Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO

Version 2.0

Angenommen am 7. Juli 2021

Versionsverlauf

Version 2.0	7. Juli 2021	Annahme der Leitlinien nach öffentlicher Konsultation
Version 1.0	2. September 2020	Annahme der Leitlinien zur öffentlichen Konsultation

ZUSAMMENFASSUNG

Die Begriffe „Verantwortlicher“, „gemeinsam Verantwortliche“ und „Auftragsverarbeiter“ spielen bei der Anwendung der Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) eine entscheidende Rolle, da sie bestimmen, wer für die Einhaltung der verschiedenen Datenschutzvorschriften verantwortlich ist und wie betroffene Personen ihre Rechte in der Praxis ausüben können. Die genaue Bedeutung dieser Begriffe und die Kriterien für ihre richtige Auslegung müssen im gesamten Europäischen Wirtschaftsraum (EWR) hinreichend klar und kohärent sein.

Die Begriffe „Verantwortlicher“, „gemeinsam Verantwortliche“ und „Auftragsverarbeiter“ sind *funktionelle* Konzepte, da sie darauf abzielen, Verantwortlichkeiten entsprechend den tatsächlichen Rollen der Parteien zuzuweisen, und Konzepte *eigener Prägung* in dem Sinne, dass sie in erster Linie im Einklang mit dem EU-Datenschutzrecht auszulegen sind.

Verantwortlicher

Grundsätzlich gibt es keine Beschränkung hinsichtlich der Art der Einrichtung, die die Rolle des Verantwortlichen übernehmen kann; in der Praxis handelt es sich jedoch in der Regel um die Organisation als solche und nicht um eine natürliche Person innerhalb der Organisation (wie den Geschäftsführer, einen Mitarbeiter oder ein Mitglied des Leitungsorgans), die als Verantwortlicher fungiert.

Ein Verantwortlicher ist eine Stelle, die über bestimmte Schlüsselelemente der Verarbeitung *entscheidet*. Die Verantwortlichkeit kann im Gesetz geregelt sein oder sich aus einer Analyse der tatsächlichen Elemente und der Umstände des Falls ergeben. Bestimmte Verarbeitungstätigkeiten können als naturgemäß mit der Rolle einer Einrichtung verbunden angesehen werden (also der des Arbeitgebers gegenüber Arbeitnehmern, des Verlegers gegenüber Abonnenten oder der einer Vereinigung gegenüber ihren Mitgliedern). Häufig können die Vertragsbedingungen dazu beitragen, den Verantwortlichen zu ermitteln, auch wenn sie nicht in allen Fällen ausschlaggebend sind.

Ein Verantwortlicher legt die Zwecke und Mittel der Verarbeitung fest, d. h. das „Warum“ und das „Wie“ der Verarbeitung. Der Verantwortliche muss sowohl über die Zwecke als auch über die Mittel entscheiden. Einige eher praktische Aspekte der Umsetzung („unwesentliche Mittel“) können jedoch dem Auftragsverarbeiter überlassen werden. Es ist nicht erforderlich, dass der Verantwortliche tatsächlich Zugang zu den verarbeiteten Daten hat, um als Verantwortlicher eingestuft zu werden.

Gemeinsam Verantwortliche

Die Einstufung als gemeinsam Verantwortlicher kommt in Betracht, wenn mehr als ein Akteur an der Verarbeitung beteiligt ist. Mit der DSGVO werden besondere Vorschriften für gemeinsam Verantwortliche eingeführt und ein Rahmen für die Beziehungen zwischen ihnen abgesteckt. Das übergeordnete Kriterium für das Bestehen einer gemeinsamen Verantwortlichkeit ist die gemeinsame Beteiligung von zwei oder mehr Stellen an der Festlegung der Zwecke und Mittel eines Verarbeitungsvorgangs. Die gemeinsame Beteiligung kann in Form einer *gemeinsam getroffenen Entscheidung* von zwei oder mehr Stellen erfolgen oder aus *konvergierenden Entscheidungen* von zwei oder mehr Stellen resultieren, wenn sich die Entscheidungen ergänzen und erforderlich sind, damit die Verarbeitung so erfolgen kann, dass sie spürbare Auswirkungen auf die Bestimmung der Zwecke und Mittel der Verarbeitung haben. Ein wichtiges Kriterium ist, dass die Verarbeitung ohne die Beteiligung beider Parteien nicht möglich wäre, und zwar in dem Sinne, dass die Verarbeitungen jeder der Parteien untrennbar, d. h. unauflösbar miteinander verbunden sind. Die gemeinsame Beteiligung muss einerseits die Festlegung der Zwecke und andererseits die Festlegung der Mittel umfassen.

