einfließen, welchen tendenziellen Einfluss diese Daten auf die Entscheidungsfindung haben (zB Formulierung wie „je höher/mehr/weniger, desto …") und was die (negativen) Folgen für sie sein können (Beispiele: Verweigerung des Kredits oder Vertragsschlusses; kein Kauf auf Rechnung[60]). Beruht die automatisierte Entscheidungsfindung auf Bonitätsauskünften und Scoring, sind auch die Vorgaben des § 31 BDSG zu beachten. Sofern die automatisierte Entscheidung auf einem Scoring beruht, in das auch **Anschriftendaten** mit einfließen, muss die betroffene Person gem. § 31 Abs. 1 Nr. 4 BDSG auf die vorgesehene Nutzung dieser Daten explizit hingewiesen werden.

Praxistipp:
Auch wenn diese Informationspflichten einerseits nicht verlangen, dass konkrete Algorithmen offengelegt werden müssen, sollten die diesbezüglichen Informationen andererseits aber auch nicht zu knapp bzw. zu abstrakt ausfallen. Es gilt insoweit nämlich zu bedenken, dass die Information der betroffenen Person zu den Maßnahmen iSd Art. 22 Abs. 3 DS-GVO bzw. Art. 22 Abs. 4 Hs. 2 DS-GVO gehört,[61] die den rechtmäßigen Einsatz solcher Verfahren formal absichern. Ein höherer Grad an Transparenz gegenüber der betroffenen Person entfaltet damit tendenziell auch eine höhere risikomitigierende bzw. legitimierende Wirkung. **111**
Sofern für die automatisierte Entscheidungsfindung spezialisierte Dienstleister wie zB Auskunfteien eingesetzt werden, sollte darauf geachtet werden, dass diese aufgrund der größeren Sachnähe vertraglich verpflichtet werden, entsprechende – im Idealfall bereits mit einer Aufsichtsbehörde abgestimmte – Informationsmuster bereitzustellen oder zumindest bei der Erstellung solcher Hinweise durch Bereitstellung der erforderlichen Informationen mitzuwirken.[62]

In **anderen Fällen einer Entscheidungsfindung basierend auf Profiling,** die tat- **112**
bestandsmäßig nicht von Art. 22 DS-GVO erfasst sind (zB Profiling im Marketingbereich) greifen zwar nach hier vertretener Auffassung die Vorgaben des Art. 13 Abs. 2 Buchst. f DS-GVO bzw. Art. 14 Abs. 2 Buchst. g DS-GVO zum Informationsinhalt nicht direkt. Der Europäische Datenschutzausschuss sieht es gleichwohl als „good practice" an, sich bei der Erfüllung der insoweit gleichwohl bestehenden Informationspflichten an den inhaltlichen Vorgaben des Art. 13 Abs. 2 Buchst. f DS-GVO bzw. Art. 14 Abs. 2 Buchst. g DS-GVO zu orientieren.[63]

g) Wird über die Datenkategorien sowie die Quelle(n) informiert? [Nur relevant für die Informationspflichten im Zusammenhang mit einer Dritterhebung von Daten nach Art. 14 DS-GVO]

Werden personenbezogene Daten nicht bei der betroffenen Person selbst erhoben, ist die **113**
betroffene Person zum einen auch über die verarbeiteten **Datenkategorien** (Art. 14 Abs. 1 Buchst. d DS-GVO) und zum anderen auch über die **Quellen,** aus denen diese Daten stammen (Art. 14 Abs. 2 Buchst. f DS-GVO), zu informieren. Diese Informationspflichten finden **in Art. 13 DS-GVO keine Entsprechung,** da die betroffene Person hier selbst an der Erhebung der Daten mitwirkt, zB durch Eingabe der Daten in ein Formular. Sie ist damit selbst „Quelle" und weiß, welche Daten sie bereitstellt.

[60] So zB im Falle des Einsatzes einer „automatisierten Zahlartensteuerung" basierend auf einer Bonitätsprüfung im Bestellprozess eines Online-Shops.
[61] Art. 29 Datenschutzgruppe WP 251rev.01, 6.2.2018, S. 7.
[62] So schon in BeckOK DatenschutzR/Schmidt/Wudy DS-GVO Art. 15 Rn. 79.
[63] Art. 29-Datenschutzgruppe, WP 251 rev.01, 6.2.2018, S. 18 (dort: Fn. 24) und S. 27.

