VERBAND KOMMUNALER UNTERNEHMEN e.V.

FAQ UND ANTWORTEN

zur Datenschutzgrundverordnung (DS-GVO)

Berlin, August 2017

Der Verband kommunaler Unternehmen (VKU) vertritt rund 1.460 kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Mit über 262.000 Beschäftigten wurden 2015 Umsatzerlöse von mehr als 115 Milliarden Euro erwirtschaftet und rund 11 Milliarden Euro investiert. Die VKU-Mitgliedsunternehmen haben im Endkundensegment große Marktanteile in zentralen Versorgungsbereichen (Strom 60 Prozent, Erdgas 65 Prozent, Trinkwasser 87 Prozent, Wärmeversorgung 69 Prozent, Abwasserentsorgung 42 Prozent). Sie entsorgen jeden Tag 31.500 Tonnen Abfall und tragen entscheidend dazu bei, dass Deutschland mit 66 Prozent die höchste Recyclingquote in der Europäischen Union hat. Die kommunalen Unternehmen versorgen 5,7 Millionen Kunden mit Breitband. Bis 2018 planen sie Investitionen von rund 1,7 Milliarden Euro, um dann insgesamt 6,3 Millionen Menschen an schnelles Internet anschließen zu können.

Verband kommunaler Unternehmen e.V. · Invalidenstraße 91 · 10115 Berlin
Fon +49 30 58580-0 · Fax +49 30 58580-100 · info@vku.de · www.vku.de

DIE KOMMUNALEN UNTERNEHMEN

Inhalt

Vorwort 5

1. Anwendungsbereich 8

1.1. Für wen gelten die DS-GVO und das DSAnpUG-EU? 8

1.2. Wo stehen die wesentlichen Begriffsbestimmungen in der DS-GVO und im DSAnpUG-EU? 14

1.3. Was ist unter „Verarbeitung“ von Daten zu verstehen und ist somit eine „Verarbeitungstätigkeit“? 14

1.4. Was ist unter einer Einwilligung zu verstehen? Wie kann eine Einwilligung erfolgen oder eingeholt werden? Welche Form kann die Einwilligung haben? .. 15

1.5. Welche Daten sind gemäß der DS-GVO personenbezogene Daten? 19

1.6. Welche besonderen Kategorien personenbezogener Daten gibt es und was gilt für sie? 20

1.7. Wer ist „Verantwortlicher“ im Sinne der DS-GVO? Können mehrere „gemeinsam Verantwortlicher“ sein? Was setzt dies voraus? 21

1.8. Wofür trägt der Verantwortliche die Verantwortung? 22

1.9. Welche Anforderungen werden an technische und organisatorische Maßnahmen sowie an die Sicherheit der Datenverarbeitung gestellt? 23

1.10. Auftragsverarbeitung: Was ist bei der Verarbeitung von Daten auf Weisung des Verantwortlichen zu beachten? 27

1.11. Rechenschaftspflicht. Was sind die Grundsätze für die Verarbeitung von personenbezogenen Daten? 29

1.12. Welche Dokumentations- und Nachweispflichten hat der Verantwortliche? 30

1.13. Wann haftet der Verantwortliche? 41

1.14. Wann haftet der Verantwortliche nicht? 42

1.15. Welche weiteren Dokumentations- und Nachweispflichten sind zu beachten? . 42

1.16. Was umfasst das Recht auf „Datenübertragbarkeit“? 45

2. Grundsätzliche organisatorische Aspekte 50

2.1. Was sind wichtige Punkte beim Aufbau von Datenschutzmanagementsystem und Datenschutzorganisation? 50

2.2. Was ist bei der Gestaltung des Datenschutzniveaus (Systeme, Anwendungen, Prozesse) zu beachten? 52

2.3. Wann muss ein Datenschutzbeauftragter benannt werden? 54

2.4. Was sind Funktion und Aufgaben des Datenschutzbeauftragten? ... 56
2.5. Welche Auswirkungen ergeben sich für die Bestellung von betrieblichen Datenschutzbeauftragten in einer Unternehmensgruppe? ... 57
2.6. Sofern ein Datenschutzbeauftragter bestellt wird, welchen externen Stellen ist dies mitzuteilen? ... 57
2.7. In welchem Verhältnis stehen Datenschutzbeauftragter und Aufsichtsbehörde zueinander? ... 58
2.8. Was sind die wesentlichen Schritte bei der Erstellung eines Verarbeitungsverzeichnisses? ... 59
2.9. Was sind die Vorgaben für die Erstellung des Verarbeitungsverzeichnisses? ... 60
2.10. Welche sind die erforderlichen Inhalte des Verarbeitungsverzeichnisses nach DS-GVO und nach DSAnpUG-EU? ... 61
2.11. Welche Verpflichtungen auf Datengeheimnisse gibt es zukünftig? ... 62
2.12. Besteht Anpassungsbedarf von Betriebsvereinbarungen und bestehenden Dokumenten? ... 63
3. Zulässigkeit und Anforderungen bei der Erhebung, Verarbeitung und Nutzung von Daten ... 64
3.1. Welches sind die wesentlichen Voraussetzungen für die Erhebung von Daten? 64
3.2. Welche Informationspflichten bestehen zukünftig? ... 65
3.3. Welche Informationspflichten bestehen bei der Erhebung personenbezogener Daten bei der betroffenen Person (Art. 13 DS-GVO)? ... 66
3.4. Welche Ausnahmen gibt es bei den Informationspflichten bei der Erhebung personenbezogener Daten bei der betroffenen Person? ... 70
3.5. Welche Informationspflichten bestehen, wenn die Erhebung NICHT direkt bei dem Betroffenen erfolgt (Art. 14 DS-GVO)? ... 72
3.6. Welche Ausnahmen gibt es bei den Informationspflichten bei der Erhebung personenbezogener Daten NICHT bei der betroffenen Person? ... 73
3.7. Was gilt für den Datenaustausch im Konzern? ... 75
3.8. Welche Grundlagen gelten zukünftig für den Betrieb von Videoeinrichtungen? 75
4. Auftragsverarbeitung ... 76
4.1. Wann liegt eine Auftragsverarbeitung vor? ... 76
4.2. Wer kommt als Auftragsverarbeiter in Frage? ... 77
4.3. Wie kommt die Beauftragung/Bestellung eines Auftragsverarbeiters zu Stande? ... 77
4.4. Was ist inhaltlich bei der Beauftragung eines Auftragsverarbeiters mindestens zu regeln? ... 78

4.5. Was gilt, wenn dem Auftragsverarbeiter Verletzungen des Schutzes personenbezogener Daten bekannt werden? 82
4.6. Was enthält das Verzeichnis der Verarbeitungstätigkeiten im Fall der Auftragsverarbeitung? 82
4.7. Was ist gemeint mit der neuen Regelung als „gemeinsam für die Verarbeitung Verantwortliche“? 83
4.8. Wer haftet, wenn sich ein Auftragsverarbeiter nicht an seine Pflichten hält? 84
4.9. Gibt es die „Funktionsübertragung“ weiterhin? 85
4.10. Wie verhält es sich mit der Übermittlung personenbezogener Daten in Drittländer? 86
5. Rechte des Betroffenen 86
5.1. Welche Rechte haben betroffene Personen auf Basis der Datenschutzgrundverordnung? 86
6. Sanktionen 95
6.1. Welche Sachverhalte sind sanktioniert? Welche Höhe haben die Sanktionen? 95

Vorwort

Für die Zukunft gilt: **Alles, was digitalisiert werden kann, wird digitalisiert:** eine City Cloud für den sicheren Datenverkehr, Abholzeiten von Abfallbehältern, Informationen zum Trinkwasser per App, Smart Home-Angebote oder leistungsfähige Kommunikationsnetze. Das sind nur Ausschnitte von vielfältigen digitalen Angeboten, welche kommunale Unternehmen bereits heute zur Verfügung stellen. Zukünftig wird es noch stärker darum gehen, Daten intelligent zu vernetzen und neue Geschäftsfelder für kommunale Unternehmen zu finden. Damit einher geht eine wachsende Bedeutung von Datenschutz und IT-Sicherheit, um das vorhandene Vertrauen an Seriosität und Verlässlichkeit zur Daseinsvorsorge zu nutzen.

Zur **Stärkung des Datenschutzes** innerhalb der Europäischen Union (EU), insbesondere im Hinblick auf den **Schutz personenbezogener Daten** u.a. bei der Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen, wurde das Datenschutzrecht innerhalb der EU reformiert und es wurden einheitliche Regelungen geschaffen:

Nach intensiven Verhandlungen von mehr als vier Jahren trat am 24. Mai 2016 die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung**, nachfolgend: **DS-GVO**) als Teil der EU-Datenschutz-reform in Kraft. Sie gilt ab dem 25. Mai 2018 unmittelbar in jedem Mitgliedsstaat der EU.

Zur Anpassung des Datenschutzrechts an die DS-GVO sowie zur Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (zum Schutz natürlicher Personen bei der Verarbeitung

personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates) wurde von der Bundesregierung das **Datenschutz-Anpassungs- und Umsetzungsgesetz EU** (nachfolgend: **DSAnpUG-EU**) entwickelt und am 12. Mai 2017 vom Bundesrat verabschiedet. Das DSAnpUG-EU wurde am 5. Juli 2017 im Bundesgesetzblatt veröffentlicht. Damit tritt es am 25. Mai 2018 zeitgleich mit dem Gültigwerden der DS-GVO in Kraft.

Die DS-GVO beinhaltet u.a. Regelungen für die Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen. Im Fokus stehen Vorgaben zur Datenverarbeitung, Rechte von Betroffenen und Pflichten von Verantwortlichen. Bereits geltende Betroffenenrechte werden erweitert und um neue Rechte ergänzt.

Die wesentlichen Änderungen für kommunale Unternehmen auf einen Blick:

- Umfangreichere **Informations- und Dokumentationspflichten**.
- Wesentlich weitergehende **Sanktionsmöglichkeiten** bei Verstößen oder Nichterfüllung von Vorgaben (bis zu € 20 Mio. oder 4 % des Vorjahresumsatzes).
- Grundlage zur Umsetzung der Dokumentationspflichten ist das **„Verzeichnis von Verarbeitungstätigkeiten“** (Prozessdarstellungen), ein „öffentliches Verfahrensverzeichnis“ ist nicht mehr erforderlich.
- Wichtigere Rolle für den **Datenschutzbeauftragten** (Verpflichtung zur Zusammenarbeit mit der Aufsichtsbehörde, Prüf- und Kontrollpflichten).
- Ausweitung von **Prüf- und Kontrollpflichten** (z.B. Erforderlichkeit einer Datenschutz-Folgenabschätzung statt Vorabkontrolle).

Nicht alle Änderungen stellen aus Sicht kommunaler Unternehmen Verschärfungen dar. Eine Erleichterung ist beispielsweise die Möglichkeit, dass Konzerne einen gemeinsamen Datenschutzbeauftragten benennen können. Zudem bestehen einige Ausnahmeregelungen für den öffentlichen Sektor.

Der nachfolgende Fragen- und Antwortenkatalog („FAQ“) soll Fragen zur Umsetzung der DS-GVO und des DSAnpUG-EU, die sich für kommunale Unternehmen typischerweise stellen können, beantworten. Die Antworten orientieren sich überwiegend am Wortlaut der DS-GVO und des DSAnpUG-EU. Rechtsprechung oder Erfahrungswerte liegen noch nicht vor. Dieser FAQ stellt einen Überblick über die wesentlichen Anforderungen des neuen Gesetzesrahmens dar. Dem Leser soll ermöglicht werden, u.a. die Pflichten, die nun auf kommunale Unternehmen zukommen, zu erfassen und die Betroffenenrechte (bspw. von Mitarbeitern, Kunden, Geschäftspartnern), zu kennen und zu wahren sowie die neuen ordnungspolitischen Vorgaben umsetzen. Dies gilt insbesondere auch im Hinblick auf die erheblich ausgedehnten Sanktionsmöglichkeiten.

Der FAQ ist nicht abschließend. Rechts- und/oder Handlungspflichten oder ein Anspruch auf Vollständigkeit werden nicht begründet.

1. Anwendungsbereich

1.1. Für wen gelten die DS-GVO und das DSAnpUG-EU?

Ein kommunales Unternehmen muss zunächst einmal prüfen, ob es unter den Anwendungsbereich der DS-GVO und des DSAnpUG-EU fällt. Dies ist im Einzelfall zu prüfen; wird aber in den meisten Fällen der Fall sein. Nachfolgend erhalten Sie einen Überblick über den sachlichen und räumlichen Anwendungsbereich a) der DS-GVO und b) des DSAnpUG-EU. Zudem geben wir Ihnen c) einen Überblick über das Verhältnis zu anderen Rechtsvorschriften sowie über d) das Verhältnis zwischen der DS-GVO und dem DSAnpUG-EU.

a) Anwendungsbereich der DS-GVO:

aa) Sachlicher Anwendungsbereich

Die DS-GVO **gilt** für:

- die ganz oder teilweise automatisierte **Verarbeitung personenbezogener Daten** sowie
- die nichtautomatisierte **Verarbeitung personenbezogener Daten**, die in einem Dateisystem gespeichert sind.[1]

Die DS-GVO findet **keine Anwendung** auf die Verarbeitung personenbezogener Daten:

- im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrecht fällt[2],
- durch die Mitgliedstaaten i.R.v. Tätigkeiten, die in den Anwendungsbereich von Titel V, Kapitel 2 EUV fallen[3],

[1] vgl. Art. 2 Abs. 1 DS-GVO.
[2] vgl. Art. 2 Abs. 2 a) DS-GVO.
[3] vgl. Art. 2 Abs. 2 b) DS-GVO.

- durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten[4],
- durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.[5]

Zu personenbezogenen Daten siehe Ziff. 1.5 des FAQ.

bb) Räumlicher Anwendungsbereich

Die DS-GVO findet Anwendung auf die **Verarbeitung personenbezogener Daten**, soweit diese im Rahmen der Tätigkeiten einer **Niederlassung** eines Verantwortlichen oder eines Auftragsverarbeiters **in der Union** erfolgt.[6] Dabei kommt es nicht darauf an, ob die Verarbeitung in der Union stattfindet.[7] Maßgeblich ist der Ort der Niederlassung.

Die DS-GVO findet weiterhin Anwendung auf die Verarbeitung personenbezogener Daten:

- von **betroffenen Personen**, die sich **in der Union** befinden,
- durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung damit in **Zusammenhang** steht,

[4] vgl. Art. 2 Abs. 2 c) DS-GVO.
[5] vgl. Art. 2 Abs. 2 d) DS-GVO.
[6] vgl. Art. 3 Abs. 1 S. 1 DS-GVO.
[7] vgl. Art. 3 Abs. 1 S. 1 DS-GVO.

- betroffenen Personen in der Union **Waren oder Dienstleistungen anzubieten**, unabhängig davon, ob von der betroffenen Person eine Zahlung zu leisten ist[8] oder
- das **Verhalten betroffener Person zu beobachten**, soweit ihr Verhalten in der Union erfolgt.[9]

Weiterhin findet die DS-GVO Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund **Völkerrechts** dem Recht eines Mitgliedstaates unterliegt.[10]

b) Anwendungsbereich des DSAnpUG-EU:

Das DSAnpUG-EU unterscheidet hinsichtlich seines Anwendungsbereiches, ob es sich um eine öffentliche oder nicht-öffentliche Stelle handelt.

aa) Sachlicher Anwendungsbereich

aaa) Öffentliche Stelle

Das DSAnpUG-EU gilt für die Verarbeitung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,[11]
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie

   a) Bundesrecht ausführen oder

   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.[12]

[8] vgl. Art. 3 Abs. 2 a) DS-GVO.
[9] vgl. Art. 3 Abs. 2 b) DS-GVO.
[10] vgl. Art. 3 Abs. 3 DS-GVO.
[11] vgl. § 1 Abs. 1 Nr. 1 DSAnpUG-EU.

bbb) Nicht-öffentliche Stelle

Für **nicht-öffentliche Stellen** gilt die DS-GVO für die **ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten** sowie die **nicht-automatisierte Verarbeitung personenbezogener Daten**, die in einem **Dateisystem gespeichert** sind oder **gespeichert werden sollen**, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.[13]

Nicht-öffentliche Stellen sind **natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts**, soweit sie keine öffentliche Stellen des Bundes, der Länder oder Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder sind, die Aufgaben der öffentlichen Verwaltung wahrnehmen.[14] Zu den weiteren Begriffsdefinitionen siehe § 2 DSAnpUG-EU.

bb) Räumlicher Anwendungsbereich

aaa) Öffentliche Stelle

Das DSAnpUG-EU gilt bei öffentlichen Stellen ohne Einschränkung.[15]

bbb) Nicht-öffentliche Stelle

Bei **nicht-öffentlichen Stellen** findet es nur Anwendung, wenn:

- der Verantwortliche oder Auftragsverarbeiter **personenbezogene Daten im Inland verarbeitet**[16]**,**

[12] vgl. § 1 Abs. 1 S. 1 Nr. 2 DSAnpUG-EU.
[13] vgl. § 1 Abs. 1 S. 2 DSAnpUG-EU.
[14] vgl. § 2 Abs. 4 DSAnpUG-EU.
[15] vgl. § 1 Abs. 4 S. 1 DSAnpUG-EU.
[16] vgl. § 1 Abs. 4 S. 2 Nr. 1 DSAnpUG-EU.

- die Verarbeitung personenbezogener Daten im **Rahmen der Tätigkeiten einer inländischen Niederlassung** des Verantwortlichen oder Auftragsverarbeiters erfolgt[17] oder
- der Verantwortliche oder Auftragsverarbeiter zwar keine Niederlassung in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat, er aber in den **Anwendungsbereich DS-GVO** fällt.[18]

c) Verhältnis zu anderen Rechtsvorschriften:

Andere Rechtsvorschriften des Bundes über den Datenschutz gehen den Vorschriften des DSAnpUG-EU vor.[19] **Die Vorschriften des DSAnpUG-EU finden Anwendung, wenn ein Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend geregelt ist.**[20] Demnach gilt das DSAnpUG-EG immer dann, wenn keine anderweitigen Gesetze einschlägig sind.

Darüber hinaus bleibt die **Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten** oder von **Berufs- oder besonderen Amtsgeheimnissen**, die nicht auf gesetzlichen Vorschriften beruhen, bestehen.[21]

Bei Verarbeitungen zu Zwecken gemäß Art. 2 DS-GVO stehen die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz den Mitgliedstaaten der EU gleich. Andere Staaten gelten insoweit als Drittstaaten.[22]

[17] vgl. § 1 Abs. 4 S. 2 Nr. 2 DSAnpUG-EU.
[18] vgl. § 1 Abs. 4 S. 2 Nr. 3 DSAnpUG-EU.
[19] vgl. § 1 Abs. 2 S. 1 DSAnpUG-EU.
[20] vgl. § 1 Abs. 2 S. 2 DSAnpUG-EU.
[21] vgl. § 1 Abs. 2 S. 3 DSAnpUG-EU.
[22] vgl. § 1 Abs. 6 S. 1 und 2 DSAnpUG-EU.

Die Vorschriften des DSAnpUG-EU finden keine Anwendung, soweit das Recht der EU (im Besonderen die DS-GVO) in der jeweils geltenden Fassung, unmittelbar gilt.[23]

d) Verhältnis DS-GVO und DSAnpUG-EU:

Die Vorschriften des DSAnpUG-EU finden keine Anwendung, soweit die DS-GVO in der jeweils geltenden Fassung, unmittelbar gilt.[24] **Das bedeutet, dass alle Regelungen der DS-GVO zu beachten sind und Vorrang vor den Regelungen des DSAnpUG-EG haben.**

Das DSAnpUG-EU enthält Regelungen zur **Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO)** und Umsetzung der Richtlinie (EU) 2016/680. Für die Anpassung des Datenschutzrechts an die DS-GVO sind Teil 1 (gemeinsame Bestimmungen, §§ 1 bis 21) sowie Teil 2 (Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäß Art. 2 der DS-GVO, s.o. §§ 22 bis 44) und Teil 4 (Besondere Bestimmungen für Verarbeitungen i.R.v. nicht in die Anwendungsbereiche der DS-GVO und Richtlinie 2016/680 fallenden Tätigkeiten, § 85) des DSAnpUG-EU relevant.[25] Teil 3 gilt nur für die Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder der Strafvollstreckung sowie zu freien Datenverkehr.

[23] vgl. § 1 Abs. 5 DSAnpUG-EU.
[24] vgl. § 1 Abs. 5 DSAnpUG-EU.
[25] siehe DSAnpUG-EU.