Auftragsverarbeiter

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Für die Einstufung als Auftragsverarbeiter gelten zwei grundlegende Voraussetzungen: Er muss gegenüber dem Verantwortlichen eine eigenständige Einheit bilden und personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten.

Der Auftragsverarbeiter darf die Daten nur nach den Weisungen des Verantwortlichen verarbeiten. Die Weisungen des Verantwortlichen können dennoch einen gewissen Ermessensspielraum in der Frage lassen, wie den Interessen des Verantwortlichen am besten gedient werden kann, sodass der Auftragsverarbeiter die am besten geeigneten technischen und organisatorischen Mittel auswählen kann. Ein Auftragsverarbeiter verstößt jedoch gegen die DSGVO, wenn er über die Weisungen des Verantwortlichen hinausgeht und beginnt, seine eigenen Zwecke und Mittel für die Verarbeitung festzulegen. Der Auftragsverarbeiter gilt dann in Bezug auf diese Verarbeitung als Verantwortlicher und kann mit Sanktionen belegt werden, wenn er über die Weisungen des Verantwortlichen hinausgeht.

Beziehung zwischen Verantwortlichem und Auftragsverarbeiter

Ein Verantwortlicher darf nur mit Auftragsverarbeitern arbeiten, die hinreichende Garantien für die Durchführung geeigneter technischer und organisatorischer Maßnahmen bieten, damit die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt. Zu berücksichtigende Elemente könnten sein: das Fachwissen des Auftragsverarbeiters (z. B. technisches Fachwissen in Bezug auf Sicherheitsmaßnahmen und Verletzungen des Schutzes personenbezogener Daten); die Zuverlässigkeit des Auftragsverarbeiters; die Ressourcen des Auftragsverarbeiters und die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch den Auftragsverarbeiter.

Jede Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter muss auf der Grundlage eines Vertrags oder eines anderen verbindlichen Rechtsinstruments erfolgen, der/das schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann. Verantwortlicher und Auftragsverarbeiter können sich dafür entscheiden, ihren eigenen Vertrag auszuhandeln, der alle obligatorischen Elemente enthält, oder sich ganz oder teilweise auf Standardvertragsklauseln stützen.

In der DSGVO sind die Elemente aufgeführt, die in der Auftragsverarbeitungsvereinbarung geregelt werden müssen. In der Auftragsverarbeitungsvereinbarung sollten jedoch nicht lediglich die Bestimmungen der DSGVO wiederholt werden; vielmehr sollte sie spezifischere, konkrete Informationen darüber enthalten, wie die Vorgaben eingehalten werden und welches Sicherheitsniveau für die Verarbeitung personenbezogener Daten, die Gegenstand der Auftragsverarbeitungsvereinbarung sind, erforderlich ist.

Beziehung zwischen gemeinsam Verantwortlichen

Gemeinsam Verantwortliche legen in einer Vereinbarung in transparenter Weise ihre jeweiligen Zuständigkeiten für die Einhaltung der sich aus der Verordnung ergebenden Verpflichtungen fest. Bei der Festlegung ihrer jeweiligen Zuständigkeiten gilt besondere Aufmerksamkeit der Ausübung der Rechte der betroffenen Person und den Informationspflichten. Darüber hinaus sollte sich die Zuständigkeitsverteilung auch auf andere Pflichten des Verantwortlichen erstrecken, etwa in Bezug auf die allgemeinen Datenschutzgrundsätze, die Rechtsgrundlage, Sicherheitsmaßnahmen, die Pflicht

zur Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzungen, die Heranziehung von Auftragsverarbeitern, Datenübermittlungen an Drittländer und Kontakte zu betroffenen Personen und Aufsichtsbehörden.