Praxistipp:

114 Sofern personenbezogene Daten zwar faktisch direkt bei der betroffenen Person erhoben werden, diese davon aber keine Kenntnis hat (zB automatische Erhebung von Daten, die in benutzten Endgeräten der betroffenen Person gespeichert bzw. von diesen ausgesendet werden, wie zB Cookies, IP–Adressen, Browser-Einstellungen, etc), sollte die betroffene Person trotzdem auch über die „im Hintergrund" erhobenen Kategorien von personenbezogenen Daten informiert werden. Insoweit ist die Situation nämlich vergleichbar mit der einer Dritterhebung.

115 Bei der Festlegung der **Datenkategorien** und deren Abstraktionsgrad besteht ein gewisser Spielraum des Verantwortlichen. Die Datenkategorien sollten unter Transparenzgesichtspunkten gleichwohl nicht zu generisch gewählt werden.[64] Es kann sich insoweit anbieten, die Datenkategorien vorab zu definieren und jeweils ein paar Beispiele für konkrete personenbezogene Daten, die unter die jeweilige Kategorie fallen, zu nennen (zB „Stammdaten wie zB Name, Vorname, Geburtsdatum, Kundennummer"; „Adressatendaten wie zB Straße, Hausnummer, PLZ, Ort" etc).

116 Grundsätzlich ist die betroffene Person über die **konkreten Quelle(n)** aus der/denen der Verantwortliche die personenbezogenen Daten erhoben hat, zu informieren (zB Auskunftei XY).[65] Sinn und Zweck dieser Informationspflicht ist es nämlich, die betroffene Person in die Lage zu versetzen, Datenströme Stück für Stück bis zur Ausgangsquelle zurückverfolgen zu können, um dann ggf. dort Betroffenenrechte (zB Auskunftsrecht oder Löschung) geltend machen und so unerwünschte nachgelagerte Datenverarbeitungen direkt „an der Wurzel" verhindern zu können.[66]

117 Sofern es sich um eine **öffentlich zugängliche Quelle** handelt, ist auch über diesen Umstand zu informieren. Öffentlich zugänglich sind Quellen, die prinzipiell jedermann ohne besondere Zugangsvoraussetzungen – abgesehen von einer etwaig erforderlichen Registrierung und/oder Gebühr[67] – offen stehen, wie zB Telefon- und Branchenverzeichnisse, öffentliche Register, deren Einsicht keine Darlegung eines rechtlichen/berechtigten Interesses erfordert (zB Handelsregister), oder Seiten in sozialen Netzwerken, die öffentlich sichtbar sind.

118 Sollte die Angabe der konkreten Quelle nicht möglich sein, weil der Verantwortliche seinen Datenbestand aus **verschiedenen Quellen** speist, sollte nach Erwgr. 61 DS-GVO zumindest eine „allgemein gehalten[e]" Unterrichtung erfolgen. Selbiges wird man auch für allgemeine „Internetrecherchen" annehmen können. Der Europäische Datenschutzausschuss macht jedoch klar, dass es sich hierbei um einen Ausnahmetatbestand handeln soll, der insbes. dann nicht einschlägig sein soll, wenn die Identifizierung der konkreten Quelle zwar möglich, aber mit einigem (zeitlichen) Aufwand verbunden ist.[68]

h) Wird über die Empfänger(kategorien) personenbezogener Daten informiert?

119 Nach Art. 13 Abs. 1 Buchst. e DS-GVO bzw. Art. 14 Abs. 1 Buchst. e DS-GVO besteht die Verpflichtung auch über die Empfänger oder zumindest die Kategorien von Empfängern zu informieren.

---

64 Vgl. dazu auch Kühling/Buchner/Bäcker DS-GVO Art. 14 Rn. 17.

65 Vgl. dazu auch Art. 29-Datenschutzgruppe, WP 260 rev.01, 11.4.2018, S. 51 *(„Sofern dies nicht unmöglich ist, sollte die genaue Datenquelle angegeben werden.")*.

66 Vgl. Kühling/Buchner/Bäcker DS-GVO Art. 14 Rn. 19.

67 AA BeckOK DatenschutzR/Schmidt-Wudy DS-GVO Art. 14 Rn. 75, der gebührenpflichtige Datenbanken nicht als öffentlich zugängliche Quellen einstuft.