1.2. Wo stehen die wesentlichen Begriffsbestimmungen in der DS-GVO und im DSAnpUG-EU?

Die wesentlichen Begriffsbestimmungen stehen in **Art. 4 DS-GVO** sowie in **§ 2 DSAnpUG-EU.**

1.3. Was ist unter „Verarbeitung“ von Daten zu verstehen und ist somit eine „Verarbeitungstätigkeit“?

„Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie:

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

- die **Vernichtung**.[26]

Die „Verarbeitung“ wird in der DS-GVO auch als **Verarbeitungstätigkeit** bezeichnet, so z.B. in § 30 DS-GVO (Erstellung eines Verzeichnisses über Verarbeitungstätigkeiten).[27]

Jede Verarbeitung personenbezogener Daten sollte **rechtmäßig** und nach **Treu und Glauben** erfolgen.[28] Für natürliche Personen soll die **Transparenz** dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden.[29]

1.4. Was ist unter einer Einwilligung zu verstehen? Wie kann eine Einwilligung erfolgen oder eingeholt werden? Welche Form kann die Einwilligung haben?

Eine Einwilligung ist jede

- **freiwillig**[30],
- **für den bestimmten Fall**,
- in **informierter Weise** und
- **unmissverständlich**

abgegebene **Willensbekundung** in Form einer **Erklärung** oder einer **sonstigen eindeutigen bestätigenden Handlung**, mit der die betroffene Person zu

[26] vgl. Art. 4 Nr. 2 DS-GVO.
[27] vgl. Art. 30 DS-GVO, EG 82 DS-GVO.
[28] EG 39 S. 1 DS-GVO.
[29] EG 39 S. 2 DS-GVO.
[30] vgl. hierzu auch EG 43 DS-GVO.

verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten **einverstanden** ist.[31]

Die Erklärung der Einwilligung sollte in **Abgrenzung von anderen Sachverhalten** eingeholt werden. Ist dies nicht möglich oder gewollt, muss das Ersuchen um Einwilligung in **verständlicher und leicht zugänglicher Form** und in einer **klaren und einfachen Sprache** erfolgen, so dass es von den anderen Sachverhalten klar zu unterscheiden ist.[32] Allerdings ist auch ohne einen zusätzlichen Sachverhalt anzuraten, die Einwilligung immer der o.g. Vorgehensweise einzuholen.

Die Einwilligung darf **keine missbräuchlichen Klauseln** enthalten.[33] Ist dies doch der Fall, sind diese nicht wirksam. [34]

Damit die betroffene Person in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.[35] Vor Abgabe der Einwilligung ist die betroffene Person darauf hinzuweisen, dass ihr das Recht zusteht, **jederzeit** ihre **Einwilligung zu widerrufen**.[36] Dabei ist darauf hinzuweisen, dass die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung nicht berührt wird.[37] **Der Widerruf muss so einfach wie die Erteilung der Einwilligung sein**.[38]

[31] Art. 4 Nr. 11 DS-GVO sowie EG 32 DS-GVO. Ausnahmsweise kann im Bereich der Forschung eine Einwilligung auch für bestimmte Bereiche wissenschaftlicher Forschung zulässig sein, vgl. EG 33 DS-GVO.
[32] Art. 7 Abs. 2 S. 1 DS-GVO. Vgl. hierzu auch EG 42 S. 3 DS-GVO.
[33] vgl. EG 42 S. 3 a.E. DS-GVO.
[34] vgl. Art. 7 Abs. 2 S. 2 DS-GVO.
[35] vgl. EG 42 S. 4 DS-GVO.
[36] vgl. Art. 7 Abs. 3 S. 1 i.V.m. S. 3 DS-GVO.
[37] vgl. Art. 7 Abs. 3 S. 2 i.V.m. S. 3 DS-GVO.
[38] Art. 7 Abs. 3 S. 4 DS-GVO.

Die Einwilligung ist nur wirksam, wenn sie auf der **freiwilligen Entscheidung** der betroffenen Person beruht. Bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, müssen die **Umstände der Erteilung** berücksichtigt werden.[39] Dabei ist dem Umstand in größtmöglichem Umfang Rechnung zu tragen, ob u.a. die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist.[40] Dabei kann die betroffene Person auch darauf hingewiesen werden, dass bei Nichterteilung der Einwilligung unter Umständen eine Vertragserfüllung (z.B. wegen fehlender Kontodaten) nicht möglich ist. Wichtig ist, dass kein Druck auf die betroffene Person ausgeübt wird.

Sollen **besondere Kategorien personenbezogener Daten**[41] (vgl. Ziff. 1.6 FAQ) verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten (z.B. Gesundheitsdaten) beziehen.

Der **Verantwortliche** (vgl. Ziff. 1.7 FAQ) muss **nachweisen** können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.[42]

Folgende **Formen** der Einwilligung sind grundsätzlich möglich:

- **Schriftliche** Erklärung,
- **Elektronische** Erklärung,
- **Mündliche** Erklärung.[43]

[39] vgl. Art. 7 Abs. 4 EG DS-GVO.
[40] Art. 7 Abs. 4 DS-GVO. Siehe hierzu auch EG 43 DS-GVO.
[41] siehe Definitionen in Art. 9 Abs. 1 DS-GVO.
[42] Art. 7 Abs. 1 DS-GVO. Siehe hierzu auch EG 42 S. 1 DS-GVO,
[43] EG 32 S. 1 DS-GVO.

Eine **elektronische Einwilligung** kann etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite erfolgen oder durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft sowie durch eine andere Erklärung oder Verhaltensweise, mit der die betroffene Person in dem jeweiligen Kontext **eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung** ihrer personenbezogenen Daten signalisiert.[44] Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen.[45] Letztlich entspricht diesen Voraussetzungen nur das **Double-Opt-In-Verfahren**. Hierbei folgt nach dem ersten **Opt-In** (d.h. eine Einwilligungserklärung durch Ankreuzen oder einer gesonderten Unterschrift) bspw. eine kurze E-Mail mit der Bitte, die Einwilligung per Klick auf einen Bestätigungslink endgültig zu bestätigen. Erst wenn dieser Link geklickt wurde, ist der Double-Opt-In abgeschlossen. Ebenso muss eine einfache Möglichkeit zum Widerruf der Einwilligung geschaffen werden (**Opt-Out**), z.B. direkt in einer Newsletter-E-Mail. Der betroffenen Person muss es ohne Aufwand möglich sein, die Einwilligung zu widerrufen.

Von der Einholung einer mündlichen Einwilligung ist abzuraten, da ein entsprechender Nachweis nur schwer einzuholen sein wird.

Wurde eine Einwilligung gemäß der Richtlinie 95/46/EG eingeholt, ist nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung hierzu erteilt, sofern die Art der bereits erteilten Einwilligung den Bedingungen der DS-GVO entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der DS-GVO fortsetzen kann.[46]

[44] vgl. EG 32 S. 2 DS-GVO.
[45] EG 32 S. 3 DS-GVO.
[46] vgl. EG 171 S. 2 DS-GVO.

1.5. Welche Daten sind gemäß der DS-GVO personenbezogene Daten?

„**Personenbezogene Daten**“ sind alle Informationen, über die natürliche Personen **identifiziert** oder durch Zuordnung weiterer Informationen identifiziert werden (Identifizierbarkeit) können.[47] Als **identifizierbar** wird eine natürliche Person angesehen, die **direkt oder indirekt**, insbesondere mittels **Zuordnung zu einer Kennung** (z.B. Name, Kennnummer, Standortdaten, Online-Kennung oder ein oder mehrere besondere Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind) identifiziert werden kann.[48] Grundsätzlich könnte jede Kennung, z.B. auch Steuernummern oder Autokennzeichen, von der Aufsichtsbehörde als datenschutzrelevant erachtet werden. Dies betrifft beispielsweise auch Geschäftskontakte, über deren Namen eine Person und dessen Funktion in einem Unternehmen identifiziert werden kann; lediglich bei Namens- und Adressdaten eines Unternehmens handelt es sich nicht um personenbezogene Daten.

Natürlichen Personen werden unter Umständen **Online-Kennungen** wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet.[49] Dies kann Spuren hinterlassen, die insbesondere in **Kombination** mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.[50] Daher müssen auch Verarbeitungen, die lediglich mit **Pseudonymen** oder **Kennungen**

[47] vgl. Art. 4 Nr. 1, 1.Hs. DS-GVO, siehe hierzu auch EG 26 S. 1 DS-GVO.
[48] vgl. Art. 4 Abs. 1 Nr. 1, 2. Hs. DS-GVO.
[49] EG 30 S. 1 DS-GVO.
[50] EG 30 S. 2 DS-GVO.

arbeiten, unter datenschutzrechtlichen Gesichtspunkten betrachtet und in das Verarbeitungsverzeichnis aufgenommen werden.[51]

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten **alle Mittel** berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person **nach allgemeinem Ermessen** wahrscheinlich genutzt werden, um die natürliche Person zu identifizieren.[52] Um festzustellen, ob ein Verantwortlicher oder ein Dritter Mittel nach allgemeinem Ermessen zur Identifizierung von natürlichen Personen einsetzt, sollten **alle objektive Faktoren** wie **Kosten der Identifizierung** und der dafür erforderliche **Zeitaufwand** herangezogen werden.[53] Dabei sind die zum Zeitpunkt der Verarbeitung verfügbaren Technologien und die technologischen Entwicklungen zu berücksichtigen.[54]

1.6. Welche besonderen Kategorien personenbezogener Daten gibt es und was gilt für sie?

Es gibt die folgenden **besonderen Kategorien personenbezogener Daten:**

- **Daten rassischer und ethnischer Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit,**
- genetische Daten,
- biometrische Daten zur eindeutigen Identifikation einer natürlichen Person,
- **Gesundheitsdaten,**

[51] vgl. EG 26 S. 2 DS-GVO.
[52] EG 26 S. 3 DS-GVO.
[53] vgl. EG 26 S. 4, 1. Hs. DS-GVO.
[54] vgl. EG 26 S. 4, 2. Hs. DS-GVO.

- Daten zum Sexualleben oder zur sexuellen Orientierung.[55]

Gegenüber dem „alten“ Bundesdatenschutzgesetz (BDSG) wurden demnach genetische und biometrische Daten ergänzt.

Die o.g. personenbezogenen Daten dürfen **grundsätzlich nicht verarbeitet** werden.[56] Art. 9 Abs. 2 a) bis j) und Abs. 3 DS-GVO bestimmen engen Voraussetzungen, unter denen derartige Daten ausnahmsweise erhoben werden dürfen.[57] Ebenso regelt § 22 DSAnpUG-EU unter welchen Voraussetzungen ergänzend zu Art. 9 Abs. 1 DS-GVO besondere Kategorien personenbezogener Daten verarbeitet werden dürfen.[58]

1.7. Wer ist „Verantwortlicher“ im Sinne der DS-GVO? Können mehrere „gemeinsam Verantwortlicher“ sein? Was setzt dies voraus?

„**Verantwortlicher**“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[59]

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der oder die Mittel zur Verarbeitung fest, so sind sie **gemeinsam Verantwortliche**[60] (vgl. Ziff. 4.6 FAQ). Hier ist eine **Vereinbarung zwischen den Verantwortlichen** erforderlich, in welcher sie in **transparenter** Form festlegen, wer **von ihnen welche datenschutzrechtliche Verpflichtung** erfüllt, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind.[61] Aus der Vereinbarung muss

[55] vgl. Art. 9 Abs. 1 DS-GVO.
[56] vgl. Art. 9 Abs. 1 DS-GVO
[57] siehe hierzu Art. 9 Abs. 2 und 3 DS-GVO.
[58] siehe hierzu § 22 DSAnpUG-EU.
[59] vgl. Art. 4 Nr. 7 DS-GVO.
[60] Art. 26 Abs. 1 S. 1 DS-GVO.
[61] vgl. Art. 26 Abs. 1 S. 1 DS-GVO, siehe hierzu auch EG 79 DS-GVO (klare Zuteilung der Verantwortlichkeiten).

insbesondere hervorgehen, wer welchen **Informationspflichten** gemäß Art. 13 und 14 DS-GVO nachzukommen hat und **wie und gegenüber wem** betroffene Personen ihre Rechte wahrnehmen können.[62] Ungeachtet dieser Vereinbarung kann die betroffene Person ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend machen.[63]

1.8. Wofür trägt der Verantwortliche die Verantwortung?

Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wurde[64] (siehe auch Ziff. 1.13, 1.14 FAQ). Dem Verantwortlichen obliegt die Verantwortung und Haftung jedweder Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt.[65]

Der Verantwortliche hat **geeignete technische und organisatorische Maßnahmen**, auch als „TOMs" bezeichnet, zum Schutz für die Rechte und Freiheiten bei der Verarbeitung von Daten natürlicher Personen zu treffen und umzusetzen (vgl. Ziff. 1.9 FAQ).[66]

Der Verantwortliche ist verpflichtet, die in **Art. 5 DS-GVO** festgelegten **Grundsätze** für die Verarbeitung personenbezogener Daten (vgl. Ziff. 1.11 FAQ) einzuhalten.[67]

Darüber hinaus obliegen dem Verantwortlichen vielfältige weitere **Dokumentations- und Nachweispflichten** (vgl. Ziff. 1.12 FAQ).

Der Verantwortliche ist verpflichtet, unter den Voraussetzungen des § 37 DS-GVO oder §§ 5 ff., 38 DSAnpUG-EU genannten Voraussetzungen einen

[62] vgl. Art. 26 Abs. 1 S. 2 DS-GVO.
[63] vgl. Art. 26 Abs. 3 DS-GVO.
[64] Art. 82 Abs. 2 DS-GVO.
[65] vgl. EG 74 S. 1 DS-GVO.
[66] vgl. Art. 24 Abs. 1 S. 1 DS-GVO, siehe hierzu auch EG 74 S. 2 und 3 DS-GVO sowie EG 75 bis 78 DS-GVO.
[67] siehe Art. 5 DS-GVO.

Datenschutzbeauftragten (vgl. Ziff. 2.3 und 2.4 FAQ) für die Behörde, öffentliche Stelle, das Unternehmen oder eine Unternehmensgruppe zu benennen.[68]

1.9. Welche Anforderungen werden an technische und organisatorische Maßnahmen sowie an die Sicherheit der Datenverarbeitung gestellt?

Bisher wurden technische und organisatorische Maßnahmen in § 9 und in der Anlage zu § 9 Satz 1 BDSG beschrieben. Zukünftig geltende Regelungen zu **geeigneten technischen und organisatorischen Maßnahmen** befinden sich in

- **Art. 24** (Verantwortung des für die Verarbeitung Verantwortlichen),
- **Art. 25** (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Einstellungen) **und**
- **Art. 32 DS-GVO** (Sicherheit der Verarbeitung).

Die unterschiedlichen Kontrollarten (Zutrittskontrolle etc.), wie sie in der Anlage zu § 9 S. 1 BDSG er-wähnt werden, gibt es nicht mehr.

Bei der **Auswahl geeigneter technischer und organisatorischer Maßnahmen** hat der Verantwortliche Folgendes zu berücksichtigen:

- den **Stand der Technik**,
- die **Implementierungskosten**,
- die **Art**, der **Umfang**, die **Umstände** und der **Zweck der Verarbeitung** sowie die unterschiedliche **Eintrittswahrscheinlichkeit** und

[68] vgl. Art. 37 Abs. 1 DS-GVO, siehe auch EG 97 S. 1 DS-GVO, wonach in Fällen, in denen die Verarbeitung durch eine Behörde (mit Ausnahme von Gerichten oder unabhängigen Justizbehörden) im privaten Sektor durch einen Verantwortlichen erfolgt, dessen Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern (…) sollte der Verantwortliche oder der Auftragsverarbeiter von einer weiteren Person, die Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden.

- die **Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen.[69]

Dabei sollen die erforderlichen technischen und organisatorischen Maßnahmen zu Folgendem führen:

- **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten[70],
- **dauerhafte Sicherstellung** der Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung[71],
- Fähigkeit zur **raschen Wiederherstellung** der Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall[72],
- Gewährleistung der Sicherheit der Verarbeitung durch ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen[73].

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die **Risiken** zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch (unbeabsichtigte oder unrechtmäßige) Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf anderer Weise verarbeitet wurden.[74]

Die Auswahl geeigneter technischer und organisatorischer Maßnahmen kann auch durch Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) oder

[69] vgl. Art. 32 Abs. 1 DS-GVO.
[70] vgl. Art. 32 Abs. 1 a) DS-GVO.
[71] vgl. Art. 32 Abs. 1 b) DS-GVO.
[72] vgl. Art. 32 Abs. 1 c) DS-GVO.
[73] Art. 32 Abs. 1 d) DS-GVO.
[74] Art. 32 Abs. 2 DS-GVO.

ein genehmigtes Zertifizierungsverfahren (Art. 42 DS-GVO) nachgewiesen werden.[75]

Der Verantwortliche und der Auftraggeber müssen sicherstellen, dass ihnen **unterstellte natürliche Personen**, die Zugang zu personenbezogenen Daten haben, diese nur auf **Anweisung** des Verantwortlichen verarbeiten.[76] Dies kann z.B. durch Verhaltensregeln oder Dienstanweisungen geschehen.

Dem Verantwortlichen obliegt darüber hinaus die **Umsetzung** der getroffenen **geeigneten technischen und organisatorischen Maßnahmen** unter Berücksichtigung von

- der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** sowie
- der unterschiedlichen **Eintrittswahrscheinlichkeit** und
- der **Schwere der Risiken** für die Rechte und Freiheiten natürlicher Personen,

um **sicherzustellen** und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß datenschutzrechtlichen Anforderungen, insbesondere der DS-GVO entsprechen.[77] Diese Maßnahmen müssen die **Anwendung geeigneter Datenschutzvorkehrungen** durch den Verantwortlichen erfassen, sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht.[78]

Die Einhaltung der genehmigten Verhaltensregeln gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 kann als Gesichtspunkt

[75] vgl. Art. 32 Abs. 3 DS-GVO.
[76] Art. 32 Abs. 4 DS-GVO.
[77] Art. 24 Abs. 1 S. 1 DS-GVO, siehe hierzu auch EG 74 S. 2 und 3 DS-GVO sowie EG 75 bis 78 DS-GVO.
[78] vgl. Art. 24 Abs. 2 DS-GVO.

herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.[79]

Weiterhin trifft den Verantwortlichen eine ähnliche Verpflichtung bereits bei der **Technikgestaltung** („data protection by design“[80]), d.h. zum **Zeitpunkt der Festlegung von Mitteln** für die Verarbeitung sowie **zum Zeitpunkt der eigentlichen Verarbeitung**. [81] Hier sind **geeignete technische und organisatorische Maßnahmen** nach folgenden Aspekten zu treffen:

- **Stand der Technik**,
- **Implementierungskosten**,
- **Art**, **Umfang**, **Umstände** und **Zweck der Verarbeitung** sowie
- die unterschiedliche **Eintrittswahrscheinlichkeit** und
- **Schwere** der mit der Verarbeitung verbundenen **Risiken** für die Rechte und Freiheiten natürlicher Personen.[82]

Hierzu gehört bspw. die **Pseudonymisierung**.[83] Die Maßnahmen sollen darauf ausgelegt sein, die Datenschutzgrundsätze wie Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen.[84] Letztlich soll der Verantwortliche Produkte auswählen und Lösungen entwickeln, die von vornherein den Schutz von personenbezogenen Daten sicherstellen.

Zudem hat der Verantwortliche **geeignete technische und organisatorische Maßnahmen** zu treffen, die sicherstellen, dass **Voreinstellungen** („data

[79] Art. 24 Abs. 3 DS-GVO.
[80] vgl. EG 78 S. 2 DS-GVO.
[81] vgl. Art. 25 Abs. 1 DS-GVO.
[82] vgl. Art. 25 Abs. 2 DS-GVO.
[83] vgl. Art. 25 Abs. 1 DS-GVO.
[84] vgl. Art. 25 Abs. 1 DS-GVO.

protection by default“[85]) grundsätzlich nur personenbezogenen Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.[86] Diese Verpflichtung gilt für

- die **Menge** der erhobenen personenbezogenen Daten,
- den **Umfang** ihrer Verarbeitung
- ihre **Speicherfrist** und
- ihre **Zugänglichkeit**.[87]

Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.[88] Voreinstellungen sind demnach so wählen, dass die Verarbeitung personenbezogener Daten **minimiert** wird. Der Nutzer soll entscheiden können, ob er diese Voreinstellungen ändert.