Jeder der gemeinsam Verantwortlichen hat die Pflicht sicherzustellen, dass er über eine Rechtsgrundlage für die Verarbeitung verfügt und dass die Daten nicht in einer Weise weiterverarbeitet werden, die mit den Zwecken unvereinbar ist, für die sie ursprünglich von dem Verantwortlichen, der die Daten weitergibt, erhoben wurden.

Die Form der Vereinbarung zwischen gemeinsam Verantwortlichen ist durch die DSGVO nicht vorgegeben. Im Interesse der Rechtssicherheit, zwecks Transparenz und zur Erfüllung der Rechenschaftspflicht empfiehlt der EDSA, eine solche Vereinbarung in Form eines verbindlichen Dokuments zu treffen, wie eines Vertrags oder eines anderen verbindlichen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem die Verantwortlichen unterliegen.

Die Vereinbarung muss die jeweiligen Rollen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln, und der wesentliche Inhalt der Vereinbarung ist der betroffenen Person zur Verfügung zu stellen.

Ungeachtet der Bestimmungen der Vereinbarung können betroffene Personen ihre Rechte bei und gegenüber jedem einzelnen der gemeinsam Verantwortlichen geltend machen. Weder in Bezug auf die Frage der Einstufung der Parteien als gemeinsam Verantwortliche noch in Bezug auf die benannte Kontaktstelle sind die Aufsichtsbehörden an die Festlegungen der Vereinbarung gebunden.

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG 3

EINLEITUNG 8

TEIL I – BEGRIFFE 9

1 ALLGEMEINE BEMERKUNGEN 9

2 DEFINITION DES BEGRIFFS „VERANTWORTLICHER“ 11

2.1 Definition des Begriffs „Verantwortlicher“ 11

2.1.1 „Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle“ 11

2.1.2 „entscheidet“ 12

2.1.3 „Allein oder gemeinsam mit anderen“ 16

2.1.4 „Zwecke und Mittel“ 16

2.1.5 „Der Verarbeitung von personenbezogenen Daten“ 19

3 DEFINITION DES BEGRIFFS „GEMEINSAM VERANTWORTLICHE“ 21

3.1 Definition des Begriffs „gemeinsam Verantwortliche“ 21

3.2 Vorliegen gemeinsamer Verantwortlichkeit 21

3.2.1 Allgemeine Erwägungen 21

3.2.2 Beurteilung der gemeinsamen Beteiligung 22

3.2.3 Situationen, in denen keine gemeinsame Verantwortlichkeit vorliegt 28

4 DEFINITION DES AUFTRAGSVERARBEITERS 29

5 DEFINITION DES BEGRIFFS „DRITTER/EMPFÄNGER“ 33

TEIL II – FOLGEN DER ZUWEISUNG UNTERSCHIEDLICHER ROLLEN 35

1 BEZIEHUNG ZWISCHEN VERANTWORTLICHEM UND AUFTRAGSVERARBEITER 35

1.1 Auswahl des Auftragsverarbeiters 36

1.2 Form des Vertrags oder sonstigen Rechtsinstruments 37

1.3 Inhalt des Vertrags oder des sonstigen Rechtsinstruments 40

1.3.1 Der Auftragsverarbeiter darf Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten (Artikel 28 Absatz 3 Buchstabe a DSGVO) 41

1.3.2 Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Artikel 28 Absatz 3 Buchstabe b DSGVO) 42

1.3.3 Der Auftragsverarbeiter muss alle nach Artikel 32 erforderlichen Maßnahmen ergreifen (Artikel 28 Absatz 3 Buchstabe c DSGVO). 43

1.3.4 Der Auftragsverarbeiter muss die in Artikel 28 Absätze 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhalten (Artikel 28 Absatz 3 Buchstabe d DSGVO). 44