68 Vgl. Art. 29-Datenschutzgruppe, WP 260 rev.01, 11.4.2018, Rn. 60.

Der Begriff des **„Empfängers"** ist in Art. 4 Nr. 9 DS-GVO sehr weit definiert und umfasst grds. jede „natürliche oder juristische Person Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden […]". Empfänger sind demnach nicht nur **„Dritte"** iSd Art. 4 Nr. 10 DS-GVO, sondern auch **Auftragsverarbeiter,** andere (Mit-)Verantwortliche (zB im Falle von gemeinsamer Verantwortlichkeit) sowie die mit der Datenverarbeitung konkret betrauten **Untereinheiten** und **Mitarbeiter des Verantwortlichen oder Auftragsverarbeiters.**[69] Auch die **betroffene Person** selbst ist nach dem Wortlaut des Art. 4 Nr. 9 DS-GVO „Empfänger", wenn sie vom Verantwortlichen – zB im Rahmen einer Datenauskunft – ihre eigenen personenbezogen Daten offengelegt bekommt. Gleichwohl besteht insoweit keine Informationspflicht, weil die betroffene Person den Empfänger seiner Daten (= sich selbst) kennt und damit der Ausnahmetatbestand des Art. 13 Abs. 4 DS-GVO bzw. Art. 14 Abs. 5 Buchst. a DS-GVO greift. **120**

Keine Empfänger sind bzw. nicht als Empfänger behandelt werden **Behörden,** denen im Rahmen eines **Untersuchungsauftrags bzw. Auskunftsersuchens**[70] nach dem Unionsrecht oder dem Recht der Mitgliedstaaten personenbezogene Daten offengelegt werden (vgl. Art. 4 Nr. 9 aE DS-GVO). Dies hat zur Folge, dass über etwaige Datenübermittlung zur Erfüllung behördlicher Auskunftsersuchen (zB an Strafverfolgungsbehörden, Steuer- und Zollbehörden, Finanzmarktbehörden etc[71]) nicht informiert werden muss. **121**

In der Literatur ist umstritten, ob der Verantwortliche ein echtes **Wahlrecht** hat, ob er über die **konkreten Empfänger** oder nur die **Kategorien der Empfänger** informiert.[72] Diese Frage stellt sich – in gesteigerter Form – auch beim Recht auf Auskunft (vgl. Art. 15 Abs. 1 Buchst. c DS-GVO) (näher dazu → § 6 Rn. 45 ff.), insbes. wenn von der betroffenen Person Auskunft zu konkreten Empfängern begehrt wird. Zu Art. 15 Abs. 1 Buchst. c DS-GVO hat der EuGH jedenfalls kürzlich entschieden, dass der Verantwortliche grds. verpflichtet ist, der betroffenen Person die Identität der konkreten Empfänger mitzuteilen.[73] Der Europäische Datenschutzausschuss tendiert auch iRv Art. 13 Abs. 1 Buchst. e DS-GVO bzw. Art. 14 Abs. 1 Buchst. e DS-GVO – mit Blick auf den Grundsatz von Treu und Glauben – zu einer grundsätzlichen Angabe der (konkret) „benannten" Empfänger.[74] Sollten hingegen (ausnahmsweise) nur Kategorien von Empfänger angegeben werden, sollte die Kategorisierung hinreichend granular erfolgen (ua Angabe der Empfängerart (zB Dritte, Auftragsverarbeiter, etc), Industrie, Sektor, Teilsektor und Standort). **122**

Praxistipps:
Grundsätzlich sollte der Verantwortliche unter Transparenzgesichtspunkten über die **konkreten Empfänger** personenbezogener Daten informieren. **123**
Eine **Beschränkung auf die Empfängerkategorie** erscheint insbes. dann geboten bzw. möglich, wenn die konkrete Angabe der Empfänger:

- **(noch) nicht möglich** ist (zB weil vorsorglich bereits über mögliche in der Zukunft liegenden Datentransfers informiert werden soll, bei denen die konkreten Empfänger noch gar nicht feststehen),

[69] Vgl. Art. 29-Datenschutzgruppe, WP 260 rev.01, 11.4.2018, S. 46; ebenso aus der Literatur GSSV/Veil DS-GVO Art. 13, 14 Rn. 78; Kühling/Buchner/Bäcker DS-GVO Art. 13 Rn. 28; Ehmann/Selmayr/Knyrim DS-GVO Art. 13 Rn. 41, die dann aber mehrheitlich davon ausgehen, dass jedenfalls über Empfänger innerhalb der Sphäre des Verantwortlichen nicht oder nur eingeschränkt zu informieren sei.

[70] Vgl. dazu GSSV/Veil DS-GVO Art. 13, 14 Rn. 77.

[71] Vgl. dazu auch Erwgr. 31 DS-GVO.

[72] Für ein echtes Wahlrecht Plath/Kamlah DS-GVO Art. 13 Rn. 13 sowie Gola/Heckmann/Franck DS-GVO Art. 13 Rn. 20; aA dagegen Kühling/Buchner/Bäcker DS-GVO Art. 13 Rn. 30 mwH *(„Es besteht allerdings kein Wahlrecht des Verantwortlichen, wie spezifisch er die Information hält. Sind bei der Datenerhebung bereits konkrete Empfänger absehbar, so muss der Verantwortliche sie der betroffenen Person nennen.");* so wohl auch Ehmann/Selmayr/Knyrim DS-GVO Art. 13 Rn. 50.