Um diese Anforderungen nachzuweisen kann ein genehmigtes Zertifizierungsverfahren nach Art. 42 DS-GVO als Faktor herangezogen werden.[89]

1.10. Auftragsverarbeitung: Was ist bei der Verarbeitung von Daten auf Weisung des Verantwortlichen zu beachten?

Bei Auftragsverarbeitungen wurden vorwiegend sprachliche Änderungen vorgenommen. Die DS-GVO spricht nunmehr von „für die Verarbeitung Verantwortlichem“ und dessen „Auftragsverarbeiter“ (vgl. Ziff. 4 FAQ).[90]

Vereinbarungen über Auftragsverarbeitungen (Vertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der

[85] vgl. EG 78 S. 2 DS-GVO.
[86] vgl. Art. 25 Abs. 2 S. 1 DS-GVO.
[87] vgl. Art. 25 Abs. 2 S. 2 DS-GVO.
[88] Art. 25 Abs. 2 S. 3 DS-GVO.
[89] vgl. Art. 25 Abs. 3 DS-GVO.
[90] vgl. u.a. Art. 28 f. DS-GVO.

Mitgliedstaaten[91]) sind **schriftlich** abzuschließen; dies kann auch in einem **elektronischen Format** erfolgen.[92] **Ein zwingendes Schriftformerfordernis (Papierformat) existiert nicht mehr.**

Die Auftragsverarbeiter sind **sorgfältig** und unter **Berücksichtigung der technischen und organisatorischen Maßnahmen** auszuwählen, so dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet.[93]

Neu zu den Anforderungen an eine Vereinbarung zur Auftragsverarbeitung hinzugekommen ist unter anderem die Pflicht zum Führen eines **Verzeichnisses über die Verarbeitungstätigkeiten**.[94] Zum Nachweis der Einhaltung der DS-GVO sollte der Auftragsdatenverarbeiter demnach ein Verzeichnis der Verarbeitungstätigkeiten führen, die seiner Zuständigkeit unterliegen (vgl. Ziff. 4.6 FAQ).[95]

Auch zukünftig wird der für die Verarbeitung **Verantwortliche** und nicht der Auftragsverarbeiter erster Ansprechpartner für Betroffene und für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich sein.[96] Der Verantwortliche kann sich aber exkulpieren. Missachtet ein Auftragsverarbeiter, welcher nur auf Weisung des Verantwortlichen tätig werden darf[97], Weisungen des Verantwortlichen, haftet der Auftragsverarbeiter und nicht der Verantwortliche.[98] Erfüllt ein weiterer, vom Auftragsverarbeiter hinzugezogener Auftragsverarbeiter seine Pflichten nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem

[91] vgl. Art. 28 Abs. 3 S. 1 DS-GVO, siehe auch EG 81 S. 3 DS-GVO.
[92] vgl. Art. 28 Abs. 9 DS-GVODS-GVO.
[93] vgl. Art. 28 Abs. 1 DS-GVO.
[94] vgl. Art. 30 Abs. 2 DS-GVO.
[95] EG 82 S. 1 DS-GVO, siehe zum Verarbeitungsverzeichnis Art. 30 DS-GVO.
[96] vgl. Art. 82 Abs. 2 S. 1 DS-GVO, siehe hierzu auch EG 146DS-GVO.
[97] vgl. Art. 29 DS-GVO.
[98] vgl. Art. 28 Abs. . 10, siehe auch Art. 82 Abs. 2 S. 2 DS-GVO.

Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.[99]

Der Auftragsverarbeiter wird jedoch von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.[100] Eine Exkulpation ist demnach sowohl auf Seiten des für die Verarbeitung Verantwortlichen als auch auf Seiten des Auftragsverarbeiters möglich.[101] Siehe hierzu auch Ziff. 1.13, 1.14 und 4.8 FAQ.

1.11. Rechenschaftspflicht. Was sind die Grundsätze für die Verarbeitung von personenbezogenen Daten?

Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden **(„Rechtmäßigkeit, Treu und Glauben, Transparenz“),**[102]
- grundsätzlich für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden **(„Zweckbindung“),**[103]
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein **(„Datenminimierung“),**[104]
- 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

[99] vgl. Art. 28 Abs. 4 S. 2 DS-GVO.
[100] vgl. Art. 82 Abs. 3 DS-GVO, siehe hierzu auch EG 146 S. 2 DS-GVO.
[101] vgl. Art. 28 Abs. 3 S. 2 a) i.V.m. Abs. 4 S. 1 und 2, Art. 82 Abs. 3 DS-GVO.
[102] Art. 5 Abs. 1 a) DS-GVO, siehe auch EG 39 S. 1 DS-GVO.
[103] vgl. Art. 5 Abs. 1 b) DS-GVO.
[104] vgl. Art. 5 Abs. 1 c) DS-GVO, siehe auch EG 39 S. 6 DS-GVO.

Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden **(„Richtigkeit“),**[105]

- grundsätzlich 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 **(„Speicherbegrenzung“),**[106]
- 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 Maßnahmen **(„Integrität und Vertraulichkeit“).**[107]

Der Verantwortliche ist für die Einhaltung der o.g. Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können („**Rechenschaftspflicht**“).[108]

1.12. Welche Dokumentations- und Nachweispflichten hat der Verantwortliche?

a) Bedingungen für die Einwilligung

Beruht die Verarbeitung der personenbezogenen Daten auf einer Einwilligung, muss der Verantwortliche **nachweisen** können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten **eingewilligt** hat (vgl. Ziff. 1.4 FAQ).[109]

2. Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

[105] vgl. Art. 5 Abs. 1 d) DS-GVO, siehe auch EG 39 S. 10 DS-GVO
[106] vgl. Art. 5 Abs. 1 e) DS-GVO, siehe auch EG 39 S. 7 DS-GVO.
[107] Art. 5 Abs. 1 f) DS-GVO, siehe auch EG 39 S. 11 DS-GVO.
[108] vgl. Art. 5 Abs. 2 DS-GVO.
[109] vgl. Art. 7 Abs. 1 DS-GVO, siehe auch EG 32, 33, 42, 43 DS-GVO.

Liegt eine Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft vor, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das **16. Lebensjahr vollendet** hat.[110] Hat das Kind das 16. Lebensjahr noch nicht vollendet, so ist die Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.[111] Durch Rechtsvorschriften können die Mitgliedstaaten niedrigere Altersgrenzen festlegen; diese dürften jedoch nicht unter dem vollendeten 13. Lebensjahr liegen.[112]

Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich bei Kindern, die noch nicht das erforderliche Alter erreicht haben, zu **vergewissern**, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.[113]

3. Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person

- alle **Informationen** gemäß den **Art. 13 DS-GVO** (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person) und **14 DS-GVO** (Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden) und
- alle Mitteilungen gemäß **Art. 15 bis 22 DS-GVO** (Auskunftsrecht der betroffenen Person, Recht auf Berichtigung und Löschung, Widerspruchsrecht und automatisierte Entscheidungsfindung) und **Art.**

[110] vgl. Art. 8 Abs. 1 S. 1 DS-GVO.
[111] vgl. Art. 8 Abs. 1 S. 2 DS-GVO.
[112] vgl. Art. 8 Abs. 1 S. 3 DS-GVO.
[113] vgl. Art. 8 Abs. 2 DS-GVO.

34 DS-GVO (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person),

die sich auf die Verarbeitung beziehen, in **präziser**, **transparenter**, **verständlicher** und **leicht zugänglicher Form** in einer **klaren und einfachen Sprache** zu übermitteln.[114] Dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.[115]

Zu weiteren Einzelheiten siehe Art. 12 Abs. 2 bis 8 DS-GVO.

Grundsätzlich hat der Verantwortliche dem Betroffenen die Informationen gemäß Art. 13 und 14 DS-GVO (s.o.) sowie alle Mitteilungen und Maßnahmen gemäß den Art. 15 bis 22 und Art. 34 DS-GVO (s.o.) **unentgeltlich** zur Verfügung zu stellen.[116] Der Verantwortliche kann, bei **offenkundig unbegründeten** oder – insbesondere im Fall von häufiger Wiederholung – **exzessiven Anträgen** einer betroffenen Person jedoch

- entweder ein **angemessenes Entgelt** verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden[117], oder
- sich **weigern**, aufgrund des Antrags tätig zu werden.[118]

Den **Nachweis** für den offenkundig **unbegründeten** oder exzessiven **Charakter** des Antrags hat der **Verantwortliche** zu erbringen.[119]

[114] vgl. Art. 12 Abs. 1 S. 1 DS-GVO, siehe hierzu auch EG 58 S. 1 DS-GVO.
[115] vgl. Art. 12 Abs. 1 S. 1 DS-GVO, siehe hierzu auch EG 58 S. 1 DS-GVO.
[116] vgl. Art. 12 Abs. 5 S. 1 DS-GVO, siehe hierzu auch EG 59 S. 1 DS-GVO.
[117] vgl. Art. 12 Abs. 5 S. 2 a) DS-GVO.
[118] vgl. Art. 12 Abs. 5 S. 2 b) DS-GVO.
[119] Art. 8 Abs. 5 S. 3 DS-GVO.

4. Informations- und Dokumentationspflichten

Zu näheren Einzelheiten zu den Informations- und Dokumentationspflichten (Art. 13, 14 DS-GVO) verweisen wir hier auf Ziff. 3.2 ff. FAQ.

5. Widerspruchsrecht

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, **jederzeit** gegen die Verarbeitung sie betreffender personenbezogenen Daten **Widerspruch** einzulegen.[120] Der **Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr**, es sei denn, er kann zwingende **schutzwürdige Gründe** für die Verarbeitung **nachweisen**, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.[121]

6. Verantwortung des für die Verarbeitung Verantwortlichen

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen** um, um sicherzustellen und den **Nachweis dafür erbringen** zu können, dass **die Verarbeitung gemäß der DS-GVO** erfolgt, insbesondere auch im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten (vgl. Ziff. 1.6 und 1.9 FAQ).[122]

Die Einhaltung der genehmigten Verhaltensregeln gemäß Art. 40 DS-GVO oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DS-GVO kann als

[120] Art. 21 Abs. 1 S. 1, 1. Hs. DS-GVO, siehe hierzu auch EG 69 und 70 DS-GVO.
[121] Art. 21 Abs. 1 S. 2 DS-GVO.
[122] vgl. Art. 24 Abs. 1 DS-GVO, siehe hierzu auch EG 78 DS-GVO.

Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.[123]

7. Gemeinsam für die Verarbeitung Verantwortliche

Legen zwei oder mehr Verantwortliche **gemeinsam die Zwecke der und die Mittel zur Verarbeitung** fest, so sind sie **gemeinsam Verantwortliche**.[124] Sie legen in einer **Vereinbarung** in **transparenter Form** fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt.[125] Siehe hierzu auch Ziff. 4.6 FAQ.

8. Auftragsverarbeiter

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der **Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten**, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind (vgl. Ziff. 1.10 und Ziff. 4.4 FAQ).[126] Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DS-GVO kann als Faktor für hinreichende Garantien der auftragsgerechten Verarbeitung herangezogen werden, um hinreichende Garantien i.S.d. Abs. 1 bis 4 des Art. 24 DS-GVO nachzuweisen.[127]

[123] Art. 24 Abs. 3 DS-GVO.
[124] Art. 26 Abs. 1 S. 1 DS-GVO, siehe hierzu auch EG 79 DS-GVO.
[125] Art. 26 Abs. 1 S. 2 DS-GVO.
[126] Art. 28 Abs. 3 S. 1 DS-GVO, siehe hierzu auch EG 81 S. 3 DS-GVO.
[127] Art. 28 Abs. 5 DS-GVO.

9. Verzeichnis von Verarbeitungstätigkeiten

Jeder **Verantwortliche** und ggf. sein Vertreter führen ein **Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen.[128] Diese Verzeichnisse sind **schriftlich** zu führen, was auch in einem **elektronischen Format** erfolgen kann.[129] Der Verantwortliche sowie ggf. deren Vertreter stellen der **Aufsichtsbehörde** das Verzeichnis **auf Anfrage** zur Verfügung. [130]

10. Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche (und der Auftragsverarbeiter) **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.[131] Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DS-GVO kann als Faktor herangezogen werden, um die Erfüllung der genannten Anforderungen nachzuweisen.[132]

11. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche **unverzüglich** und **möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Art. 51 DS-GVO zuständigen **Aufsichtsbehörde** bzw. dem Bundesbeauftragten, es sei denn, dass die Ver-

[128] Art. 30 Abs. 1 DS-GVO.
[129] Art. 30 Abs. 3 DS-GVO, siehe auch EG 82 S. 1 DS-GVO.
[130] Art. 30 Abs. 4 DS-GVO.
[131] vgl. Art. 32 S. 1 1. Hs. DS-GVO, siehe hierzu auch EG 83 DS-GVO.
[132] Art. 32 Abs. 3 DS-GVO.

letzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.[133] Erfolgt die Meldung an die Aufsichtsbehörde bzw. der oder den Bundesbeauftragen **nicht innerhalb von 72 Stunden**, so ist die **Verzögerung zu begründen**.[134] Zu den unternehmensinternen Prozessen siehe auch Ziff. 2.1 lit. c FAQ).

Der Verantwortliche **dokumentiert Verletzungen** des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden **Fakten**, von deren **Auswirkungen** und der **ergriffenen Abhilfemaßnahmen**.[135] Diese Dokumentation muss der **Aufsichtsbehörde** die Überprüfung der einzelnen Bestimmungen des Art. 33 DS-GVO ermöglichen.[136]

§ 34 Abs. 3 DS-GVO sieht Ausnahmen von der Benachrichtigungspflicht vor. Die Pflicht zur Benachrichtigung gemäß Art. 34 DS-GVO besteht ergänzend zu den in Art. 34 Abs. 3 DS-GVO genannten **Ausnahmen nicht**, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der **überwiegenden berechtigten Interessen eines Dritten**, geheim gehalten werden müssen.[137] Abweichend von der Ausnahme nach § 29 Abs. 1 S. 3 DSAnpUG-EU ist die betroffene Person nach Art. 34 DS-GVO zu **benachrichtigen**, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.[138]

12. Datenschutz-Folgenabschätzung und vorherige Konsultation

[133] Art. 33 Abs. 1 S. 1 DS-GVO, siehe hierzu auch EG 85 S. 2 DS-GVO.
[134] vgl. Art. 33 Abs. 1 S. 2 DS-GVO.
[135] Art. 33 Abs. 5 S. 1 DS-GVO, siehe hierzu auch EG 87 S. 1 DS-GVO.
[136] Art. 33 Abs. 5 S. 2 DS-GVO, siehe hierzu auch EG 88 DS-GVO.
[137] vgl. § 29 Abs. 1 S. 3 DSAnpUG-EU.
[138] vgl. § 29 Abs. 1 S. 4 DSAnpUG-EU.

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge, so führt der Verantwortliche **vorab** eine **Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.[139] Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.[140]

Bei der Durchführung der Datenschutz-Folgenabschätzung ist der **Datenschutzbeauftragte** hinzuzuziehen, sofern einer benannt wurde.[141]

Eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 3 DS-GVO ist insbesondere in folgenden Fällen erforderlich:

- bei der **systematischen und umfassenden Bewertung persönlicher Aspekte** natürlicher Personen, die sich auf **automatisierte Verarbeitung** einschließlich **Profiling** gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen[142],
- bei der **umfangreichen Verarbeitung besonderer Kategorien** von personenbezogenen Daten gemäß Art. 9 Abs. 1 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO[143] oder

[139] vgl. Art. 35 Abs. 1 S. 1 DS-GVO, siehe auch EG 84 sowie EG 89 bis 95 DS-GVO.
[140] vgl. Art. 35 Abs. 1 S. 2 DS-GVO
[141] vgl. Art. 35 Abs. 2 DS-GVO.
[142] vgl. Art. 35 Abs. 3 a) DS-GVO.
[143] vgl. Art. 35 Abs. 3 b) DS-GVO.

- bei der **systematischen Überwachung öffentlich zugänglicher Bereiche**[144]**.**

Die **Aufsichtsbehörde** erstellt eine **Liste** der Verarbeitungsvorgänge, für die nach den obigen Voraussetzungen eine Datenschutz-Folgenabschätzung erforderlich ist.[145]

Die Datenschutz-Folgenabschätzung muss Folgendes enthalten:

- eine **systematische Beschreibung** der geplanten **Verarbeitungsvorgänge** und der **Zwecke** der Verarbeitung, ggf. einschließlich der von dem Verantwortlichen verfolgten **berechtigten Interessen**[146]
- eine **Bewertung** der **Notwendigkeit** und **Verhältnismäßigkeit** der Verarbeitungsvorgänge in Bezug auf den Zweck[147]
- eine **Bewertung** der **Risiken** für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 (Voraussetzungen Datenschutz-Folgenabschätzung)[148]
- die zur Bewältigung der Risiken **geplanten Abhilfemaßnahmen**, einschließlich **Garantien**, **Sicherheitsvorkehrungen** und **Verfahren**, durch die der Schutz personenbezogener Daten **sichergestellt** und der **Nachweis** dafür erbracht wird, dass die DS-GVO eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird[149]

Der Verantwortliche hat ggf. den **Standpunkt der betroffenen Personen** oder ihrer Vertreter zu der beabsichtigten Verarbeitung einzuholen, unbeschadet

[144] vgl. Art. 35 Abs. 3 c) DS-GVO
[145] vgl. Art. 35 Abs. 4 S. 1 DS-GVO.
[146] vgl. Art. 35 Abs. 7 a) DS-GVO.
[147] vgl. Art. 35 Abs. 7 b) DS-GVO
[148] vgl. Art. 35 Abs. 7 c) DS-GVO
[149] vgl. Art. 35 Abs. 7 d) DS-GVO.

des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge.[150]

Der Verantwortliche führt, sofern erforderlich, eine **Überprüfung** durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird. Die gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.[151]

13. Datenübermittlung an Drittstaaten vorbehaltlich geeigneter Garantien

Falls kein Beschluss für eine Datenübermittlung an Stellen in Drittstaaten auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 Abs. 3 DS-GVO, Art. 36 Abs. 3 DS-GVO) vorliegt, darf ein Verantwortlicher oder ein Auftragsdatenverarbeiter personenbezogene Daten an ein Drittland oder einer internationalen Organisation nur übermitteln, sofern der Verantwortliche oder Auftragsdatenverarbeiter **geeignete Garantien** vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.[152]

Diese können, **ohne** dass hierzu eine **besondere Genehmigung** einer Aufsichtsbehörde erforderlich wäre, bestehen in

- einem **rechtlich bindenden und durchsetzbaren Dokument** zwischen den Behörden oder öffentlichen Stellen,[153]
- verbindlichen **internen Datenschutzvorschriften** gemäß Art. 47 DS-GVO,[154]

[150] vgl. Art. 35 Abs. 9 DS-GVO.
[151] vgl. Art. 35 Abs. 11 DS-GVO
[152] vgl. Art. 46 Abs. 1 DS-GVO, siehe auch EG 108, 109 DS-GVO.
[153] vgl. Art. 46 Abs. 2 a) DS-GVO.
[154] vgl. Art. 46 Abs. 2 b) DS-GVO

- **Standarddatenschutzklauseln**, die von der Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 DS-GVO erlassen werden,[155]
- von einer Aufsichtsbehörde angenommenen **Standardschutzklauseln**, die von der Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 DS-GVO **genehmigt** wurden,[156]
- **genehmigten Verhaltensregeln** gemäß Art. 40 DS-GVO oder einem **genehmigten Zertifizierungsverfahren** gemäß Art. 42 DS-GVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder Auftragsdatenverarbeiters in dem Drittland zur Anwendung geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.[157]

Ist eine **Genehmigung** erforderlich, können geeignete Garantien auch bestehen in:

- **Vertragsklauseln**, die zwischen dem Verantwortlichem oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger personenbezogener Daten im Drittland oder der internationalen Organisation vereinbart wurden,[158]
- Bestimmungen, die in **Verwaltungsvereinbarungen** zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die Betroffenen einschließen.[159]

[155] vgl. Art. 46 Abs. 2 c) DS-GVO
[156] vgl. Art. 46 Abs. 2 d) DS-GVO
[157] vgl. Art. 46 Abs. 2 e) und f) DS-GVO.
[158] vgl. Art. 46 Abs. 3 a) DS-GVO
[159] vgl. Art. 46 Abs. b) DS-GVO.

