. Die dargelegte Ansicht, dass es beim Datenschutz darum geht, das Machtungleichgewicht zwischen dem Verantwortlichen und der betroffenen Person auszugleichen, verdeutlicht auch den Begriff des Risikos:

Das Hauptrisiko besteht darin, dass die Verarbeitung personenbezogener Daten tatsächlich zu einem Machtungleichgewicht führt, das die Rechte und Freiheiten der betroffenen Personen einschränkt. Unter diesem Gesichtspunkt wird deutlich, dass das Risiko nicht darin besteht, dass ein unerwünschtes Ereignis eintritt (wie ein Angriff oder eine Naturkatastrophe), sondern vielmehr darin, dass der Verantwortliche eine übermäßige Macht über die betroffenen Personen ausübt.

Dieses Risikoverständnis unterscheidet sich stark vom Risikoverständnis im Bereich der Cybersicherheit. Dort wird der Verantwortliche in der Regel als der „Gute" gesehen, der sich gegen überwiegend externe „Angriffe" verteidigt. Im Datenschutz hingegen ist das Verhalten des Verantwortlichen, d. h. die Verarbeitungstätigkeit, die Quelle des Risikos. Die Wahrscheinlichkeit, dass dies geschieht, liegt bei 100 %. Anders als bei der Cybersicherheit müssen die Verantwortlichen nun die schwächere betroffene Person vor den Risiken schützen, die aus ihrer eigenen Verarbeitung resultieren. Die Verantwortlichen sind also nicht mehr automatisch die Guten, sondern müssen sich ausdrücklich darum bemühen, nicht selbst zum Bösen zu werden.

Für Menschen, die hauptsächlich mit der Cybersicherheit vertraut sind, kann das Verständnis des Datenschutzes einen erheblichen mentalen Wandel erfordern. Das Verständnis dieses Unterschieds ist eine Voraussetzung für die Einhaltung der Datenschutz-Grundverordnung. Zur weiteren Lektüre empfehlen wir einen Artikel[61] über acht verschiedene Arten von Risiken.

60 Siehe zum Beispiel Art. 24 Absatz 1, 35 Absatz 1 und die Erwägungsgründe 75 und 84.

61 Martin Rost, Risks in the context of data protection, http://www.maroki.de/pub/privacy/Rost_Martin_2019-02_Risk:_8types_v1.pdf (zuletzt besucht am 5.8.2020).