[73] EuGH GRUR–RS 2023, 89 Rn. 51 – Österreichische Post AG.

[74] Vgl. dazu und zum Folgenden Art. 29-Datenschutzgruppe, WP 260 rev.01, 11.4.2018, S. 46 f.

- **nicht praktikabel,** dh insbes. mit einem unverhältnismäßigen Aufwand verbunden wäre (zB bei Empfängern die einem stetigen Wechsel unterliegen, wie zB die mit der Datenverarbeitung betrauten Mitarbeiter des Verantwortlichen) oder
- **berechtigten Geheimhaltungsinteressen zuwider laufen** würde (so könnte bspw. die konkrete Angabe des Anbieters eines eingesetzten Fraud Prevention Tools dazu führen, das Betrüger über den konkreten Anbieter Rückschlüsse auf die Funktionsweise des Tools ziehen und Umgehungsstrategien entwickeln).

Bei der Frage wie detailliert über die Empfänger zu informieren ist, müssen auch etwaige **datenschutzvertragliche Regelungen mit einem Empfänger** beachtet werden. Insoweit könnte unter Umständen die vertragliche Verpflichtung des übermittelnden Verantwortlichen bestehen, den Empfänger konkret zu benennen. Dies kann bspw. der Fall sein, wenn der Empfänger selbst ein Verantwortlicher iSd Art. 4 Nr. 7 DS-GVO ist (zB Auskunftei), der aus Praktikabilitätsgründen mit dem übermittelnden Verantwortlichen vereinbart hat, dass dieser – zB aufgrund seiner exklusiven Kundenbeziehung – gewissermaßen für den verantwortlichen Empfänger nach Maßgabe des Art. 14 DS-GVO initial „mitinformiert".

Sofern keine konkreten Empfänger genannt werden, sollte die **Beschreibung der Empfänger(-kategorien) nicht zu abstrakt** ausfallen (zB „verschiedene IT–Dienstleister"). Es sollte versucht werden, die Übermittlung der personenbezogenen Daten an die betreffende Empfängerkategorie für die betroffene Person möglichst nachvollziehbar zu machen. Das kann – wie vom Europäischen Datenschussausschuss vorgeschlagen – durch Zusatzangaben, wie Sektoren, Sub-Sektoren, Standorten etc. erfolgen. Eine „Rückkoppelung" der Empfänger an den Hauptzweck der Datenverarbeitung, zu dessen Erfüllung die personenbezogenen Daten an die jeweilige Empfängerkategorie übermittelt werden, sorgt ebenfalls für ein Mehr an Transparenz gegenüber der bloßen Auflistung von Empfängerkategorien.

i) Wird über (beabsichtigte) Übermittlungen von personenbezogenen Daten in Drittländer informiert?

124 Nach Art. 13 Abs. 1 Buchst. f DS-GVO bzw. Art. 14 Abs. 1 Buchst. f DS-GVO ist die betroffene Person auch darüber zu informieren, ob eine Übermittlung ihrer personenbezogenen Daten an einen Empfänger in einem Drittland[75] bzw. eine internationale Organisation geplant ist (eingehender zu den rechtlichen Anforderungen an die Übermittlung von personenbezogenen Daten in Drittländer → § 12 Rn. 3 ff.).

125 Unter einem **„Drittland"** versteht die DS-GVO einen Staat, der weder zur Europäischen Union (EU) noch zum Europäischen Wirtschaftsraum[76] gehört.[77]

126 Eine **internationale Organisation** ist gem. Art. 4 Nr. 26 DS-GVO „eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde."

127 Eine **Übermittlung** an einen Empfänger in einem Drittland setzt nicht zwingend voraus, dass die personenbezogenen Daten physisch im Drittland gespeichert sein müssen. Eine

[75] Bei der etwas abweichenden Formulierung in Art. 13 Abs. 1 Buchst. f DS-GVO („an ein Drittland") handelt es sich offensichtlich um ein Redaktionsversehen; s. dazu bereits Gola/Heckmann/Franck DS-GVO Art. 13 Rn. 22.

[76] Zum EWR gehören neben den EU–Mitgliedstaaten derzeit Island, Liechtenstein und Norwegen. Seit 20.7.2018 gilt die DS-GVO auch in diesen drei Staaten; vgl. dazu die Pressemitteilung abrufbar unter der URL: https://www.efta.int/media-resources/news/general-data-protection-regulation-gdpr-entered-force-eea (letzter Abruf: 3.5.2026).