1.13. Wann haftet der Verantwortliche?

Jeder an einer Verarbeitung beteiligte Verantwortliche haftet grundsätzlich für den Schaden, der durch eine nicht der DS-GVO, oder anderen auf ihre Verarbeitung anwendbaren Vorschriften entsprechende Verarbeitung verursacht wurde.[160]

Ein Auftragsverarbeiter, der unter Verstoß gegen die DS-GVO die Zwecke und Mittel der Verarbeitung bestimmt, wird in Bezug auf diese Verarbeitung **selbst zum Verantwortlichen**.[161]

Ist **mehr als ein Verantwortlicher** oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an **derselben Verarbeitung** beteiligt und sind sie gemäß Art. 82 Abs. 2 und 3 DS-GVO für einen durch die Verarbeitung verursachten Schaden verantwortlich, so **haftet jeder Verantwortliche** oder jeder Auftragsverarbeiter für den **gesamten Schaden**, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.[162] Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Art. 82 Abs. 4 DS-GVO vollständigen Schadensersatz gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung Beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadensersatzes zurückzufordern, der unter den in Art. 82 Abs. 2 DS-GVO festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.[163]

[160] Art. 82 Abs. 2 S. 1 DS-GVO, siehe hierzu auch EG 146, 147 DS-GVO.
[161] vgl. Art. 28 Abs. 10 DS-GVO.
[162] Art. 82 Abs. 4 DS-GVO.
[163] vgl. Art. 82 Abs. 5 DS-GVO.

1.14. Wann haftet der Verantwortliche nicht?

Der Verantwortliche wird von der Haftung für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wurde, befreit, **wenn er nachweist**, dass er in **keinerlei Hinsicht** für den Umstand, durch den der Schaden eingetreten ist, **verantwortlich** ist.[164]

Der Verantwortliche kann sich exkulpieren, wenn der **Auftragsverarbeiter Weisungen des Verantwortlichen missachtet**. Ein Auftragsverarbeiter haftet dann für den durch eine Verarbeitung verursachten Schaden, wenn er seinen speziell als Auftragsverarbeiter auferlegten Pflichten aus der DS-GVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.[165]

Der Verantwortliche haftet auch dann nicht, wenn der Auftragsverarbeiter einen weiteren von ihm beauftragten Auftragsverarbeiter einsetzt.[166] Erfüllt ein weiterer, vom Auftragsverarbeiter hinzugezogener Auftragsverarbeiter seine Pflichten nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.[167]

Zur Haftung des Auftragsverarbeiters siehe auch Ziff. 1.10 und 4.8 FAQ.

1.15. Welche weiteren Dokumentations- und Nachweispflichten sind zu beachten?

a) Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften

Die Verwendung eines **Wahrscheinlichkeitswerts** über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung

[164] Art. 82 Abs. 3 i.V.m. Abs. 2 S. 1 DS-GVO.
[165] Art. 82 Abs. 2 S. 2 i.V.m. § 28 Abs. 3 S. 2 a), 29 DS-GVO, siehe hierzu auch EG 146, 147 DS-GVO.
[166] vgl. Art. 28 Abs. 4 S. 1 DS-GVO.
[167] vgl. Art. 28 Abs. 4 S. 2 DS-GVO.

über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person (Scoring) ist nur unter bestimmten in § 31 Abs. 1 Nr. 1 bis 4 DSAnpUG-EU aufgeführten Voraussetzungen zulässig.[168] Im Fall der **Nutzung von Anschriftendaten** ist die betroffene Person beispielsweise vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten zu unterrichten; die **Unterrichtung ist zu dokumentieren**.[169]

Die Verwendung eines von **Auskunfteien** ermittelten Wahrscheinlichkeitswerts über die **Zahlungsfähigkeit** und **Zahlungswilligkeit** einer natürlichen Person ist im Fall der Einbeziehung von Informationen über Forderungen nur zulässig, soweit die Voraussetzungen nach § 31 Abs. 1 DSAnpUG-EG vorliegen und nur solche Forderungen über eine geschuldete Leistung berücksichtigt werden, die trotz Fälligkeit nicht erbracht worden ist.[170] Dies können bspw. solche Forderungen sein,

- die durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden sind oder[171]
- die der Schuldner ausdrücklich anerkannt hat[172] oder
- deren zugrunde liegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und bei denen der Schuldner zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet hat (Nr. 5).[173]

Die Ermittlung von Wahrscheinlichkeitswerten von anderen bonitätsrelevanten Daten richtet sich nach dem **allgemeinen Datenschutzrecht**.[174]

[168] § 31 Abs. 1 Nr. 1 bis 4 DSAnpUG-EU.
[169] § 31 Abs. 1 Nr. 4 DSAnpUG-EU.
[170] § 31 Abs. 2 S. 1 DSAnpUG-EU.
[171] vgl. Art. 31 Abs. 2 S. 1 Nr. 1 DSAnpUG-EU.
[172] vgl. Art. 31 Abs. 2 S. 1 Nr. 3 DSAnpUG-EU
[173] vgl. § 31 Abs. 2 S. 1 Nr. 5 DSAnpUG-EU.
[174] vgl. § 31 Abs. 2 S. 2 DSAnpUG-EU.

b) Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person

Unterbleibt eine Information der betroffenen Person nach Maßgabe von § 32 Abs. 1 DSAnpUG-EU, ist der Verantwortliche verpflichtet, geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person zu ergreifen, einschließlich der Bereitstellung der in Art. 13 Absatz 1 und 2 der DS-GVO genannten Informationen für die Öffentlichkeit in **präziser, transparenter, verständlicher und leicht zugänglicher Form** in einer **klaren und einfachen Sprache.**[175] Der Verantwortliche hält in diesem Fall **schriftlich fest**, aus welchen Gründen er von einer **Information abgesehen** hat.[176] In den Fällen des § 32 Abs. 1 Nr. 4 und 5 DSAnpUG-EU gilt dies nicht (vgl. Ziff. 3.4 FAQ).[177]

Liegt nur ein **vorübergehender Hinderungsgrund** vor und unterbleibt die Benachrichtigung deshalb in den Fällen des § 32 Abs. 1 Nr. 1 bis 5 DSAnpUG-EU, muss der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer **angemessenen Frist nach Fortfall des Hinderungsgrundes**, spätestens jedoch **innerhalb von zwei Wochen**, nachkommen.[178]

c) Dokumentation der Gründe bei Auskunftsverweigerung

Die **Gründe** einer **Auskunftsverweigerung,** d.h. dem Nichtnachkommen der Auskunftsverpflichtung, sind zu **dokumentieren**[179]. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu **begründen**, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die

[175] vgl. § 32 Abs. 2 S. 1 i.V.m. Abs. 1 Nr. 1 bis 3 DSAnpUG-EU.
[176] vgl. § 32 Abs. 2 S. 2.
[177] § 32 Abs. 2 S. 3 DSAnpUG-EU
[178] vgl. § 32 Abs. 3 DSAnpUG-EU.
[179] § 34 Abs. 2 S. 1 DSAnpUG-EU.

die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.[180]

d) Informationspflicht, wenn ausnahmsweise keine Löschung stattfindet

Der Verantwortliche ist im Fall, dass **ausnahmsweise keine Löschung** stattfinden muss, wenn eine Beeinträchtigung schutzwürdiger Interessen der betroffenen Person vorliegt, verpflichtet, die betroffene Person über die Einschränkung der Verarbeitung zu **unterrichten**, sofern sich die Unterrichtung nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.[181]

e) Informationspflicht bei Datenpannen

Besteht ausnahmsweise **keine Verpflichtung zur Benachrichtigung** der betroffenen Person bei einer Verletzung des Schutzes personenbezogener Daten (Art. 34 DS-GVO), soweit durch die Information Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden Interessen eines Dritten, geheim gehalten werden müssen[182], ist die betroffene Person zu **benachrichtigen**, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.[183]

1.16. Was umfasst das Recht auf „Datenübertragbarkeit“?

Art. 20 DS-GVO beschreibt das Recht auf Datenübertragbarkeit. Dieses Recht ist eng mit dem Auskunftsrecht (Art. 15 DS-GVO) verbunden[184]. Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie

[180] § 34 Abs. 2 S. 2 DSAnpUG-EU.
[181] vgl. § 35 Abs. 2 S. 1 und 2 DSAnpUG-EU.
[182] vgl. § 29 Abs. 1 S. 3 DSAnpUG-EU
[183] vgl. § 29 Abs. 1 S. 4 DSAnpUG-EU.
[184] vgl.: Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit, S. 5.

dem Verantwortlichen bereitgestellt hat, in einem **strukturieren, gängigen und maschinenlesbaren Format** zu erhalten.[185] Zudem hat sie das Recht, diese **Daten einem anderen Verantwortlichen (Dritten)** ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu **übermitteln**.[186] Allerdings gilt beides nur, wenn folgende Voraussetzungen erfüllt sind:

- die Verarbeitung muss auf **Einwilligung** gemäß Art. 6 Abs. 1 a) oder Art. 9 Abs. 2 a) oder auf einem **Vertrag** gemäß Art. 6 Abs. 1 b) (Erforderlichkeit zur Erfüllung eines Vertrages) beruhen und[187]
- die Verarbeitung muss mithilfe **automatisierter Verfahren** erfolgt sein.[188]

Dieses Recht soll naturgemäß nicht gegen Verantwortliche ausgeübt werden, die personenbezogene Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten.[189]

Durch o.g. Rechte sollen betroffene Personen mit **Befugnissen in Bezug auf ihre eigenen personenbezogenen Daten** ausgestattet werden, indem es ihnen ermöglicht wird, Daten problemlos von einer IT-Umgebung in eine andere zu verschieben, zu kopieren oder zu übertragen.[190] So soll ihnen eine **größere Kontrolle** über die sie betreffenden personenbezogenen Daten eingeräumt werden.[191] Der Wechsel von einem Dienstanbieter zu einem anderen soll vereinfacht und somit der Wettbewerb zwischen Diensten gefördert werden,

[185] vgl. Art. 20 Abs. 1, 1. Hs. DS-GVO, vgl. EG 68 S. 1 DS-GVO.
[186] vgl. Art. 20 Abs. 1 1. Hs. DS-GVO.
[187] vgl. Art. 20 Abs. 1, 2. Hs. a) DS-GVO, vgl. EG 68 S. 3 und 4 DS-GVO
[188] vgl. Art. 20 Abs. 1, 2. Hs. b)DS-GVO, vgl. EG 68 S. 3 DS-GVO.
[189] vgl. EG 68 S. 5 DS-GVO, siehe hierzu weiter EG 68 S. 6 ff. DS-GVO.
[190] vgl. Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit, S. 4, Einführung, Abs. 2, S. 2.
[191] vgl. Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit, S. 3, Zusammenfassung, Abs. 1.

indem es für Einzelpersonen leichter wird, zwischen verschiedenen Anbietern zu wechseln.[192]

Bei der Ausübung des Rechts auf Datenübertragbarkeit hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten **direkt** von einem Verantwortlichen an einen anderen Verantwortlichen übermittelt werden, soweit dies **technisch machbar** ist.[193]

Der Verantwortliche ist angehalten, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen.[194] Ein geeignetes Mittel ist beispielsweise eine Self-Service Portallösung. Für den Verantwortlichen soll jedoch nicht die Pflicht begründet werden, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten.[195] Im Sinne einer bewährten Praxis sollten die für die Verarbeitung Verantwortlichen damit beginnen, Mittel wie Download-Tools und Anwendungsprogrammierschnittstellen zu entwickeln, um dem Verlangen nach Datenübertragbarkeit zu entsprechen.[196] Personenbezogene Daten sollten in Formaten bereitgestellt werden, die über ein sehr hohes Abstraktionsniveau verfügen.[197] Verantwortliche sollten mit den Daten möglichst viele Metadaten in bestmöglicher Qualität, was die Granularität betrifft, bereitstellen, so dass die genaue Bedeutung der ausgetauschten Daten erhalten bleibt. So wäre z. B. die Bereitstellung von PDF-Versionen eines E-Mail-Postfachs nicht ausreichend strukturiert.[198] E-Mail-Daten müssen in einem

[192] vgl. Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit, S. 4, Einführung, Abs. 2, S. 3.
[193] vgl. Art. 20 Abs. 2 DS-GVO, vgl. EG 68 S. 10 DS-GVO.
[194] vgl. EG 68 S. 2 DS-GVO.
[195] vgl. EG 68 S. 7 DS-GVO.
[196] vgl. Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit, Zusammenfassung S. 3 Abs. 4.
[197] vgl. Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit S.16,Abs. 2 .
[198] vgl. Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit, S. 16 Abs. 3.

Format bereitgestellt werden, in dem Metadaten beibehalten werden, um eine effektive Wiederverwendung der Daten zu ermöglichen.[199]

Ist im Fall eines bestimmten Satzes personenbezogener Daten mehr als eine betroffene Person tangiert, so sollte das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach der DS-GVO unberührt lassen.[200] In Grundrechte Dritter darf demnach nicht eingegriffen werden.

Das o.g. Recht der betroffenen Person lässt grundsätzlich das Recht auf **Löschung** (Art. 17 DS-GVO) unberührt[201] (siehe hierzu Ziff. 5.1 lit. c FAQ). D.h. das Recht auf Löschung besteht weiter. Dies soll insbesondere nicht bedeuten, dass die Daten, die sich auf die betroffene Person beziehen und von ihr zur Erfüllung eines Vertrags zur Verfügung gestellt worden sind, gelöscht werden, soweit und solange diese personenbezogenen Daten für die Erfüllung des Vertrags notwendig sind.[202] Dies bedeutet, dass Daten solange nicht gelöscht werden, wie es für die Erfüllung des Vertrages erforderlich ist. Durch die Datenübertragbarkeit ist der Verantwortliche nicht verpflichtet, personenbezogene Daten länger als notwendig oder über einen bestimmten Aufbewahrungszeitraum hinaus zu speichern.[203]

Die verlangten Informationen müssen in der Regel **unverzüglich**, **spätestens innerhalb eines Monats** nach Eingang des Antrags zur Verfügung gestellt werden.[204] Diese Frist kann um **zwei weitere Monate verlängert** werden, wenn dies unter Berücksichtigung der **Komplexität** und der **Anzahl von Anträgen**

[199] vgl. Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit S. 16, Abs. 3.
[200] vgl. EG 68 S. 7 DS-GVO, vgl. hierzu auch § 29 Abs. 1 DSAnpUG-EU.
[201] Art. 20 Abs. 3 DS-GVO.
[202] vgl. EG 68 S. 8 DS-GVO.
[203] vgl. Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit S. 6.
[204] vgl. Art. 12 Abs. 3 S. 1 DS-GVO.

erforderlich ist.[205] Der Verantwortliche hat die betroffene Person **innerhalb eines Monats** nach Eingang des Antrags über eine **Fristverlängerung**, zusammen mit den **Gründen für die Verzögerung**, zu **unterrichten**.[206] **Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.**[207]

Sofern der Verantwortliche dem Antrag der betroffenen Person **nicht nachkommen** wird, ist er verpflichtet, die betroffene Person **ohne Verzögerung**, **spätestens aber innerhalb eines Monats** nach Eingang des Antrags über die Gründe hierfür und über die **Möglichkeit**, bei der Aufsichtsbehörde **Beschwerde** oder einen **gerichtlichen Rechtsbehelf** einzulegen, zu unterrichten.[208]

Kosten für die Bearbeitung der Anfragen dürfen den Nutzern grundsätzlich nicht in Rechnung gestellt werden. Die Informationen sind grundsätzlich **unentgeltlich** zur Verfügung zu stellen.[209]

Bei **offenkundig unbegründeten** oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person, kann der Verantwortliche ein **angemessenes Entgelt** verlangen oder sich **weigern**, aufgrund des Antrags tätig zu werden.[210] Die Nachweispflicht liegt beim Verantwortlichen.[211]

[205] vgl. Art. 12 Abs. 3 S. 2 DS-GVO.
[206] vgl. Art. 12 Abs. 3 S. 3 DS-GVO.
[207] Art. 12 Abs. 3 S. 4 DS-GVO.
[208] vgl. Art. 12 Abs. 4 DS-GVO.
[209] vgl. Art. 12 Abs. 5 S. 1 DS-GVO.
[210] vgl. Art. 12 Abs. 5 S. 2 a) und b) DS-GVO.
[211] vgl. Art. 12 Abs. 5 S. 3 DS-GVO.

Der Umfang, die technische Umsetzung sowie die Auswirkungen der Regelung zur Datenübertragbarkeit sind zum jetzigen Zeitpunkt nicht absehbar. Es gibt derzeit keine Standards. Die Art.-29-Datenschutzgruppe empfiehlt deshalb nachdrücklich, dass Branchenvertreter und Fachverbände gemeinsam interoperable Standards und Formate erarbeiten, um dem Erfordernis des Rechts auf Datenübertragbarkeit Genüge zu tun.[212] Hierbei ist auch auf die Auslegung der Aufsichtsbehörden zu achten.

2. Grundsätzliche organisatorische Aspekte

2.1. Was sind wichtige Punkte beim Aufbau von Datenschutzmanagementsystem und Datenschutzorganisation?

a) Datenschutzmanagementsystem (DSMS)

Die Anforderung an ein DSMS leiten sich aus **Art. 24, 25 und 32 DS-GVO**[213] sowie dem **DSAnpUG-EU** ab.

Dem Verantwortlichen kommt die Aufgabe zu, die datenschutzrechtlichen Vorgaben der DS-GVO und des DSAnpUG-EU umzusetzen, Maßnahmen zu überprüfen, zu aktualisieren und dies entsprechend nachzuweisen.

Art. 24 DS-GVO beschreibt einen kontinuierlichen Verbesserungsprozess, welcher Bestandteil vieler Qualitätsmanagementsysteme ist. Die Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben wird in der Praxis häufig durch ein internes Kontrollsystem sichergestellt.

Der Datenschutzbeauftragte berät den Verantwortlichen, unterstützt den Aufbau eines Managementsystems und überprüft die Funktion interner Kontrollsysteme.

[212] vgl. Art. 29-Gruppe, Leitlinien zum Recht auf Datenübertragbarkeit S, 16.
[213] siehe hierzu auch EG 83 DS-GVO.

Das DSMS ist ein **Teil des Unternehmensmanagementsystems**, welches in der eigenen Verantwortung des Unternehmens unabhängig vom Datenschutzbeauftragten wirksam sein muss. Die schon vorhandenen Regelungen, z.B. der Dokumentenlenkung nach ISO 9001 QM, und die einheitliche Wahl der Begriffe, z.B. Policy, Leitlinie oder Richtlinie, sollten als Synergieeffekte genutzt werden. Der Ansatz des PDCA-Zyklus'[214] hat sich in der Praxis oftmals bewährt. Voraussetzung ist eine Standardisierung von Prozessen und die Implementierung eines Change Managements zur Verbesserung erkannter Mängel.

Es gibt eine Vielzahl von Anforderungen an die Dokumentation und den Nachweis durch die Rechenschaftspflicht/Accountability (nicht abschließend: Abschluss Auftragsverarbeitungsvertrag[215] , Erstellung Verzeichnis von Verarbeitungstätigkeiten[216], Treffen von Maßnahmen zur Sicherheit der Verarbeitung[217], Meldungen von Verletzungen des Schutzes personenbezogener Daten[218], Datenübermittlungen unter Verwendung geeigneter Garantien[219]). Ein Datenschutzkonzept kann durch das Standard-Datenschutzmodell unterstützt werden.[220]

Die ISO 27001 für die Informationssicherheit/TOMs ist für kleine und mittlere Unternehmen oftmals zu aufwändig und kann durch ISIS12 ersetzt werden. Die DS-GVO und ein vorhandenes IT-Sicherheitsmanagementsystem haben z.T.

[214] Unter dem PDCA-Zyklus versteht man das Modell zur Qualitätsverbesserung mit den vier Phasen planen (plan), ausführen (do), überprüfen (check) und verbessern (act) nach Shewhart.
[215] vgl. Art. 28 Abs. 3 S. 1 DS-GVO, siehe auch EG 109 DS-GVO zu Standard-Datenschutzklauseln der Kommission oder Aufsichtsbehörde.
[216] siehe Art. 30 DS-GVO.
[217] siehe Art. 32 DS-GVO, siehe EG 83 DS-GVO.
[218] siehe Art. 33 DS-GVO, siehe EG 85 S. 2, 88 DS-GVO.
[219] siehe Art. 46 DS-GVO, siehe auch EG 108 DS-GVO zu Fehlen eines Angemessenheitsbeschlusses.
[220] vgl.: Das Standard-Datenschutzmodell, Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele; Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2015), abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/10/SDM-Handbuch_V09a.pdf.

deckungsgleiche Schutzziele (z.B. Art. 32 Abs. 1 lit. b) DS-GVO, i.V.m. EG 83 DS-GVO).

b) Datenschutzorganisation

Im Unternehmen müssen **organisatorische Rahmenbedingungen**, insbesondere im Hinblick auf die vielfachen Dokumentations- und Nachweispflichten, geschaffen werden.