[77] DSK, Kurzpapier Nr. 4: Datenübermittlung in Drittländer, 22.7.2019, S. 1.

solche Drittlandübermittlung liegt vielmehr auch dann vor, wenn der Empfänger im Drittland Zugriff auf die innerhalb der EU bzw. des EWR gespeicherten personenbezogenen Daten hat.[78]

Sofern eine Übermittlung von personenbezogenen Daten an einen Empfänger in einem Drittland geplant ist, sollte nach Auffassung des Europäischen Datenschutzausschusses unter Transparenzgesichtspunkten grds. auch das betreffende Drittland **namentlich genannt** werden. **128**

aa) Wird insoweit auch über das Vorliegen oder Fehlen eines Angemessenheitsbeschlusses informiert?

Ferner muss in einem solchen Fall gem. Art. 13 Abs. 1 Buchst. f DS-GVO bzw. Art. 14 Abs. 1 Buchst. f DS-GVO auch darüber informiert werden, ob für das betreffende Drittland ein Angemessenheitsbeschluss der EU-Kommission (vgl. Art. 45 DS-GVO) vorhanden ist oder nicht. **129**

Auf Basis des Art. 45 DS-GVO sind bislang erst vier **Beschlüsse der EU-Kommission** ergangen, in denen Japan[79], dem Vereinten Königreich (befristet bis Ende 2025)[80], Südkorea[81] sowie den unter dem EU-U. S. Data Privacy Framework zertifizierten Unternehmen[82] ein angemessenes Datenschutzniveau bestätigt wurden. Darüber hinaus bleiben die auf der Grundlage der alten Datenschutz-RL getroffenen Angemessenheitsentscheidungen der EU–Kommission gem. Art. 45 Abs. 9 DS-GVO weiterhin in Kraft, bis sie durch einen Beschluss der EU–Kommission geändert, ersetzt oder aufgehoben werden. Für folgende Länder sind nach dieser Regelung gegenwärtig noch Angemessenheitsentscheidungen der EU–Kommission (nach altem Recht) in Kraft: Andorra, Argentinien, Färöer-Inseln, Guernsey, Isle of Man, Israel, Jersey, Kanada (nur kommerzielle Organisationen), Neuseeland, Schweiz und Uruguay.[83] **130**

Die in der Praxis häufig vorkommende Datenübermittlung an Empfänger (zB Cloud-Provider) in den USA können hingegen zwischenzeitlich nicht (mehr) über einen solchen Angemessenheitsbeschluss legitimiert werden. Der damalige Durchführungsbeschluss (EU) 2016/1250 der Kommission (B (EU) 2016/1250), das sog. **EU-US Privacy Shield,** wurde vom EuGH in der sog. „Schrems-II"-Entscheidung im Juli 2020 für ungültig erklärt (näher dazu → § 12 Rn. 24 ff.).[84] Mit dem EU-U. S. Data Privacy Framework ist aber seit Juli 2023 wieder ein Angemessenheitsbeschluss für entsprechend zertifizierte U. S. Unternehmen vorhanden. **131**

---

78 BeckOK DatenschutzR/Juarez DS-GVO Art. 44 Rn. 15.

79 Durchführungsbeschluss (EU) 2019/419 der Kommission vom 23. Januar 2019 nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen (ABl. 2019 L 76, 1).

80 Durchführungsbeschluss (EU) 2021/1772 der Kommission vom 28. Juni 2021 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (ABl. 2021 L 360, 1).

81 Durchführungsbeschluss (EU) 2022/254 der Kommission vom 17. Dezember 2021 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten durch die Republik Korea im Rahmen des koreanischen Gesetzes über den Schutz personenbezogener Daten (ABl. 2021 L 44, 1).

82 Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA (ABl. 2023 L 231, 118).

83 Näher dazu Kühling/Buchner/Schröder DS-GVO Art. 45 Rn. 34 f. Die Angemessenheitsbeschlüsse sind abrufbar im Internet unter der URL: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (letzter Abruf: 3.5.2026).

84 EuGH NJW 2020, 2613.

132 Soll eine Übermittlung an einen Empfänger in einem Drittland erfolgen, für das **kein Angemessenheitsbeschluss** der EU–Kommission vorhanden ist, muss auch über diese **Negativtatsache informiert** werden.

bb) Ist bei Fehlen eines Angemessenheitsbeschlusses ein Verweis auf die geeigneten/angemessenen Garantien sowie ein Hinweis auf deren Kenntnisnahmemöglichkeit enthalten?

133 Greift kein Angemessenheitsbeschluss der EU-Kommission, steht die Übermittlung personenbezogener Daten an den betreffenden Empfänger im Drittland grds.[85] unter dem Vorbehalt **geeigneter (Datenschutz-)Garantien beim Empfänger** gem. Art. 46 DS-GVO bzw. – in Ausnahmefällen – Art. 49 Abs. 1 UAbs. 2 DS-GVO. In solchen Fällen trägt Art. 13 Abs. 1 Buchst. f DS-GVO bzw. Art. 14 Abs. 1 Buchst. f DS-GVO dem Verantwortlichen auf, die betroffenen Personen auf die konkret zur Anwendung kommenden geeigneten bzw. angemessenen Garantien aus Art. 46 f. DS-GVO bzw. Art. 49 Abs. 1 UAbs. 2 DS-GVO hinzuweisen.

134 Von besonderer Praxisrelevanz sind in diesem Zusammenhang vor allem die Garantien, die der datenimportierende Empfänger im Drittland durch den **Abschluss von EU-Standardvertragsklauseln der EU-Kommission** (näher dazu → § 12 Rn. 31 ff.) vertraglich gegenüber dem datenexportierenden Verantwortlichen aus der EU bzw. dem EWR übernimmt (Art. 46 Abs. 2 Buchst. c DS-GVO). Der Inhalt dieser Standardvertragsklauseln (= Garantien) ist von der EU-Kommission vorgegeben und darf von den Parteien nicht abgeändert werden. Wird die Drittlandübermittlung durch Standardvertragsklauseln „abgesichert", sollte auf die im konkreten Fall zur Anwendung kommenden EU-Standardvertragsklauseln[86] sowie etwaige **ergänzende vertragliche, organisatorische und/oder technische Maßnahmen** (näher dazu → § 12 Rn. 50 ff.) hingewiesen werden.

135 Insbes. bei großen international tätigen Konzernen können die geeigneten Garantien auch in Form von **verbindlichen internen Datenschutzvorschriften** (Art. 46 Abs. 2 Buchst. b DS-GVO iVm Art. 47 DS-GVO) (näher dazu → § 12 Rn. 55 ff.) oder **genehmigten Verhaltensregeln** (Art. 46 Abs. 2 Buchst. e DS-GVO iVm Art. 40 DS-GVO) (näher dazu → § 12 Rn. 63) vorliegen, auf die dann in den Datenschutzinformationen als Legitimationsgrundlage Bezug zu nehmen ist. Was die Art der Kenntnisnahmemöglichkeit durch die betroffene Person anbelangt, so ergibt sich diese bei verbindlichen internen Datenschutzvorschriften aus den diesbezüglichen Regelungen der Datenschutzvorschriften selbst (vgl. Art. 47 Abs. 2 Buchst. g DS-GVO). Regelmäßig werden die verbindlichen internen Datenschutzvorschriften auf der Unternehmenswebsite veröffentlicht sein. Genehmigte Verhaltensregeln sind hingegen von der genehmigenden Datenschutzaufsichtsbehörde bzw. vom Europäischen Datenschutzausschuss in ein Verzeichnis aufzunehmen und zu veröffentlichen (vgl. Art. 40 Abs. 6 DS-GVO bzw. Art. 40 Abs. 11 DS-GVO). Auf die betreffenden Websites kann dann in den Datenschutzinformationen verwiesen/verlinkt werden.

136 Greifen (auch) keine der in Art. 46 DS-GVO genannten Garantien, ist ein Drittlandtransfer nur noch in den **Ausnahmefällen des Art. 49 DS-GVO** (näher dazu → § 12 Rn. 65 ff.) zulässig. Jedenfalls für den Ausnahmetatbestand des Art. 49 Abs. 1 UAbs. 2 DS-GVO („zwingende berechtigte Interessen des Verantwortlichen") muss der Verantwortliche gem. Art. 13 Abs. 1 Buchst. f DS-GVO bzw. Art. 14 Abs. 1 Buchst. f DS-GVO auch über

[85] Nur in Ausnahmefällen (vgl. Art. 49 Abs. 1 UAbs. 1 DS-GVO) können personenbezogene Daten auch ohne das Vorliegen solcher Garantien an einen Empfänger in einem Drittland ohne angemessenes Datenschutzniveau übermittelt werden.