Wichtig ist die Festlegung der Grundsätze und Ziele mit organisatorischen Regelungen und Verantwortlichkeiten in Bezug auf die DS-GVO.

Die Prozesse und Arbeitsanweisungen sollten auf Konformität mit den Datenschutzrichtlinien des Unternehmens überprüft werden. Für die einzelnen Verarbeitungen sind abhängig von der Risikobewertung und der Schutzbedarfsermittlung angemessene technische und organisatorische Maßnahmen zu definieren und umzusetzen. Ein internes Kontrollsystem sollte implementiert werden, welches die Erfüllung der DS-GVO-Anforderungen in den Datenschutzprozessen gewährleistet.

c) Konzept zum Umgang mit Datenpannen (Verletzung des Schutzes personenbezogener Daten)

Der Verantwortliche muss **unternehmensintern** ein Konzept definieren, wie mit Verletzungen des Schutzes personenbezogener Daten (Datenpannen) umzugehen ist (vgl. Ziff. 1.12 lit. k) FAQ).

2.2. Was ist bei der Gestaltung des Datenschutzniveaus (Systeme, Anwendungen, Prozesse) zu beachten?

“Privacy by design” und “privacy by default”

Der Verantwortliche trifft unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere** der mit der Verarbeitung

verbundenen **Risiken** für die Rechte und Freiheiten natürlicher Personen sowohl zum **Zeitpunkt der Festlegung der Mittel** für die Verarbeitung als auch zum **Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen**.[221] Diese müssen darauf ausgelegt sein, die **Datenschutzgrundsätze** wie etwa Datenminimierung wirksam umzusetzen und die **notwendigen Garantien** in die Verarbeitung aufzunehmen, um den Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen zu schützen.[222]

Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch **Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.[223]

Ein genehmigtes Zertifizierungsverfahren gemäß Art. 42 kann als Faktor herangezogen werden, um die Erfüllung der o.g. Anforderungen nachzuweisen.[224]

Auch der Auftragsverarbeiter ist verpflichtet, technische und organisatorische Maßnahmen zu treffen[225] (siehe hierzu auch Ziff. 4.4 FAQ).

„Privacy by design“ meint die Technikgestaltung (Lösch- und Sperrmöglichkeiten, Verschlüsselung, Protokollierung und Zugriffsrechte). **„Privacy by default“** meint die datenschutzfreundlichen Voreinstellungen. Dazu sollte eine interne Strategie festgelegt werden. Zum Beispiel: Minimierung der Verarbeitung personenbezogener Daten, möglichst schnelle Pseudonymisierung.

[221] vgl. Art. 25 Abs. 1 DS-GVO, siehe auch EG 78 S. 1 DS-GVO.
[222] vgl. Art. 25 Abs. 1 DS-GVO, siehe auch EG 78 S. 2 und S. 3 DS-GVO.
[223] vgl. Art. 25 Abs. 2 S. 1 DS-GVO, siehe auch EG 78 S. 2 DS-GVO.
[224] Art. 25 Abs. 3 DS-GVO.
[225] vgl. Art. 32 Abs. 1 1. Hs. DS-GVO.

2.3. Wann muss ein Datenschutzbeauftragter benannt werden?

Die Pflicht zur Benennung eines Datenschutzbeauftragten besteht, wenn

- die **Verarbeitung von einer Behörde oder öffentlichen Stelle** durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln[226],
- die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der **Durchführung von Verarbeitungsvorgängen** besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen** erforderlich machen, oder[227]
- die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der **umfangreichen Verarbeitung besonderer Kategorien von Daten** gemäß Art. 9 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO besteht.[228]

In diesen Fällen sollte der Verantwortliche oder Auftragsverarbeiter bei der Überwachung der internen Einhaltung der Bestimmungen der DS-GVO von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt (d.h. einem Datenschutzbeauftragten), unterstützt werden.[229] (Zu den Aufgaben des Datenschutzbeauftragten siehe Ziff. 2.4 FAQ).

In anderen als den in Art. 37 Abs. 4 DS-GVO genannten Fällen können der Verantwortliche oder Auftragsdatenverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern

[226] vgl. Art. 39 Abs. 1 a) DS-GVO.
[227] vgl. Art. 39 Abs. 1 b) DS-GVO.
[228] vgl. Art. 37 Abs. 1 c) DS-GVO, vgl. EG 97 S. 1 DS-GVO.
[229] vgl. EG 97 S. 1 DS-GVO.

vertreten, einen Datenschutzbeauftragten benennen.[230] Wird kein Datenschutzbeauftragter bestellt, muss der Verantwortliche oder der Auftragsverarbeiter die sonst dem Datenschutzbeauftragten obliegenden Aufgaben übernehmen.

Damit ist die Bestellung eines Datenschutzbeauftragten für viele kleine und mittlere Unternehmen hiernach nicht zwingend erforderlich, da derartige Verarbeitungen zwar vorkommen können, aber nicht zur Kerntätigkeit gerechnet werden können. Allerdings könnte die Benennung nach weiteren Vorschriften erforderlich sein, zu beachten ist u.a. § 38 DSAnpUG-EG (s.u.).

Ergänzend zu den Anforderungen in Art. 37 Abs. 1 b) und c) DS-GVO[231] benennen der **Verantwortliche und der Auftragsverarbeiter nicht-öffentlicher Stellen** einen Datenschutzbeauftragten, soweit sie in der Regel **mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten** beschäftigen.[232]

Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer **Datenschutz-Folgenabschätzung** nach Art. 35 DS-GVO unterliegen (siehe Ziff. 1.12 lit. l) FAQ), oder verarbeiten sie personenbezogene Daten **geschäftsmäßig** zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie **unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen**.[233]

Der Datenschutzbeauftragte wird auf **Grundlage seiner beruflichen Qualifikation** und insbesondere des **Fachwissens** benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der

[230] vgl. Art. 37 Abs. 4, 1. Hs. DS-GVO.
[231] Art. 37 Abs. 1 b und c DS-GVO
[232] § 38 Abs. 1 S. 1 DSAnpUG-EU.
[233] § 38 Abs. 1 S. 2 DSAnpUG-EU.

Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DS-GVO genannten Aufgaben.[234]

Der Datenschutzbeauftragte kann **Beschäftigter** des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf Grundlage eines **Dienstleistungsvertrages** erfüllen.[235]

2.4. Was sind Funktion und Aufgaben des Datenschutzbeauftragten?

Der Datenschutzbeauftragte hat folgende Aufgaben:[236]

- die **Unterrichtung und Beratung des Verantwortlichen** oder des **Auftragsverarbeiters** und der **Beschäftigten**, die Verarbeitungen durchführen, hinsichtlich ihrer **datenschutzrechtlichen Pflichten**[237]
- die **Überwachung der Einhaltung der Vorgaben der DS-GVO**, **anderer Datenschutzvorschriften** der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der **Zuweisung von Zuständigkeiten**, der **Sensibilisierung** und **Schulung** der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen[238]
- die **Beratung** – auf Anfrage – im Zusammenhang mit der **Datenschutz-Folgenabschätzung** und **Überwachung ihrer Durchführung** gemäß Art. 35 DS-GVO[239] (vgl. Ziff. 1.12 lit. l) FAQ)

[234] vgl. Art. 37 Abs. 5 DS-GVO.
[235] vgl. Art. 37 Abs. 7 DS-GVO.
[236] siehe Art. 39 Abs. 1 DS-GVO.
[237] vgl. Art. 39 Abs. 1 a) DS-GVO.
[238] vgl. Art. 39. Abs. 1 b) DS-GVO.
[239] vgl. Art. 39 Abs. 1 c) DS-GVO.

- die **Zusammenarbeit mit der Aufsichtsbehörde**[240] (siehe auch Ziff. 2.7 FAQ)
- die Tätigkeit als **Anlaufstelle für die Aufsichtsbehörde** in mit der Verarbeitung zusammenhängenden Fragen einschließlich der vorherigen Konsultation gemäß Art. 36 DS-GVO, und ggf. Beratung zu allen sonstigen Fragen.[241]

Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen **Risiko** gebührend Rechnung und berücksichtigt dabei die **Art**, den **Umfang**, die **Umstände** und die **Zwecke der Verarbeitung**.[242]

2.5. Welche Auswirkungen ergeben sich für die Bestellung von betrieblichen Datenschutzbeauftragten in einer Unternehmensgruppe?

Neu ist die ausdrückliche Möglichkeit zur Bestellung eines **gemeinsamen Datenschutzbeauftragten** für eine Unternehmensgruppe (Konzern)[243] (siehe auch Ziff. 3.7 FAQ).Dieser muss vom ganzen Konzern sowie jedem Betroffenen aus leicht erreichbar sein.[244]

2.6. Sofern ein Datenschutzbeauftragter bestellt wird, welchen externen Stellen ist dies mitzuteilen?

Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht und der Aufsichtsbehörde mitgeteilt werden (siehe auch Ziff. 2.7 FAQ).[245] Die Nutzung der Formulierung „Namen und Kontaktdaten“ an anderen Stellen der

[240] vgl. Art. 39 Abs. 1 d) DS-GVO.
[241] vgl. Art. 39 Abs. 1 e) DS-GVO.
[242] vgl. Art. 39 Abs. 2 DS-GVO.
[243] vgl. Art. 37 Abs. 2 DS-GVO, siehe hierzu auch EG 97 S. 1 DS-GVO.
[244] vgl. Art. 37 Abs. 2 DS-GVO a.E..
[245] Art. 37 Abs. 7 DS-GVO.

DS-GVO lassen darauf schließen, dass zumindest bei der Veröffentlichung, z. B. in der Datenschutzerklärung auf der Internetseite des Unternehmens, auf den Namen des Datenschutz-beauftragten verzichtet werden kann und lediglich die reinen Kontaktdaten wie Adresse, Telefonnummer und E-Mailadresse anzugeben sind.

Der Aufsichtsbehörde wird voraussichtlich, nicht zuletzt wegen der Zusammenarbeitspflichten, auch der Name des Datenschutzbeauftragten genannt werden müssen.

2.7. In welchem Verhältnis stehen Datenschutzbeauftragter und Aufsichtsbehörde zueinander?

Der Datenschutzbeauftragte ist zur **Zusammenarbeit** mit der Aufsichtsbehörde verpflichtet.[246] Seine **Kontaktdaten** müssen der Aufsichtsbehörde **mitgeteilt** werden.[247]

Der Datenschutzbeauftragte dient als Anlaufstelle für die Aufsichtsbehörde in Fragen, die mit der Verarbeitung von personenbezogenen Daten zusammenhängen. Insbesondere benannt ist die Verpflichtung zur Konsultation der Aufsichtsbehörde im Zusammenhang mit einer **Datenschutz-Folgenabschätzung**, wenn aus dieser hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.[248]

Eine Konsultation der Aufsichtsbehörde sollte auch während der **Ausarbeitung von Gesetzes- oder Regelungsvorschriften** erfolgen, in denen eine Verarbeitung personenbezogener Daten vorgesehen ist, um die Vereinbarkeit

[246] Art. 39 Abs. 1 d) DS-GVO.
[247] Art. 37 Abs. 7 DS-GVO.
[248] Art. 36 Abs. 1 DS-GVO, siehe auch EG 94 S. 1 DS-GVO.

der geplanten Verarbeitung mit der DS-GVO sicherzustellen und insbesondere das mit ihr für die betroffene Person verbundene Risiko einzudämmen.[249]

Die Zusammenarbeitspflicht mit der Aufsichtsbehörde kann für den Datenschutzbeauftragten zu **Interessenkonflikten** führen, da er nicht nur Interessen von Betroffenen (Beschäftigten, Kunden), sondern auch berechtigte Interessen des Unternehmens berücksichtigen und ggf. vertreten muss. Der Datenschutzbeauftragte sollte sich daher mit der Unternehmensleitung über **Regeln zur Kommunikation mit der Aufsichtsbehörde** abstimmen.

2.8. Was sind die wesentlichen Schritte bei der Erstellung eines Verarbeitungsverzeichnisses?

Zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten sollten folgende Schritte beachtet werden:

- **Identifizierung** aller Datenerhebungen, -verarbeitungen mit personenbezogenen Daten (z.B. Kunden, Mitarbeiter, Lieferanten, Besucher) und bestimmen des Zwecks (Zweckbindung der Datenerhebung gemäß Art. 5 Abs. 1 b DS-GVO),
- **Analyse** des ggf. schon bestehenden Verfahrensverzeichnisses oder Bestandsaufnahme aller eingesetzten Verfahren und Erstellung der notwendigen Informationen,
- **Entscheidung über Zuständigkeiten** für die Erstellung und vor allem auch Pflege und Aktualisierung des Verarbeitungsverzeichnisses.

Für weitere Hinweise siehe Ziff. 2.9 FAQ.

[249] EG 96 DS-GVO.

2.9. Was sind die Vorgaben für die Erstellung des Verarbeitungsverzeichnisses?

Jeder Verantwortliche und ggf. sein Vertreter führen ein **Verzeichnis über alle Verarbeitungstätigkeiten**, die ihrer **Zuständigkeit** unterliegen.[250] Auch der **Auftragsdatenverarbeiter** muss ein Verarbeitungsverzeichnis führen (vgl. Ziff. 1.10 und 4.6 FAQ).[251] Das Verzeichnis ist die Grundlage zur Umsetzung der Dokumentationspflichten (vgl. Art. 24 Abs. 1 DS-GVO).

Die Verpflichtung zur Erstellung eines Verarbeitungsverzeichnisses besteht grundsätzlich **nicht in Unternehmen oder Einrichtungen mit weniger als 250 Beschäftigten**.[252] **Dies gilt jedoch nicht**, wenn

- die von dem Verantwortlichen oder Auftragsverarbeiter vorgenommene Verpflichtung ein **Risiko für die Rechte und Freiheiten der betroffenen Personen** birgt,
- die Verarbeitung **nicht nur gelegentlich** erfolgt oder
- die Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten i.S.d. Art. 10 einschließt.[253]

Insofern wird die Ausnahmeregelung nur selten greifen, da die die Verarbeitung häufig „nicht nur gelegentlich" erfolgt.

Das Verarbeitungsverzeichnis ist **schriftlich** zu führen.[254] Dies kann auch in einem **elektronischen Format** erfolgen.[255] Ggf. wird der Auftragnehmer im

[250] Art. 30 Abs. 1 S. 1 DS-GVO.
[251] vgl. Art. 30 Abs. 2 DS-GVO.
[252] vgl. Art. 30 Abs. 5 DS-GVO.
[253] vgl. Art. 30 Abs. 5 DS-GVO.
[254] vgl. Art. 30 Abs. 3 DS-GVO.
[255] vgl. Art. 30 Abs. 3 DS-GVO.

Rahmen von Vertragsverhandlungen, z.B. bei Auftragsdatenverarbeitungen, das Verzeichnis verlangen (ggf. als Anlage zum Vertrag).

Der Verantwortliche (oder der Auftragsverarbeiter) sowie ggf. der Vertreter des Verantwortlichen (oder des Auftragsverarbeiters) haben der **Aufsichtsbehörde** das Verarbeitungsverzeichnis **auf Anfrage** zur Verfügung zu stellen.[256] Ein „öffentliches Verfahrensverzeichnis“ ist nicht mehr erforderlich: Das Verarbeitungsverzeichnis ist nicht mehr, wie bislang das Verfahrensverzeichnis nach dem BDSG, öffentlich zugänglich zu machen.

Zu den Inhalten des Verzeichnisses vgl. Ziff. 2.10 FAQ. Die genaue Frage nach der Detailliertheit des Verzeichnisses ist derzeit jedoch noch nicht absehbar.

2.10. Welche sind die erforderlichen Inhalte des Verarbeitungsverzeichnisses nach DS-GVO und nach DSAnpUG-EU?

Jeder **Verantwortliche und ggf. sein Vertreter** führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.[257] Das Verzeichnis hat sämtliche der folgenden Angaben zu enthalten:

- **Name und Kontaktdaten des Verantwortlichen** und ggf. des **gemeinsam mit ihm Verantwortlichen**, des Vertreters des Verantwortlichen sowie eines etwaigen **Datenschutzbeauftragten**[258],
- **Zwecke der Verarbeitung**[259],
- **Beschreibung der Kategorien** betroffener Personen und der Kategorien personenbezogener Daten[260],
- **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,

[256] vgl. Art. 30 Abs. 4 DS-GVO.
[257] Art. 30 Abs. 1 S. 1 DS-GVO, siehe auch EG 82 DS-GVO.
[258] Art. 30 Abs. 1 a) DS-GVO.
[259] Art. 30 Abs. 1 b) DS-GVO.
[260] Art. 30 Abs. 1 c) DS-GVO.

einschließlich Empfänger in Drittländern oder internationalen Organisationen[261],

- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, sowie bei den in Art. 49 Abs. 1 Unterabs. 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien[262]
- wenn möglich, die **vorgesehenen Fristen für die Löschung** der verschiedenen Datenkategorien[263]
- wenn möglich, eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Art. 32 Abs. 1 DS-GVO (Sicherheit der Verarbeitung)[264].

Auch der **Auftragsverarbeiter** hat ein Verfahrensverzeichnis zu führen (siehe hierzu Ziff. 1.10 und 4.5 FAQ).

2.11. Welche Verpflichtungen auf Datengeheimnisse gibt es zukünftig?

In der DS-GVO existiert **keine ausdrückliche Verpflichtung** auf das Datengeheimnis. Das DSAnpUG-EU sieht lediglich eine Verpflichtung auf das Datengeheimnis im Hinblick auf die Datenschutz-Richtlinie für Polizei und Strafjustiz (Richtlinie (EU) 2016/680) vor. **Auf Basis der DS-GVO hat das Unternehmen dafür Sorge zu tragen, dass die datenschutzrechtlichen Regelungen eingehalten werden.**[265] Das schließt ein, dass Beschäftigte Daten nicht rechtswidrig verarbeiten dürfen. **Die Dokumentation über die**

[261] Art. 30 Abs. 1 d) DS-GVO.
[262] Art. 30 Abs. 1 e) DS-GVO.
[263] Art. 30 Abs. 1 f) DS-GVO.
[264] vgl. Art. Abs. 1 g) DS-GVO.
[265] siehe hierzu auch EG 74 bis 77 DS-GVO.

Verpflichtung auf das Datengeheimnis sollte demzufolge erhalten bleiben und auf die neuen Rechtsnormen angepasst werden.

Weiterhin darf der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf **Weisung des Verantwortlichen** verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.[266] Dies sollte **dokumentiert** werden.

Zudem muss der **Auftragsverarbeiter** im Rahmen der Auftragsverarbeitung gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur **Vertraulichkeit** verpflichtet haben oder einer **angemessenen gesetzlichen Verschwiegenheitspflicht** unterliegen.[267] Auch dies sollte entsprechend **dokumentiert** werden.

Zusätzlich können **spezielle Verpflichtungen zur Wahrung von Geschäftsgeheimnissen** in den jeweiligen Unternehmen erforderlich sein, die auf der Grundlage anderer gesetzlicher Normen basieren. Sofern sie nicht im Zuge des DSAnpUG-EU geändert werden, haben sie weiterhin Bestand.[268]

2.12. Besteht Anpassungsbedarf von Betriebsvereinbarungen und bestehenden Dokumenten?

Es ist zu empfehlen, Betriebsvereinbarungen zu prüfen und ggf. an die Regelungen zum Beschäftigtendatenschutz[269] anzupassen.

[266] Art. 29 DS-GVO, siehe auch § 28 Abs. 3 S. 2 a) DS-GVO.
[267] Art. 28 Abs. 3 b) DS-GVO.
[268] vgl. § 1 Abs. 2 S. 3 DS-GVO.
[269] siehe hierzu § 26 DSAnpUG-EU.

3. Zulässigkeit und Anforderungen bei der Erhebung, Verarbeitung und Nutzung von Daten

3.1. Welches sind die wesentlichen Voraussetzungen für die Erhebung von Daten?

Die Verarbeitung personenbezogener Daten ist **nur rechtmäßig**, wenn **mindestens eine** der nachstehenden Bedingungen erfüllt ist[270]:

- die betroffene Person hat ihre **Einwilligung** zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben,[271]
- die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder ist zur Durchführung vorvertraglicher Maßnahmen **erforderlich**, die auf Anfrage der betroffenen Person erfolgen;[272]
- die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;[273]
- die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;[274]
- 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;[275]
- die Verarbeitung ist zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen

[270] siehe hierzu auch EG 44 bis 50 DS-GVO.
[271] vgl. Art. 6 Abs. 1 a) DS-GVO.
[272] vgl. Art. 6 Abs. 1 b) DS-GVO.
[273] vgl. Art. 6 Abs. 1 c) DS-GVO.
[274] vgl. Art. 6 Abs. 1 d) DS-GVO.
[275] vgl. Art. 6 Abs. 1 e) DS-GVO.

Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.[276]

Ein **berechtigtes Interesse** könnte beispielsweise vorliegen, wenn eine **maßgebliche und angemessene Beziehung** zwischen der betroffenen Person und dem Verantwortlichen besteht, z.B. wenn die betroffene Person ein **Kunde** des Verantwortlichen ist oder in seinen **Diensten** steht.[277] Das Bestehen eines berechtigten Interesses ist in jedem Fall **sorgfältig abzuwägen**.[278] Dabei ist auch zu prüfen, ob die betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.[279] Muss die betroffene Person nicht mit einer weiteren Verarbeitung rechnen, könnten die Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen.[280] Letztlich ist der **konkrete Zweck für die Verarbeitung** der personenbezogenen Daten im **Einzelfall** klar zu definieren.

Die wesentlichen Prinzipien des bisherigen Datenschutzrechts (Einwilligung, Erforderlichkeit zur Erfüllung eines Vertrages, Verarbeitung nur aufgrund einer Rechtsgrundlage) bleiben erhalten. Die Bedeutung der berechtigten Interessen ist jetzt an dieser zentralen Stelle im Gesetz verortet.[281]

3.2. Welche Informationspflichten bestehen zukünftig?

Die Informationspflichten des Verantwortlichen oder Auftragsverarbeiters **erweitern** sich mit der Umsetzung der DS-GVO um ein Vielfaches, so dass die

[276] Art. 6 Abs. 1 f) DS-GVO.
[277] EG 47 S. 2 DS-GVO.
[278] EG 47 S. 3 DS-GVO.
[279] EG 47 S. 3 DS-GVO.
[280] EG 47 S. 4 DS-GVO.
[281] vgl. Art. 6 Abs. 1, f) DS-GVO.

Überarbeitung und Erweiterung von Datenschutzerklärungen erforderlich ist[282]. Für nähere Erläuterungen vgl. Ziff. 3.3 und 3.5.

3.3. Welche Informationspflichten bestehen bei der Erhebung personenbezogener Daten bei der betroffenen Person (Art. 13 DS-GVO)?

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person **zum Zeitpunkt der Erhebung dieser Daten** Folgendes mit[283]:

a) **Name und Kontaktdaten** des **Verantwortlichen** sowie ggf. auch Namen und Kontaktdaten seines **Vertreters** (Anschrift sowie die elektronische und/oder telefonische Erreichbarkeit),

b) Kontaktdaten des **Datenschutzbeauftragten**,

c) **Zwecke**, für die personenbezogene Daten **verarbeitet** werden sollen sowie die **Rechtsgrundlage** (genaue Angabe des §, Abs. und Gesetz, Verordnung etc.),

d) wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder Dritten erforderlich ist (Art. 6 Abs. 1 f DS-GVO): die **berechtigten Interessen**, die von dem Verantwortlichen oder Dritten verfolgt werden,

e) ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten,

f) ggf. Absicht des Verantwortlichen, die personenbezogenen Daten an eine Drittland oder eine internationale Organisation zu übermitteln sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission oder Verweis auf geeignete oder angemessene Garantien

[282] Art. 13 ff. DS-GVO.
[283] vgl. Art. 13 Abs. 1 DS-GVO.

und Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.[284]

Zusätzlich zu den o.g. Informationen stellt der Verantwortliche der betroffenen Person **zum Zeitpunkt der Erhebung dieser Daten** folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten[285]:

- die **Dauer**, für die die personenbezogene Daten **gespeichert** werden oder, falls dies nicht möglich ist, die **Kriterien der Festlegung** der Dauer der Speicherung (in der Regel ist konkret anzugeben, wie lange die personenbezogenen Daten gespeichert werden),[286]
- **Hinweis auf die Rechte der betroffenen Person** (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch, Datenübertragbarkeit),[287]
- sofern die Verarbeitung auf einer Einwilligung der betroffenen Person beruht, der **Hinweis** auf das Bestehen eines Rechts, die **Einwilligung jederzeit zu widerrufen**, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird,[288]
- Aufklärung über das **Bestehen eines Beschwerderechts** bei der Aufsichtsbehörde,[289]
- Information, ob die Bereitstellung der personenbezogenen Daten **gesetzlich oder vertraglich** vorgeschrieben, oder für einen Vertragsschluss erforderlich ist,[290]

[284] vgl. Art. 13 Abs. 1 a) bis f) DS-GVO, siehe hierzu auch EG 60 DS-GVO.
[285] vgl. Art. 13 Abs. 2 DS-GVO.
[286] vgl. Art. 13 Abs. 2 a) DS-GVO, siehe hierzu auch EG 60 DS-GVO.
[287] vgl. Art. 13 Abs. 2 b) DS-GVO.
[288] vgl. Art. 13 Abs. 2 c) DS-GVO.
[289] vgl. Art. 13 Abs. 2 d) DS-GVO.
[290] vgl. Art. 13 Abs. 2 e) DS-GVO.

- Information, ob die betroffene Person **verpflichtet** ist, die **personenbezogenen Daten bereitzustellen**, und welche möglichen Folgen eine Nichtbereitstellung hätte und[291]
- inwiefern **automatisierte Entscheidungsfindungen** einschließlich **Profiling** erfolgen und welche **Tragweite** und **Auswirkungen** diese haben.[292]

Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß Art. 13 (und 14) in **präziser, transparenter, verständlicher und leicht zugänglicher Form** in einer **klaren und einfachen Sprache** zu übermitteln; dies gilt insbesondere für Informationen, die sich an Kinder richten.[293] Die Übermittlung der Information hat **schriftlich oder in anderer Form**, ggf. auch elektronisch, zu erfolgen.[294] Sofern die betroffene Person eine **mündliche Auskunft** verlangt, kann auch diese erfolgen, sofern die **Identität** der betroffenen Person in anderer Form **nachgewiesen** wurde.[295]

Zeitliche Vorgaben, in welcher Frist die Information erfolgen soll, existieren für die o.g. Informationen gemäß Art. 13 DS-GVO nicht. Allerdings sollte die **Frist** je nach konkretem Einzelfall **angemessen** sein.[296]

Sofern der Verantwortliche dem Antrag der betroffenen Person **nicht nachkommen** wird, ist er verpflichtet, die betroffene Person **ohne Verzögerung**, spätestens aber **innerhalb eines Monats** nach Eingang des Antrags über die Gründe hierfür zu **unterrichten** und über die **Möglichkeit**, bei

[291] vgl. Art. 13 Abs. 2 e) DS-GVO.
[292] vgl. hierzu Art. 13 Abs. 2 f) DS-GVODS-GVO.
[293] vgl. Art. 12 Abs. 1 S. 1, 2. Hs. DS-GVO.
[294] vgl. Art. 12 Abs. 1 S. 2 DS-GVO.
[295] vgl. Art. 12 Abs. 1 S. 3 DS-GVO.
[296] vgl. EG 61 S. 1 DS-GVO.

der **Aufsichtsbehörde Beschwerde** oder einen **gerichtlichen Rechtsbehelf** einzulegen, zu **unterrichten**.[297]

Die o.g. Informationen sind grundsätzlich **unentgeltlich** zur Verfügung zu stellen.[298] Bei **offenkundig unbegründeten** oder – insbesondere im Fall von häufiger Wiederholung – **exzessiven** Anträgen einer betroffenen Person, kann der Verantwortliche ein **angemessenes Entgelt** verlangen oder sich **weigern**, aufgrund des Antrags tätig zu werden.[299] Die **Nachweispflicht** liegt beim **Verantwortlichen**.[300]

Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen **anderen Zweck** weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung **Informationen über diesen anderen Zweck** und alle anderen maßgeblichen Informationen gemäß Art. 13 Abs. 2 DS-GVO (s.o. 2. Absatz) zur Verfügung.[301]

Die Verarbeitung **besonderer Kategorien personenbezogener Daten** i.S.d. Art. 9 Abs. 1 DS-GVO (vgl. Ziff. 1.6 FAQ) zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen von § 24 Abs. 1 DSAnpUG-EU und ein Ausnahmetatbestand nach Art. 9 Abs. 2 DS-GVO oder nach § 22 DSAnpUG-EU vorliegen.[302]

Die o.g. **Informationspflichten gelten nicht**, wenn und soweit die **betroffene Person bereits über die Informationen verfügt**.[303] Die Pflicht Informationen zur Verfügung zu stellen, erübrigt sich auch dann, wenn die Speicherung oder

[297] vgl. Art. 12 Abs. 4 DS-GVO.
[298] vgl. Art. 12 Abs. 5 S. 1 DS-GVO.
[299] vgl. Art. 12 Abs. 5 S. 2 DS-GVO.
[300] Art. 12 Abs. 5 S. 3 DS-GVO.
[301] Art. 13 Abs. 3 DS-GVO.
[302] § 24 Abs. 2 DSAnpUG-EU.
[303] vgl. Art. 13 Abs. 4 DS-GVO, siehe auch EG 62, insbesondere S. 1 DS-GVO.

Offenlegung der personenbezogenen Daten **ausdrücklich** durch **Rechtsvorschriften** geregelt ist oder wenn sich die **Unterrichtung** der betroffenen Person als **unmöglich** erweist oder mit **unverhältnismäßig hohem Aufwand** verbunden ist.[304]

3.4. Welche Ausnahmen gibt es bei den Informationspflichten bei der Erhebung personenbezogener Daten bei der betroffenen Person?

Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen **Berufsgeheimnisträger** (z.B. Ärzte, Rechtsanwälte, Steuerberater) übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Art. 13 Abs. 3 DS-GVO nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.[305]

Das DSAnpUG-EU sieht in § 32 DSAnpUG-EG **weitere Ausnahmen** von der Verpflichtung zur Information der betroffenen Person vor. Dies ist in folgenden Fällen der Fall:

- Weiterverarbeitung betrifft **analog gespeicherte Daten**, bei der sich der Verantwortliche durch die Weiterverarbeitung **unmittelbar an die betroffene Person** wendet, der Zweck mit dem **ursprünglichen Erhebungszweck** gemäß der DS-GVO vereinbar ist, die Kommunikation mit der betroffenen Person **nicht in digitaler Form** erfolgt und das **Interesse** der betroffenen Person an der **Informationserteilung** nach den Umständen des Einzelfalls, insbesondere mit Blick auf den

[304] vgl. EG 62 S. 1 DS-GVO.
[305] § 29 Abs. 2 DSAnpUG-EU.

Zusammenhang, in dem die Daten erhoben wurden, als **gering** anzusehen ist[306],

- im Fall einer öffentlichen Stelle Gefährdung der ordnungsgemäßen Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 a bis e der DS-GVO und Überwiegen der Interessen des Verantwortlichen an der Nichterteilung denen der betroffenen Person[307],
- **Gefährdung** der **öffentlichen Sicherheit oder Ordnung** oder Nachteile für das Wohl des Bundes oder eines Landes und Überwiegen der Interessen des Verantwortlichen an der Nichterteilung der Information denen der betroffenen Person[308],
- **Beeinträchtigung** der **Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche** und Überwiegen die Interessen des Verantwortlichen an der Nichterteilung der Information denen der betroffenen Person oder[309],
- Gefährdung einer vertraulichen Übermittlung von Daten an öffentliche Stellen[310].

§ 24 Abs. 1 DSAnpUG-EU bestimmt zusätzlich, dass die Verarbeitung personenbezogener Daten zu einem **anderen Zweck** als zu demjenigen, zu dem die Daten erhoben wurden, durch eine nicht-öffentliche Stelle zulässig ist, wenn:

- sie zur **Abwehr von Gefahren** für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder

[306] vgl. § 33 Abs. 1 Nr. 1 DSAnpUG-EU.
[307] vgl. § 33 Abs. 1 Nr. 2 DSAnpUG-EU.
[308] § 33 Abs. 1 Nr. 3 DSAnpUG-EU.
[309] § 33 Abs. 1 Nr. 4 DSAnpUG-EU.
[310] § 33 Abs. 1 Nr. 5 DSAnpUG-EU.

- sie zur **Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche** erforderlich ist,

sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.[311]

3.5. Welche Informationspflichten bestehen, wenn die Erhebung NICHT direkt bei dem Betroffenen erfolgt (Art. 14 DS-GVO)?

Wenn die personenbezogenen Daten **NICHT** bei der betroffenen Person erhoben werden, bestehen **nahezu die gleichen Informationspflichten** wie bei der Erhebung direkt bei der betroffenen Person[312] (siehe Ziff. 3.3 FAQ). Verpflichtend kommt hier hinzu, dass über **Kategorien personenbezogener Daten**, die verarbeitet werden, informiert werden muss.[313]

Als zusätzliche Informationen[314] muss der Verantwortliche die betroffene Person darüber informieren, aus welcher Quelle die personenbezogenen Daten stammen und ob es sich dabei um eine öffentlich zugängliche Quelle handelt.[315]Die betroffene Person muss hier jedoch nicht über eine Verpflichtung zur Bereitstellung informiert werden, da sie selbst nicht über die Bereitstellung entscheiden kann; ebenso wenig kann eine Einwilligung vorliegen.

Hinsichtlich Zeitpunkt, Unterrichtungspflicht, Kosten für die Zurverfügungstellung von Informationen sowie Weiterverarbeitung zu einem anderen Zweck siehe Ziff. 3.3 FAQ.[316].

Eine Informationspflicht gemäß Art. 14 Abs. 1 bis 4 DS-GVO besteht **nicht**, wenn und soweit:

[311] vgl. § 24 Abs. 1 Nr. 1 und 2 DSAnpUG-EU.
[312] vgl. Art. 14 Abs. 1 und 2 DSAnpUG-EU.
[313] vgl. Art. 14 Abs. 1 d) DS-GVO.
[314] vgl. Art. 14 Abs. 2 DS-GVO.
[315] vgl. Art. 14 Abs. 2 f) DS-GVO, siehe hierzu auch EG 61 S.1 DS-GVO.
[316] vgl. Art 12 Abs. 1, 4 und 5 DS-GVO.

- die **betroffenen Person** bereits über die **Informationen verfügt**,[317]
- die Erteilung dieser Information sich als **unmöglich** erweist oder einen **unverhältnismäßigen** Aufwand erfordern würde,[318]
- die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, **ausdrücklich geregelt** ist[319] oder
- die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem **Berufsgeheimnis** einschließlich einer **satzungsmäßigen Geheimhaltungspflicht**, unterliegen und daher vertraulich behandelt werden müssen[320].

Siehe auch Ziff. 3.6 FAQ.

3.6. Welche Ausnahmen gibt es bei den Informationspflichten bei der Erhebung personenbezogener Daten NICHT bei der betroffenen Person?

Es besteht keine Pflicht zur Information der betroffenen Person gemäß Art. 14 Abs. 1 bis 4 DS-GVO, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem **Wesen nach**, insbesondere wegen der **überwiegenden berechtigten Interessen eines Dritten**, **geheim gehalten** werden müssen.[321] Das DSAnpUG-EU sieht in § 33 **weitere Ausnahmen** von der Verpflichtung zur Information der betroffenen Person gemäß Art. 14 Abs. 1, 2 und 4 DS-GVO vor, in Ergänzung zu Art. 14 Abs. 5 DS-GVO und § 29 Abs. 1 S. DSAnpUG-EU.

[317] § 14 Abs. 5 a) DS-GVO.
[318] § 14 Abs. 5 b) DS-GVO.
[319] § 14 Abs. 5 c) DS-GVO.
[320] § 14 Abs. 5 d) DS-GVO.
[321] vgl. § 29 Abs. 1 S. 1 DSAnpUG-EU.

Dies gilt:

- im Fall einer öffentlichen Stelle,

- wenn die **ordnungsgemäße Erfüllung** der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben i.S.d. Art. 23 Abs. 1 a bis e der DS-GVO **gefährden** würde oder[322]
- wenn die **öffentliche Sicherheit oder Ordnung gefährdet** würde oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.[323]

- im Fall einer nicht-öffentlichen Stelle

- die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Verarbeitung **Daten aus zivilrechtlichen Verträgen** beinhaltet und der Verhütung von Schäden durch Straftaten dient, sofern nicht das berechtigte Interesse der betroffenen Person an der Informationserteilung überwiegt, oder[324]
- die zuständige öffentliche Stelle gegenüber dem Verantwortlichen festgestellt hat, dass das Bekanntwerden der Daten die **öffentliche Sicherheit oder Ordnung gefährden** oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde; im Falle der Datenverarbeitung für Zwecke der Strafverfolgung bedarf es keiner Feststellung nach dem ersten Halbsatz[325].

[322] vgl. § 33 Abs. 1 Nr. 1 a) DSAnpUG-EU.
[323] vgl. § 33 Abs. 1 Nr. 1 b) DSAnpUG-EU.
[324] vgl. § 33 Abs. 1 Nr. 2 a) DSAnpUG-EU.
[325] vgl. § 33 Abs. 1 Nr. 2 b) DSAnpUG-EU.

3.7. Was gilt für den Datenaustausch im Konzern?

Die DS-GVO kennt die „**Unternehmensgruppe**“, bestehend aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen.[326] **Innerhalb einer Unternehmensgruppe kann der Austausch von Kunden- und Beschäftigtendaten zu internen Verwaltungszwecken ein berechtigtes Interesse darstellen.**[327] Trotzdem ist dabei jedes Verfahren unter Abwägung der schützenswerten Interessen der Betroffenen auf seine Rechtmäßigkeit hin zu prüfen und zu bewerten. So kann ein konzernweites Kunden-Managementsystem einen entsprechenden internen Verwaltungszweck darstellen, sowie auch der Austausch von Kundendaten zu Werbezwecken.[328]

Verträge zum Datenaustausch können auch zwischen Konzernunternehmen sinnvoll und angemessen sein. Inhalte von konzerneinheitlichen Informationssicherheits- und Datenschutzrichtlinien müssen darin allerdings nicht wiederholt werden, da sie ohnehin für beide Vertragspartner gelten. Es sollte aber auf sie verwiesen und sie einbezogen werden.

Ausgenommen von dieser Regelung sind Unternehmen einer Unternehmensgruppe mit Sitz in einem Drittland[329].

Im öffentlichen Bereich ist eine separate Prüfung vorzunehmen Hierbei sind auch die Landesdatenschutzgesetze zu beachten.

3.8. Welche Grundlagen gelten zukünftig für den Betrieb von Videoeinrichtungen?

In der DS-GVO wird das Thema „Videoüberwachung“ nicht explizit geregelt. Das deutsche DSAnpUG-EU jedoch nimmt dies für gewisse Anwendungsgebiete

[326] Art. 4 Nr. 11 DS-GVO.
[327] vgl. EG 47 S. 2, 48 S. 1 DS-GVO.
[328] vgl.: Best Practice Guide Europäische Datenschutzgrundverordnung, Auswirkungen auf das Dialogmarketing; Deutscher Dialogmarketing Verband e.V. (2016); abrufbar unter: https://www.ddv.de/verband/publikationen/best-practice-guides.html.
[329] vgl. Art. 2 Abs. 2 a) oder b) DS-GVO.

(wie Einkaufszentren, Parkplätze, Sport- und Versammlungsstätten, öffentlicher Personennahverkehr) auf.[330]

4. Auftragsverarbeitung

4.1. Wann liegt eine Auftragsverarbeitung vor?

Eine Auftragsverarbeitung liegt dann vor, wenn eine Verarbeitung (Art. 4 Nr. 2 DS-GVO) im Auftrag eines Verantwortlichen erfolgt.[331] **Der Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet**.[332] Dies bedeutet: Bedient sich ein Verantwortlicher eines Dienstleisters, der im Auftrag des Verantwortlichen mit dessen personenbezogenen oder personenbeziehbaren Daten (Kunden oder Beschäftigte) in Kontakt kommt und diese i.S.d. Art. 4 Nr. 2 DS-GVO verarbeitet, handelt es sich um eine Auftragsverarbeitung.

Somit sind von dem Verarbeitungsvorgang auch Wartungs- und Pflegeleistungen erfasst, welche Dritte bei dem und für den Verantwortlichen durchführen.

Beispiel: Zu „anderen Formen der Bereitstellung“ zählt auch der Inhalt von personenbeziehbaren Log-Dateien (z. B. ein Ereignis-Protokoll, aus dem ersichtlich wird, welche Aktionen wann von wem und wo stattgefunden haben). Denn der Dienstleister kann sehen, welcher Techniker wann was geändert hat. Dabei ist es unerheblich, ob ein Zugriff des Auftragsverarbeiters per Fernwartung oder vor Ort erfolgt.