[86] Die verschiedenen EU–Standardvertragsklausel Sets bzw. Module sind abrufbar unter der URL: https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_en (letzter Abruf: 3.5.2026).

die insoweit vorzusehenden „angemessenen Garantien" informieren. Darüber hinaus ist die betroffene Person in diesem Fall gem. Art. 49 Abs. 1 UAbs. 2 S. 4 DS-GVO auch über die zwingenden berechtigten Interessen an diesem Drittlandtransfer zu informieren. Jedenfalls nach dem Wortlaut der Art. 13 Abs. 1 Buchst. f DS-GVO und Art. 14 Abs. 1 Buchst. f DS-GVO besteht in den Fällen, in denen der Drittlandtransfer auf Art. 49 Abs. 1 UAbs. 1 Buchst. a – g DS-GVO gestützt wird, keine diesbezügliche Informationspflicht. Der Europäische Datenschutzausschuss geht jedoch gleichwohl davon aus, dass auch in diesen Fällen über die Legitimationsgrundlage zu informieren ist.[87]

j) Wird über die Speicherdauer bzw. die Kriterien zur Festlegung der Speicherdauer informiert?

Nach Art. 13 Abs. 2 Buchst. a DS-GVO bzw. Art. 14 Abs. 2 Buchst. a DS-GVO ist der betroffenen Person grds. auch die konkrete Speicherdauer mitzuteilen. Sollte dies nicht möglich sein, ist zumindest über die Kriterien für die Festlegung der Speicherdauer zu informieren. **137**

Da die Speicherdauer nach dem Grundsatz der Speicherbegrenzung gem. Art. 5 Abs. 1 Buchst. e DS-GVO **zweckbezogenen** ist, sollten die Informationen zur Speicherdauer jeweils bezogen auf einen bestimmten primären Verarbeitungszweck (zB Vertragsdurchführung) sowie etwaiger damit in Verbindung stehender Sekundär- bzw. Folgezwecke (wie zB Speicherung zur Geltendmachung, Ausübung, Verteidigung von Rechtsansprüchen während der Gewährleistungs-/Verjährungsfristen sowie ggf. darüber hinaus zur Erfüllung handels- und steuerrechtlicher Aufbewahrungsfristen erfolgen. Wichtig ist gerade in Fällen von Sekundär- bzw. Folgezwecken, dass die betroffene Person auch über den Startzeitpunkt des (Folge-)Zwecks und der daran gekoppelten Speicherfrist informiert wird. **138**

Formulierungsbeispiel: Speicherdauer von personenbezogener Daten abgelehnter Bewerber

„Im Falle einer erfolglosen Bewerbung speichern wir ihre Bewerberdaten bis zu zwei Monate nach Absage zum Zwecke der Verteidigung von etwaig geltend gemachten Ansprüchen der abgelehnten Bewerbenden nach dem allgemeinen Gleichbehandlungsgesetz." **139**

Eine Information zur **absoluten Speicherdauer von Daten(-kategorien)** wird dagegen aufgrund der unterschiedlichen Zwecke, zu denen viele Daten(-kategorien) (wie zB Stamm- oder Kontaktdaten) regelmäßig verarbeitet werden, **oftmals nicht oder nur mit unverhältnismäßigen Aufwand möglich** sein. Es erscheint insoweit ausreichend, wenn die Speicherdauer jeweils **relativ zum betreffenden Verarbeitungszweck** erfolgt (→ Rn. 138),[88] verbunden mit dem Hinweis, dass die betreffenden Daten(-kategorien) auch nach Ablauf der Speicherfrist für den betreffenden Zweck X ggf. aufgrund eines der anderen genannten und fortbestehenden Zwecke weiter gespeichert werden. **140**

Nach Auffassung des Europäischen Datenschutzausschusses soll es jedoch nicht ausreichen, wenn sich die Information im Wesentlichen auf die Wiedergabe des Grundsatzes der Speicherbegrenzung beschränkt, dh die betroffene Person nur darüber informiert wird, dass ihre Daten „solange wie nötig für die legitimen Zwecke der Verarbeitung" gespeichert bleiben.[89] **141**

[87] Vgl. Art. 29-Datenschutzgruppe, WP 260 rev.01, 11.4.2018, S. 47 f. *(„Ausnahmen und Garantien nach Art. 49").*

[88] Diesen Ansatz erkennt auch Art. 29-Datenschutzgruppe, WP 260 rev.01, 11.4.2018, S. 49 an *(„Gegebenenfalls sollten verschiedene Speicherfristen – und bei Bedarf auch Archivfristen – für unterschiedliche Kategorien personenbezogener Daten und/oder unterschiedliche Verarbeitungszwecke vorgesehen werden.").*

[89] Art. 29-Datenschutzgruppe, WP 260 rev.01, 11.4.2018, S. 49.

k) Wird über die einschlägigen Betroffenenrechte informiert?