[330] vgl. § 4 DSAnpUG-EU.
[331] Art. 28 Abs. 1 DS-GVO.
[332] Art. 4 Nr. 8 DS-GVO.

4.2. Wer kommt als Auftragsverarbeiter in Frage?

Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die **hinreichende Garantien** dafür bieten, dass **geeignete technische und organisatorische Maßnahmen** so durchgeführt werden, dass die Verarbeitung im Einklang mit der Anforderungen der DS-GVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.[333]

Hierzu zählen insbesondere folgende Anforderungen und Vorgaben:

- Sicherheit der Verarbeitung, z.B. durch Verschlüsselung zur Risikoeindämmung[334],
- Meldepflichten gegenüber dem Verantwortlichen.335

Bestehende Zertifikate sind zu prüfen und ggf. durch eigene Kontrollen zu ergänzen.

4.3. Wie kommt die Beauftragung/Bestellung eines Auftragsverarbeiters zu Stande?

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines **Vertrags** oder eines **anderen zugelassenen Rechtsinstruments** nach dem Unionsrecht oder dem Recht der Mitgliedstaaten.[336]

Dieser ist **schriftlich** abzufassen, was auch in einem **elektronischen Format** geschehen kann.[337] Ein zwingendes Schriftformerfordernis existiert demnach zwar nicht mehr, kann jedoch wegen anderer Dokumentationspflichten (z. B.

[333] Art. 28 Abs. 1 i.V.m. Art. 32 DS-GVO, siehe auch EG 81 S. 1 DS-GVO.
[334] vgl. EG 83 S. 1 DS-GVO.
[335] vgl. § 28 Abs. 3 S. 1 f) i.V.m. Art. 32 bis 36 DS-GVO, § 28 Abs. 3 S. 2 h i.V.m. Abs. 3 S. 3 DS-GVO.
[336] Art. 28 Abs. 3 S. 1 DS-GVO, siehe hierzu auch EG 81 S. 3 DS-GVO.
[337] vgl. Art. 28 Abs. 9 DS-GVO.

ISMS: **I**nformations-**S**icherheits-**M**anagement-**S**ystem in Bezug auf die Lieferantenbeziehung gemäß den Vorgaben der ISO 27001) geboten sein.

4.4. Was ist inhaltlich bei der Beauftragung eines Auftragsverarbeiters mindestens zu regeln?

Der **Vertrag** bzw. das **andere Rechtsinstrument** müssen folgende Punkte regeln:

- **Gegenstand** und **Dauer der Verarbeitung**,
- **Art** und **Zweck der Verarbeitung**,
- **Art der personenbezogenen Daten**,
- die **Kategorien** betroffener Personen,
- **Rechte und Pflichten des Verantwortlichen**.[338]

In Bezug auf Vertragsregelungen bietet es sich an, dass schon in der Beauftragung/Bestellung die ersten drei Punkte festgelegt werden.

Die danach folgenden konkreten datenschutzrechtlichen Vorgaben könnten in einer gesonderten Auftragsverarbeiter-Regelung (Vertrag oder anderes Rechtsinstrument) als Anlage zum konkreten (Dienstleistungs-)Vertrag bzw. der Beauftragung/Bestellung ausgewiesen werden.

In dem Vertrag oder anderen Rechtsinstrument ist insbesondere zu regeln[339], dass der Auftragsverarbeiter:

- personenbezogene Daten grundsätzlich **nur auf dokumentierte Weisung des Verantwortlichen** (auch in Bezug auf die Übermittlung

[338] Art. 28 Abs. 3 S. 1 DS-GVO.
[339] vgl. Art. 28 Abs. 3 S. 2 a) bis h), S. 3 i.V.m. Abs. 2 und 4 DS-GVO, siehe hierzu auch EG 81 S. 3 DS-GVO.

personenbezogener Daten an ein Drittland oder eine internationale Organisation) verarbeitet[340],

- gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten **befugten Personen** zur **Vertraulichkeit verpflichtet** werden, soweit sie keiner angemessenen gesetzlichen **Verschwiegenheitspflicht** unterliegen;[341]der Verantwortliche und der Auftragsdatenverarbeiter **geeignete technische und organisatorische Maßnahmen** treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und alle gemäß Art. 32 DS-GVO erforderlichen Maßnahmen ergreifen[342] (vgl. Ziff. 1.12 lit. j) FAQ).
- die in **Art. 28 Abs. 2 und 4 DS-GVO** genannten **Bedingungen** für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters **einhält**[343],
- **ohne vorherige schriftliche Genehmigung** des Verantwortlichen **keine weiteren Auftragsverarbeiter** hinzuzieht; der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter zu informieren hat und der Verantwortliche die Möglichkeit hat, gegen derartige Ersetzungen Einspruch erhebt;[344]
- bei Hinzuziehungen von weiteren Auftragsverarbeitern, diesen **dieselben Verpflichtungen** aus seinem Vertrag mit dem Verantwortlichen auferlegt, die auch für ihn gelten. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende

[340] Art. 28 Abs. 3 S. 2, a) DS-GVO.
[341] Art. 28 Abs. 3 S. 2, b) DS-GVO.
[342] zu den Maßnahmen im Einzelnen siehe Art. 32 Abs. 1 Hs. 2 a) bis d) DS-GVO.
[343] vgl. Art. 28 Abs. 3 S. 2, d) DS-GVO.
[344] vgl. Art. 28 Abs. 3 S. 2, d) i.V.m. Abs. 2 DS-GVO

Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters[345],

- angesichts der Art der Verarbeitung den Verantwortlichen mit **geeigneten technischen und organisatorischen Maßnahmen** dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf der in Kapitel III genannten Rechte (Art. 12 ff. DS-GVO, z.B. Informationsrechte, Recht auf Berichtigung und Löschung, Widerspruchsrecht) der betroffenen Person nachzukommen[346],
- unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der **Einhaltung der in Art. 32 bis 36 DS-GVO[347] genannten Pflichten unterstützt**[348],
- **nach Abschluss** der Erbringung der Verarbeitungsleistungen grundsätzlich **alle personenbezogenen Daten** nach Wahl des Verantwortlichen entweder **löscht oder zurückgibt und bestehende Kopien vernichtet**, wenn nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;[349]
- dem Verantwortlichen alle **erforderlichen Informationen** zum Nachweis der Einhaltung der in Art. 28 niedergelegten Pflichten **zur Verfügung stellt** und **Überprüfungen** – einschließlich Inspektionen –, die vom

[345] vgl. Art. 28 Abs. 3 S. 2, d) i.V.m. Abs. 4 DS-GVO.
[346] vgl. Art. 28 Abs. 3 S. 2, e) DS-GVO.
[347] Art. 32 (Sicherheit der Verarbeitung), Art. 33 (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde), Art. 34 (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffener Personen), Art. 35 (Datenschutz-Folgenabschätzung), Art. 36 (Vorherige Konsultation Aufsichtsbehörde).
[348] vgl. Art. 28 Abs. 3 S. 2, f) DS-GVO.
[349] Art. 28 Abs. 3 S. 2, g) DS-GVO.

Verantwortlichen oder einem anderen von diesem **beauftragten Prüfer** durchgeführt werden, **ermöglicht** und dazu **beiträgt**.[350]

Mit Blick auf Abs. 3 S. 2, h) DS-GVO informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.[351]

Home-Office/Telearbeit beim Auftragsverarbeiter

Bei Auftragsverarbeitungsvereinbarungen sollte bei Fernzugriffen weiterhin darauf geachtet werden, dass dies ausschließlich über eine „sichere Infrastruktur“ erfolgt und nicht z.B. von einem beliebigen Hotelzimmer über unsichere Hot-Spots.

Formulierungsvorschlag: „Eine Verarbeitung von personenbezogenen Daten außerhalb des Firmengeländes (in Privatwohnungen der Mitarbeiter) des Auftragsverarbeiters (Telearbeitsplätze / Heimarbeitsplätze / Home-Office) ist nicht zulässig, es sei denn, dass die Zugriffe auf solche Daten ausdrücklich über das gesicherte Datennetz (IT-Sicherheitsinfrastruktur) des Auftragsverarbeiters erfolgt.“

Verbindung des Verantwortlichen mit „öffentlichem Bereich“

Soweit ein Verantwortlicher (z.B. Stadtwerk als eigene GmbH) das Datennetz gemeinsam mit einer öffentlichen Stelle/Behörde betreibt, sind auch immer Vorgaben aus den Landesdatenschutzgesetzen einzubeziehen. Ggf. erweitern sich dadurch auch die TOMs.

[350] Art. 28 Abs. 3 S. 2 h) DS-GVO.
[351] vgl. Art. 28 Abs. 3 S. 3 DS-GVO.

4.5. Was gilt, wenn dem Auftragsverarbeiter Verletzungen des Schutzes personenbezogener Daten bekannt werden?

Wird dem **Auftragsverarbeiter** eine Verletzung des Schutzes personenbezogener Daten bekannt, hat er diese **unverzüglich dem Verantwortlichen** zu melden.[352]

4.6. Was enthält das Verzeichnis der Verarbeitungstätigkeiten im Fall der Auftragsverarbeitung?

Ein Auftragsverarbeiter und ggf. sein Vertreter hat ein **Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitungen** zu führen[353]. Dabei sind folgende Inhalte auszuweisen:

- der **Namen und die Kontaktdaten** des **Auftragsverarbeiters** oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten,[354]
- **Kategorien von Verarbeitungen**, die **im Auftrag jedes Verantwortlichen** durchgeführt werden[355],
- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlandes oder der betreffenden Organisation, sowie bei

[352] vgl. Art. 33 Abs. 2 DS-GVO.
[353] Art. 30 Abs. 2 DS-GVO, siehe hierzu auch EG 82 S. 1 DS-GVO.
[354] Art. 30 Abs. 2 a) DS-GVO.
[355] Art. 30 Abs. 2 b) DS-GVO.

den in Art. 49 Abs. 1 Unterabs. 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien[356],

- wenn möglich eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** in Bezug auf die Sicherheit der Datenverarbeitung (Art. 32 DS-GVO)[357],

Das Verzeichnis der Verarbeitungstätigkeiten ist **schriftlich** zu führen, was auch in **elektronischer** Form erfolgen kann.[358] **Auf Anfrage** ist dieses Verzeichnis der **Aufsichtsbehörde** zur Verfügung zu stellen (siehe auch Ziff. 1.12 lit. i) FAQ).[359]

Diese Pflichten gelten **nicht** für Unternehmen und Einrichtungen, die **weniger als 250 Mitarbeiter** beschäftigen. Diese Einschränkung **gilt aber nicht**, sofern die von ihnen vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die **Verarbeitung nicht nur gelegentlich** erfolgt oder die Verarbeitung **besonderer Datenkategorien** gemäß Art. 9 Abs. 1 DS-GVO bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten i.S.d. Art. 10 DS-GVO einschließt.[360] Aufgrund der Voraussetzung „nicht nur gelegentlich“ wird in den meisten Fällen ein Verarbeitungsverzeichnis erstellt werden müssen.

4.7. Was ist gemeint mit der neuen Regelung als „gemeinsam für die Verarbeitung Verantwortliche“?

Dies ist eine neue, zusätzlich aufgenommene Variante, zu verstehen als „gemeinsam verarbeitende und verantwortliche Stellen“.

[356] Art. 30 Abs. 2 c) DS-GVO.
[357] Art. 30 Abs. 2, d) DS-GVO, siehe hierzu auch EG 83 DS-GVO.
[358] Art. 30 Abs. 3 DS-GVO.
[359] Art. 30 Abs. 4 DS-GVO, siehe hierzu auch EG 82 S. 2 DS-GVO.
[360] Art. 30 Abs. 5 DS-GVO.

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als **gemeinsam Verantwortliche**.[361]

Gemeinsam Verantwortliche haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in **transparenter** Form in einer **Vereinbarung** festzulegen.[362]

Es handelt sich dann auch um einen Vertrag (auf Gegenseitigkeit) und nicht um eine schlichte Beauftragung eines Dienstleisters/Auftragsverarbeiters durch einen Verantwortlichen. Dieser ist und bleibt in vollem Umfang allein „Herr der Daten".

Aus der Vereinbarung muss insbesondere hervorgehen, **wer welchen Informationspflichten nachzukommen** hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können (siehe hierzu auch Ziff. 1.7 FAQ).

In diesem Fall haben dann auch alle Verantwortlichen die Regelungen zu einer möglichen weiteren Auftragsvereinbarung zu unterzeichnen.

4.8. Wer haftet, wenn sich ein Auftragsverarbeiter nicht an seine Pflichten hält?

Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen die DS-GVO bestimmt, wird in Bezug auf diese Verarbeitung dann **selbst Verantwortlicher**.[363] Damit haftet er dann auch direkt für alle auftretenden Schäden allein.

Ebenso haftet der Auftragsverarbeiter für den durch eine Verarbeitung verursachten Schaden, wenn er seinen **speziell als Auftragsverarbeiter auferlegten Pflichten aus der DS-GVO nicht nachgekommen** ist oder unter

[361] Art. 26 Abs. 1 S. 1 DS-GVO, siehe auch EG 79 DS-GVO.
[362] Art. 26 Abs. 1 S. 2 DS-GVO.
[363] vgl. Art. 28 Abs. 10 DS-GVO.

Nichtbeachtung der rechtmäßig erteilten **Anweisungen** des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.[364]

Kommt ein Subunternehmer eines Auftragsverarbeiters seinen Datenschutzpflichten nicht nach, haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters bzw. Subunternehmers.[365]

Siehe hierzu auch Ziff. 1.10 und 1.14 FAQ.

4.9. Gibt es die „Funktionsübertragung“ weiterhin?

Eine Funktionsübertragung lag bislang vor, wenn dem Dienstleister bei der Datenverarbeitung eine gewisse Eigenverantwortlichkeit und Entscheidungsbefugnis zukam, die seine Tätigkeit über die reine Hilfsfunktion hinaushob. Der Auftraggeber hatte also keine Eingriffsmöglichkeit mehr. Darauf kommt es in der DS-GVO jedoch nicht mehr an. Ausreichend ist die Vorlage eines Vertrags- bzw. Auftragsverhältnis.

In der DS-GVO wird nunmehr lediglich auf ein **Auftragsverhältnis** abgestellt, nicht jedoch auf Weisungsrechte und Verantwortlichkeiten.[366]

Ein **eigenverantwortliches Handeln** des Auftragsverarbeiters ist nach der Definition ebenso wenig ausgeschlossen wie **Entscheidungsspielräume** des Auftragsverarbeiters.

[364] Art. 82 Abs. 2 S. 2 i.V.m. § 28 Abs. 3 S. 2 a), 29 DS-GVO, siehe hierzu auch EG 146, 147 DS-GVO.
[365] Art. 28 Abs. 4 S. 2 DS-GVO.
[366] vgl. Art. 4 Nr. 8 DS-GVO.

Das Cloud Computing lässt sich zwanglos mit der Definition vereinbaren. Die herkömmliche **Abgrenzung zur „Funktionsübertragung“ wird damit jedoch obsolet**.

Es werden daher in jedem Fall entsprechende vertragliche Regelungen erforderlich sein. Bei allen Funktionsübertragungen ist zu prüfen, ob sie einer Auftragsverarbeitungsregelung bedürfen.

4.10. Wie verhält es sich mit der Übermittlung personenbezogener Daten in Drittländer?

Der Datentransfer in Drittländer wird in Kapitel V der DS-GVO bzw. Kapitel 5 des DSAnpUG-EU separat behandelt und ist hier nicht Gegenstand der Betrachtungen zur Auftragsverarbeitung.

5. Rechte des Betroffenen

5.1. Welche Rechte haben betroffene Personen auf Basis der Datenschutzgrundverordnung?

a) Recht auf Auskunft[367]

Das Auskunftsrecht ermöglicht der betroffenen Person, einen Einblick in das Ob und Wie der Verarbeitung ihrer personenbezogenen Daten zu erhalten. Im Falle einer Verarbeitung hat die betroffene Person das Recht auf Auskunft und auf folgende Informationen:

- **Verarbeitungszwecke**,[368]
- **Kategorien** der personenbezogenen Daten, die verarbeitet werden,[369]
- **Empfänger** oder **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch

[367] Art. 15 DS-GVO, siehe hierzu auch EG 63, insbesondere S. 3 DS-GVO.
[368] Art. 15 Abs. 1 a) DS-GVO.
[369] Art. 15 Abs. 1 b) DS-GVO.

offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen[370]

- falls möglich die **geplante Dauer**, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die **Kriterien** für die Festlegung dieser Dauer[371];
- das **Bestehen eines Rechts auf Berichtigung oder Löschung** der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung,[372]
- Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde[373]
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle **verfügbaren Informationen über die Herkunft** der Daten;[374]
- Bestehen einer **automatisierten Entscheidungsfindung** einschließlich **Profiling** gemäß Art. 22 DS-GVO und – zumindest in diesen Fällen – aussagekräftigte Informationen über die involvierte **Logik** sowie **Tragweite** und die **angestrebten Auswirkungen** einer derartigen Verarbeitung für die betroffene Person[375]

Der Verantwortliche stellt hierzu eine **Kopie der personenbezogenen Daten**, die Gegenstand der Verarbeitung sind, zur Verfügung.[376] Dies hat grundsätzlich **unentgeltlich** zu erfolgen.[377] Nur für alle weiteren Kopien, die die betroffene

[370] Art. 15 Abs. 1 c) DS-GVO.
[371] Art. 15 Abs. 1 d) DS-GVO.
[372] Art. 15 Abs. 1 e) DS-GVO.
[373] Art. 15 Abs. 1 f) DS-GVO.
[374] Art. 15 Abs. 1 g) DS-GVO.
[375] Art. 15 Abs. 1 h) DS-GVO.
[376] Art. 15 Abs. 3 S. 1 DS-GVO.
[377] vgl. Art. 12 Abs. 5 DS-GVO.

Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen.[378] Stellt die betroffene Person den Antrag **elektronisch**, so sind die Informationen in einem gängigen **elektronischen Format** zur Verfügung zu stellen.[379]

Darüber hinaus besteht das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DS-GVO **nicht**, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der **überwiegenden berechtigten Interessen eines Dritten**, **geheim gehalten** werden müssen.[380]

Das Recht auf Auskunft besteht zudem in Ergänzung zu den in § 27 Abs. 2, 28 Abs. 2 und 29 Abs. 1 S. 2 DSAnpUG-EG genannten Ausnahmen **nicht**, wenn

- die betroffene Person nach § 33 Abs. 1 und 3 DSAnpUG-EG **nicht zu informieren** ist[381] oder
- die Daten

  a) nur deshalb gespeichert sind, weil sie aufgrund **gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht** werden dürfen oder[382]

  b) **ausschließlich Zwecken** der **Datensicherung** oder der **Datenschutzkontrolle** dienen und die Auskunftserteilung einen **unverhältnismäßigen Aufwand** erfordern würde sowie eine Verarbeitung

[378] vgl. Art. 15 Abs. 3 S. 2 DS-GVO.
[379] Art. 15 Abs. 3 S. 3 DS-GVO.
[380] vgl. § 29 Abs. 1 S. 2 DSAnpUG-EU.
[381] § 34 Abs. 1 Nr. 1 DSAnpUG-EU.
[382] § 34 Abs. 1 Nr. 2 a) DSAnpUG-EU

zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.[383]

Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine öffentliche Stelle weder automatisiert noch nicht-automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person **Angaben** macht, die das **Auffinden der Daten ermöglichen** und der für die Erteilung der Auskunft erforderliche Aufwand **nicht außer Verhältnis** zu dem von der betroffenen Person geltend gemachten Informationensinteresse steht.[384]

b) Recht auf Berichtigung[385]

Die betroffene Person hat das Recht, von dem Verantwortlichen **unverzüglich** die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.[386] Die betroffene Person hat auch das Recht auch mittels ergänzender Erklärung, die **Vervollständigung** personenbezogener Daten zu verlangen.[387]

c) Recht auf Löschung („Recht auf Vergessenwerden“)[388]

Die betroffen Person hat das Recht, von dem Verantwortlichen **unverzüglich** die Löschung der sie betreffenden personenbezogenen Daten zu verlangen. [389]
Der Verantwortliche ist verpflichtet, personenbezogene Daten **unverzüglich** zu löschen, wenn u.a. folgende Gründe zutreffen:

[383] § 34 Abs. 1 Nr. 2 b) DSAnpUG-EU.
[384] § 34 Abs. 4 DSAnpUG-EU.
[385] Art. 16 DS-GVO, siehe hierzu auch EG 65 S. 1 DS-GVO.
[386] Art. 16 S. 1 DS-GVO, siehe hierzu auch EG 65 S. 1 DS-GVO.
[387] vgl. Art. 16 S. 2 DS-GVO.
[388] Art. 17 DS-GVO, siehe auch EG 65 S. 2 DS-GVO.
[389] vgl. Art. 17 Abs. 1, 1. Hs. DS-GVO, siehe hierzu auch EG 65 S. 2 DS-GVO.

- die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, **nicht mehr notwendig**[390]**,**
- die betroffene Person **widerruft** ihre Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 Abs. 1 a) oder Art. 9 Abs. 2 a) DS-GVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung[391],
- die betroffene Person legt gemäß Art. 21 Absatz 1 DS-GVO **Widerspruch** gegen die Verarbeitung ein und es liegen **keine vorrangigen berechtigten Gründe für die Verarbeitung** vor, oder die betroffene Person legt gemäß Art. 21 Abs. 2 DS-GVO Widerspruch gegen die Verarbeitung ein[392],
- die personenbezogenen Daten wurden **unrechtmäßig** verarbeitet[393],
- die Löschung ist zur **Erfüllung einer rechtlichen Verpflichtung** nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt[394],
- die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DS-GVO erhoben[395].

Das „Recht auf Vergessenwerden“ besteht auch, wenn der Verantwortliche die zu löschenden Daten **öffentlich** gemacht hat und er zur Löschung gemäß Art. 17 Abs. 1 DS-GVO **verpflichtet** ist.[396] Unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten trifft der Verantwortliche angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die

[390] vgl. Art. 17 Abs. 1 a) DS-GVO, siehe hierzu auch EG 65 S. 2 DS-GVO.
[391] vgl. Art. 17 Abs. 1 b) DS-GVO, siehe hierzu auch EG 65 S. 2 DS-GVO.
[392] vgl. Art. 17 Abs. 1 c) DS-GVO, siehe hierzu auch EG 65 S. 2 DS-GVO.
[393] vgl. Art. 17 Abs. 1 d) DS-GVO.
[394] vgl. Art. 17 Abs. 1 e) DS-GVO.
[395] vgl. Art. 17 Abs. 1 f) DS-GVO.
[396] vgl. Art. 17 Abs. 2 DS-GVO, siehe auch EG 66 DS-GVO.

Löschung aller Links zu diesen personenbezogenen Daten oder von **Kopien** oder **Replikationen** dieser personenbezogenen Daten verlangt.[397] Zu benachrichtigen sind in diesem Fall alle Stellen, die die gelöschten Daten verarbeiten (insbesondere Suchmaschinen).

In **Ausnahmefällen** besteht das Recht auf Vergessenwerden allerdings nicht.[398] Dies ist beispielsweise der Fall bei der Verarbeitung zur Ausübung des Rechts auf **freie Meinungsäußerung** und Information[399] oder zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen**[400].

Das DSAnpUG-EU bestimmt, dass das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Art. 17 Abs. 1 der DS-GVO ergänzend zu den in Art. 17 Abs. 3 DS-GVO genannten Ausnahmen **nicht** besteht, wenn eine Löschung im Falle nicht automatisierter Datenverarbeitung wegen der **besonderen Art** nicht oder nur mit **unverhältnismäßig hohem Aufwand** möglich ist.[401] In diesem Fall tritt an die Stelle einer Löschung die **Einschränkung der Verarbeitung** gemäß Art. 18 DS-GVO.[402].

Dies gilt nicht, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.[403] Ergänzend zu Art. 18 Abs. 1 b) und c) DS-GVO gilt § 35 Absatz 1 S. 1 und 2 entsprechend im Fall des Art. 17 Abs.1 a) und d) der DS-GVO, solange und soweit der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung **schutzwürdige Interessen** der betroffenen Person beeinträchtigt

[397] vgl. Art. 17 Abs. 2 DS-GVO.
[398] vgl. Art. 17 Abs. 3 a) bis e) DS-GVO, siehe hierzu auch EG 65 S. 4 DS-GVO.
[399] vgl. Art. 17 Abs. 3 a) DS-GVO.
[400] vgl. Art. 17 Abs. 3 e) DS-GVO.
[401] vgl. § 35 Abs. 1 S. 2 DSAnpUG-EU.
[402] vgl. § 36 Abs. 1 S. 2 DSAnpUG-EU.
[403] vgl. § 35 Abs. 1 S. 3 DSAnpUG-EU

würden.[404] Der Verantwortliche unterrichtet die betroffene Person über die Einschränkung der Verarbeitung, sofern sich die Unterrichtung nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.[405]

Ergänzend zu Art. 17 Abs. 3 b) DS-GVO gilt § 35 Abs. 1 DSAnpUG-EU entsprechend im Fall des Art. 17 Abs. 1 a) DS-GVO, wenn einer Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen.[406]

d) **Recht auf Einschränkung der Verarbeitung**[407]

Das Recht besteht, wenn eine der folgenden Voraussetzungen gegeben ist:

- die **Richtigkeit** der Daten wird von der betroffenen Person **bestritten**[408],
- die Verarbeitung ist **unrechtmäßig** und die betroffene Person lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die **Einschränkung der Nutzung der Daten**[409],
- der Verantwortliche benötigt die personenbezogenen Daten nicht länger für die Zwecke der Verarbeitung, die **betroffenen Person benötigt** sie jedoch zur **Geltendmachung**, **Ausübung** oder **Verteidigung von Rechtsansprüchen**[410] oder
- die betroffene Person hat **Widerspruch** gegen die Verarbeitung gemäß Art. 21 Abs. 1 DS-GVO eingelegt, **solange nicht feststeht**, ob die **berechtigten Gründe** des Verantwortlichen gegenüber denen der betroffenen Person **überwiegen**.[411]

[404] § 35 Abs. 2 S. 1 DSAnpUG-EU.
[405] vgl. § 35 Abs. 2 S. 2 DSAnpUG-EU.
[406] vgl. § 35 Abs. 3 DSAnpUG-EU.
[407] vgl. Art. 18 DS-GVO, siehe hierzu auch EG 67 DS-GVO.
[408] vgl. Art. 18 Abs. 1 a) DS-GVO.
[409] vgl. Art. 18 Abs. 1 b) DS-GVO.
[410] vgl. Art. 18 Abs. 1 c) DS-GVO.
[411] vgl. Art. 18 Abs. 1 d) DS-GVO.

Methoden zur Beschränkung der Verarbeitung personenbezogener Daten könnten u.a. darin bestehen, dass ausgewählte personenbezogene Daten **vorübergehend in ein anderes Verarbeitungssystem** übertragen werden, dass sie **für Nutzer gesperrt** werden oder dass **veröffentlichte Daten vorübergehend von einer Website entfernt** werden.[412]

Der Verantwortliche teilt **grundsätzlich allen Empfängern**, denen personenbezogene Daten offen gelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Art. 16, Art. 17 Abs. 1 und Art. 18 DS-GVO mit.[413] Diese Verpflichtung besteht nur dann nicht, wenn sich vorgenanntes als unmöglich erweist oder mit einem unverhältnismäßig großen Aufwand verbunden ist.[414] Der Verantwortliche ist verpflichtet, die betroffene Person über diese Empfänger zu unterrichten, wenn sie es verlangt.[415]

e) Recht auf Datenübertragbarkeit[416]

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem **strukturierten, gängigen und maschinenlesbaren Format** zu erhalten.[417] Sie hat zudem das Recht, diese Daten einem anderen Verantwortlichen **ohne Behinderung** durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, unter folgenden Voraussetzungen zu übermitteln:

[412] vgl. EG 67 S. 1 DS-GVO.
[413] vgl. Art. 19 S. 1, 1. Hs. DS-GVO.
[414] vgl. Art. 19 S. 1, 2. Hs. DS-GVO.
[415] vgl. Art. 19 S. 2 DS-GVO.
[416] vgl. Art. 20 DS-GVO.
[417] vgl. Art. 20 Abs. 1, 1. Hs. DS-GVO, siehe hierzu auch EG 68, insbesondere S. 1 DS-GVO.

- die Verarbeitung beruht auf **Einwilligung** gemäß Art. 67 Abs. 1 a) oder Art. 9 Abs. 2 a) oder auf einem Vertrag gemäß Art. 6 Abs.1 b) DS-GVO und[418]
- die Verarbeitung erfolgt **mit Hilfe automatisierter Verfahren**.[419]

Das Recht auf Löschung (vgl. Ziff. 5.1 lit. c) FAQ) bleibt unberührt (Art. 17 DS-GVO).[420] Ebenso gilt dieses Recht nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.[421] Damit können die Daten von dem einem zu einem anderen Anbieter mitgenommen werden. Das Recht ist beschränkt auf Daten, die der Betroffene dem Verarbeiter zur Verfügung gestellt hat und gilt nicht im öffentlichen Bereich.

f) **Widerspruchsrecht**[422]

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer **besonderen Situation** ergeben, **jederzeit** die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 e) DS-GVO (Verarbeitung ist für Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt) oder f) DS-GVO (Verarbeitung ist zur Wahrung der berechtigten Interessen erforderlich) erfolgt, **Widerspruch** einzulegen.[423] **Der Verantwortliche verarbeitet die personenbezogenen Daten sodann nicht mehr**, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen,

[418] Art. 20 Abs. 1 , 2. Hs. a) DS-GVO
[419] Art. 20 Abs. 1 , 2. Hs. b) DS-GVO.
[420] Art. 20 Abs. 3 S. 1 DS-GVO.
[421] Art. 20 Abs. 3 S. 2 DS-GVO.
[422] Art. 21 DS-GVO.
[423] Art. 20 Abs. 1 S. 1, 1. Hs. DS-GVO, siehe hierzu auch EG 69 S. 1 DS-GVO.

oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.[424]

Nach Erhalt des Widerspruchs ist der Verantwortliche demnach bis zu dem Zeitpunkt, an dem die Interessen des Betroffenen abgewogen sind, zur **Sperrung** verpflichtet.

Werden personenbezogene Daten verarbeitet, um **Direktwerbung** zu betreiben, so hat die betroffene Person das Recht, **jederzeit Widerspruch** gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen.[425]

Die betroffene Person muss **spätestens zum Zeitpunkt der ersten Kommunikation** mit ihr ausdrücklich auf das in Art. 21 Abs. 1 und 2 DS-GVO genannte Widerspruchsrecht hingewiesen werden.[426] Dieser Hinweis muss in einer **verständlichen** und **von anderen Informationen getrennten Form** erfolgen.[427] Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht **mittels automatisierter Verfahren** ausüben, bei denen technische Spezifikationen verwandt werden.[428]

6. Sanktionen

6.1. Welche Sachverhalte sind sanktioniert? Welche Höhe haben die Sanktionen?

Die Aufsichtsbehörde ist berechtigt, Bußgelder zu verhängen.[429] Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich oder anstelle von

[424] vgl. Art. 20 Abs. 1 S. 2 DS-GVO, siehe hierzu auch EG 69 S. 2 DS-GVO.
[425] Art. 20 Abs. 2, 1. Hs. DS-GVO, siehe hierzu auch EG 70 DS-GVO.
[426] vgl. Art. 21 Abs. 4 Hs. 1 DS-GVO.
[427] vgl. Art. 21 Abs. 4 Hs. 2 DS-GVO
[428] vgl. Art. 21 Abs. 5 DS-GVO.
[429] Art. 83 Abs. 1 DS-GVO, siehe hierzu auch EG 148 S. 1 DS-GVO.

Maßnahmen nach Art. 58 Abs. 2 a) bis h) und i) DS-GVO[430] verhängt.[431] Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall gesondert geprüft.[432] Berücksichtigt werden u.a.:

- **Art**, **Schwere** und **Dauer** des Verstoßes, unter Berücksichtigung der **Art**, des **Umfangs** oder des **Zwecks** der betreffenden Verarbeitung sowie der **Zahl** der von der Verarbeitung betroffenen Personen und des **Ausmaßes des erlittenen Schadens**[433],
- **Vorsätzlichkeit** oder **Fahrlässigkeit** des Verstoßes[434],
- **Grad der Verantwortung** des Verantwortlichen oder des Auftragsverarbeiters[435],
- **etwaige frühere Verstöße** des Verantwortlichen oder des Auftragsverarbeiters[436].

Die Bußgelder betragen bei Verstößen eher **administrativer Art** bis zu **10 Mio. EUR oder bis zu 2% des globalen Jahresumsatzes**, je nachdem, welcher der Beträge höher ist.[437] Dies können folgende Verstöße sein:

- Verstoß gegen Pflichten der Verantwortlichen und Auftragsverarbeiter gemäß **Art. 8** (fehlende Einwilligung Kind), **11** (Identifikation der betroffenen Person), **25 bis 39**, **42** und **43 DS-GVO**,[438]

[430] z.B. Durchführung von Untersuchungen in Form von Datenschutzüberprüfungen (Art. 58 Abs. 1 b) DS-GVO.
[431] vgl. Art. 83 Abs. 2 S. 1 DSVGO.
[432] Art. 83 Abs. 2 S. 2 DS-GVO, siehe hierzu auch EG 150 S. 2 DS-GVO.
[433] Art. 83 Abs. 2 S. 2 a) DS-GVO.
[434] Art. 83 Abs. 2 S. 2 b) DS-GVO.
[435] Art. 83 Abs. 2 S. 2 d) DS-GVO.
[436] Art. 83 Abs. 2 S. 2 e) DS-GVO.
[437] Art. 83 Abs. 4 DS-GVO.
[438] vgl. Art. 83 Abs. 4 a) DS-GVO.

- Verstoß gegen Pflichten der Zertifizierungsstelle gemäß Art. 42 und 43 DS-GVO[439],
- Verstoß gegen Pflichten der Überwachungsstelle gemäß Art. 41 Abs. 3 DS-GVO[440]

Dieses Bußgeld kann beispielsweise dann verhängt werden, wenn zwischen dem Verantwortlichen und Auftragsverarbeiter nach den Voraussetzungen des Art. 28 DS-GVO kein Auftragsdatenverarbeitungsvertrag abgeschlossen wird. Gerade im Hinblick darauf, dass es keine Funktionsübertragung mehr gibt, ist hierauf besonders zu achten.

Bei Verstößen, die sich an der **betroffenen Person** orientieren und gegen Rechte dieser Personen verstoßen, können durch die Aufsichtsbehörde Bußgelder bis zu **20 Mio. EUR oder bis zu 4% des globalen Jahresumsatzes** verhängt werden, je nachdem, welcher der Beträge höher ist.[441] Darunter fallen z. B.

- Verstöße gegen die **Grundsätze der Verarbeitung**, einschließlich der Bedingungen für die Einwilligung, gemäß den Art. 5, 6, 7 und 9 DS-GVO[442].
- Verstöße gegen die **Rechte der betroffenen Person** gemäß Art. 12-22 DS-GVO,[443]
- Verstöße gegen die **Übermittlung personenbezogener Daten** an einen Empfänger in ein Drittland oder an eine internationale Organisation gemäß Art. 44 bis 49 DS-GVO,[444]

[439] vgl. Art. 83 Abs. 4 b) DS-GVO.
[440] vgl. Art. 83 Abs. 4 c) DS-GVO.
[441] Art. 83 Abs. 5 DS-GVO.
[442] vgl. Art. 83 Abs. 5 a) DS-GVO.
[443] vgl. Art. 83 Abs. 5 b) DS-GVO.
[444] vgl. Art. 83 Abs. 5 c) DS-GVO.

- Verstöße gegen alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden (Vorschriften für besondere Verarbeitungssituationen)[445]
- **Nichtbefolgung einer Anweisung** oder einer **vorübergehenden oder endgültigen Beschränkung** oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Art. 58 Abs. 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 DS-GVO.[446]

Auch bei **Nichtbefolgen einer Anweisung der Aufsichtsbehörde** gemäß Art. 58 Abs. 2 DS-GVO werden im Einklang mit Art. 58 Abs. 2 DS-GVO Geldbußen von **bis zu 20 Mio. EUR** oder im Fall eines Unternehmens von **bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres verhängt, je nachdem welcher Betrag höher ist.[447]

Bußgeldkatalog der DS-GVO	
Bußgeld bis zu **10 Mio. EUR oder bis zu 2% des globalen Jahresumsatzes**, je nachdem, welcher der Beträge höher ist	Bußgeld bis zu **20 Mio. EUR oder bis zu 4% des globalen Jahresumsatzes** verhängt werden, je nachdem, welcher der Beträge höher ist
Verstöße gegen Regelungen z.B. - zu Schutzmaßnahmen (technisch-organisatorische Maßnahmen) - zur Auftragsverarbeitung (auch durch Auftragsverarbeiter) - zum Verzeichnis der Verarbeitungstätigkeiten - zur Datenschutz-Folgenabschätzung - zur Bestellung eines Datenschutzbeauftragten	Verstöße gegen Regelungen z. B. - zu den Grundsätzen der Verarbeitung - zu den Rechten der betroffenen Person - zu den Einwilligungen - zur Zusammenarbeit mit der Aufsichtsbehörde Nichtbefolgung von Anweisungen der Aufsichtsbehörde

[445] vgl. Art. 83 Abs. 5 d) DS-GVO.
[446] vgl. Art. 5 e) DS-GVO.
[447] Art. 83 Abs. 6 DS-GVO.

Es gilt nach den neuen Regelungen eine **Beweislastumkehr**, das heißt, **Unternehmen müssen nachweisen, dass die Datenverarbeitung rechtmäßig erfolgt ist**. Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Art. 82 Abs. 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.[448] Können die Unternehmen das nicht nachweisen, gilt die Datenverarbeitung als unrechtmäßig und ist sanktionsbewährt.

Im DSAnpUG-EU sind die Bußgeldvorschriften in § 43 geregelt. Sie gelten zusätzlich zu den Regelungen in der DS-GVO.

Für Verstöße nach Art. 83 Abs. 4 bis 6 DS-GVO gelten, soweit das DSAnpUG-EU nichts anderes bestimmt, die Vorschriften des **Gesetzes über Ordnungswidrigkeiten (OWiG)** sinngemäß.[449] Keine Anwendung finden die §§ 17, 35 und 36 OWiG.[450]

Für Verstöße nach Art. 83 Abs. 4 bis 6 DS-GVO gelten, soweit das DSAnpUG-EU nichts anderes bestimmt, die Vorschriften des OWiG und der allgemeinen Gesetze über das Strafverfahren (Strafprozessordnung und Gerichtsverfassungsgesetz), entsprechend.[451] Zu Ausnahmen siehe § 41 Abs. 2 S. 2 und 3 DSAnpUG-EU.

---

[448] vgl. Art. 82 Abs. 3 DS-GVO.
[449] vgl. § 41 Abs. 1 S. 1 DSAnpUG-EU.
[450] vgl. § 41 Abs. 1 S. 2 DSAnpUG-EU.
[451] vgl. § 41 Abs. 2 S. 1 DSAnpUG-EU.

Ansprechpartnerinnen:

Romy Sucher

Fachgebietsleiterin Arbeits- und Vertragsrecht

Syndikusrechtsanwältin, Datenschutzbeauftragte

Tel.: + 49 30 58580139
E-Mail: sucher@vku.de

Isabel Orland

Fachgebietsleiterin Gasnetze

Tel.: + 49 30 58580196

E-Mail: orland@vku.de

Wir danken den Mitgliedern der ad hoc AG-Datenschutz für die gute

Zusammenarbeit bei der gemeinsamen Erstellung der Inhalte dieses FAQ:

Stefan Beyer, Datenschutzbeauftragter, badenova AG & Co. KG

Jürgen Brockhausen, Datenschutz und Informationsfreiheit, Berliner Wasserbetriebe AöR

Carsten Domat, Leiter Datenschutz; Stadtwerke Düsseldorf AG

Jörg Kehrmann, Datenschutzbeauftragter; WSW Wuppertaler Stadtwerke GmbH

Armin Loreck, Revision, Betrieblicher Datenschutzbeauftragter, NEW AG

Matthias Platzer, Stadtwerke München

Dirk Ritter, Datenschutzbeauftragter, Stadtwerke Bielefeld GmbH

Ralf Schmachtel, Revision und Datenschutzbeauftragter, HAMBURG WASSER

Thorsten Schneider, aov IT.Services GmbH

Ingo Schütt, Datenschutzbeauftragter, Stromnetz Hamburg GmbH

Klaus Seeger, IT-Sicherheits- und Datenschutzbeauftragter, rku.it GmbH

Julia Simon, Datenschutzbeauftragte, Berliner Stadtreinigung