142 Der Verantwortliche muss die betroffenen Personen nach Art. 13 Abs. 2 Buchst. b, c DS-GVO bzw. Art. 14 Abs. 2 Buchst. c, d DS-GVO auch auf ihre nachfolgend unter → Rn. 146–156 aufgezählten **Betroffenenrechte** (näher dazu → §§ 6–8), sofern diese **im Einzelfall auch bestehen (können),** hinweisen. Kann ausgeschlossen werden, dass die Voraussetzungen eines bestimmten Betroffenenrechts vorliegen werden, muss und sollte über dieses Betroffenenrecht auch nicht informiert werden.[90] Dies kann bspw. im Fall der Widerspruchsrechte aus Art. 21 DS-GVO der Fall sein, wenn der Verantwortliche keine Datenverarbeitungen auf Basis der Rechtsgrundlagen des Art. 6 Abs. 1 S. 1 Buchst. e – f DS-GVO oder zumindest keine Datenverarbeitungen zum Zwecke der Direktwerbung vornimmt und somit keine Widerspruchsrechte nach Art. 21 Abs. 1 DS-GVO und/oder Art. 21 Abs. 2 DS-GVO bestehen.

143 Was den **Detaillierungsgrad der Information über die (bestehenden) Betroffenenrechte** anbelangt, so reicht es nach dem Wortlaut der Art. 13 Abs. 2 Buchst. b, c DS-GVO und Art. 14 Abs. 2 Buchst. c, d DS-GVO aus, wenn abstrakt – ggf. unter Verweis auf den jeweiligen DS-GVO-Artikel – über das Bestehen dieser Rechte informiert wird. Es ist insoweit nicht erforderlich, dass der Verantwortliche hier mehr oder weniger den Gesetzeswortlaut der Betroffenenrechte wiedergibt.[91] Gleichwohl sollte der Verantwortliche – auch aus eigenem Interesse – zumindest über die **wesentlichen Voraussetzungen für die Geltendmachung** sowie über **etwaige Einschränkungen dieser Rechte** informieren, um sich dann im Nachgang nicht einer Fülle von unbegründeten Anträgen auf Wahrnehmung von Betroffenenrechten ausgesetzt zu sehen, die auf eine Fehlvorstellung der betroffenen Person bezüglich der Voraussetzungen und des Umfangs ihrer Betroffenenrechte zurückzuführen sind. Das gilt insbes. für das Recht auf Löschung gem. Art. 17 DS-GVO. Hier besteht bei juristischen Laien in der Praxis der weitverbreitete Irrtum, dass jederzeit *alle* personenbezogenen Daten gelöscht werden könnten, was aber insbes. aufgrund bestehender (langer) Aufbewahrungs- und Dokumentationspflichten in vielen Fällen nicht möglich ist, mit der Folge, dass entsprechende Begehren zumindest in Teilen abgelehnt werden müssen.

144 In jedem Fall muss der Verantwortliche darüber informieren, **auf welchem Wege** die betroffene Person die genannten Rechte geltend machen kann. Soll die Geltendmachung per Brief und/oder E-Mail[92] erfolgen, ist die betreffende (E-Mail-)Adresse, an welche die Begehren zu richten sind, anzugeben. In diesem Zusammenhang sollte dann auch geregelt werden, **welche Angaben** die betroffene Person zu ihrer Person und zu ihrem Begehren machen sollten, um die betroffene Person zu **verifizieren** sowie die Anfrage richtig **einordnen** und umsetzen zu können.

145 Unter Umständen können bestimmte Betroffenenrechte auch im Wege des **„Self-Service"** direkt umgesetzt werden. Sofern dies der Fall ist, sollte die betroffene Person auch über diese Möglichkeiten informiert werden (zB Abmeldung von E-Mail-Werbung an Bestandskunden (= Widerspruch gem. § 7 Abs. 3 UWG/Art. 21 Abs. 2 DS-GVO) via Abmelde-Link in Werbemails; Möglichkeit zur Beauskunftung, Berichtigung und Löschung (bestimmter) personenbezogenen Daten über einen etwaig vorhandenen Kundenaccount etc).

---

[90] Kühling/Buchner/Bäcker DS-GVO Art. 13 Rn. 37; Paal/Pauly/Paal/Hennemann DS-GVO Art. 13 Rn. 27a; Plath/Kamlah DS-GVO Art. 13 Rn. 19.

[91] So auch Plath/Kamlah DS-GVO Art. 13 Rn. 19.

[92] Nach Erwgr. 59 DS-GVO „sollte" der Verantwortliche auch eine elektronische Möglichkeit zur Antragsstellung bereitstellen.