1.3.5 Der Auftragsverarbeiter unterstützt den Verantwortlichen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person nachzukommen (Artikel 28 Absatz 3 Buchstabe e DSGVO). 44

1.3.6 Der Auftragsverarbeiter muss den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützen (Artikel 28 Absatz 3 Buchstabe f DSGVO). ..45

1.3.7 Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen löschen oder zurückgeben (Artikel 28 Absatz 3 Buchstabe g DSGVO). 46

1.3.8 Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 niedergelegten Pflichten zur Verfügung und ermöglicht und trägt zu Überprüfungen – einschließlich Inspektionen – bei, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden (Artikel 28 Absatz 3 Buchstabe h DSGVO). 47

1.4 Weisungen, die gegen das Datenschutzrecht verstoßen 48

1.5 Auftragsverarbeiter, der die Verarbeitungszwecke und -mittel bestimmt 49

1.6 Unterauftragsverarbeiter 49

2 Folgen GEMEINSAMER VERANTWORTLICHKEIT 51

2.1 Transparente Festlegung der jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen für die Erfüllung der Verpflichtungen aus der DSGVO 51

2.2 Die Zuweisung der Zuständigkeiten muss im Wege einer Vereinbarung erfolgen 54

2.2.1 Form der Vereinbarung 54

2.2.2 Pflichten gegenüber betroffenen Personen 55

2.3 Pflichten gegenüber den Datenschutzbehörden 56

Der Europäische Datenschutzausschuss

gestützt auf Artikel 70 Absatz 1 Buchstabe e der 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 (im Folgenden „DSGVO“ oder „Verordnung“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung,[1]

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

In der Erwägung, dass im Zuge der Vorarbeiten zu diesen Leitlinien zur Ermittlung der dringlichsten Probleme Beiträge von Interessenträgern sowohl schriftlich als auch bei einer Veranstaltung der Interessenträger eingeholt wurden;

HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN:

EINLEITUNG

1. Dieses Dokument soll als Orientierungshilfe zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ auf der Grundlage der Begriffsbestimmungen in Artikel 4 und der Bestimmungen über Verpflichtungen in Kapitel IV DSGVO dienen. Hauptziel ist es, die Bedeutung der Begriffe zu klären sowie die verschiedenen Rollen und Zuständigkeiten zwischen diesen Akteuren zu klären.

2. Das Konzept des Verantwortlichen und seine Wechselwirkung mit dem Konzept des Auftragsverarbeiters spielen bei der Anwendung der DSGVO eine entscheidende Rolle, da sie bestimmen, wer für die Einhaltung der verschiedenen Datenschutzvorschriften verantwortlich ist und wie betroffene Personen ihre Rechte in der Praxis ausüben können. Mit der DSGVO wird ausdrücklich der Grundsatz der Rechenschaftspflicht eingeführt, d. h. der Verantwortliche ist für die Einhaltung der in Artikel 5 genannten Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und muss in der Lage sein, die Einhaltung dieser Grundsätze nachzuweisen. Darüber hinaus werden mit der DSGVO detailliertere Vorschriften für den Einsatz von Auftragsverarbeitern eingeführt, und einige Bestimmungen über die Verarbeitung personenbezogener Daten richten sich nicht nur an Verantwortliche, sondern auch an Auftragsverarbeiter.

3. Es ist daher von allergrößter Bedeutung, dass die genaue Bedeutung dieser Begriffe und die Kriterien für ihre korrekte Verwendung in der gesamten Europäischen Union und im EWR hinreichend klar und einheitlich sind.

[1] Soweit hierin auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

4. Die Artikel 29-Datenschutzgruppe hat in ihrer Stellungnahme 1/2010 (WP 169)[2] Hilfestellung zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ mit Klarstellungen und konkreten Beispielen zu diesen Begriffen geboten. Seit dem Inkrafttreten der DSGVO wurde immer wieder gefragt, inwieweit die DSGVO zu Änderungen bei den Konzepten des „Verantwortlichen“ und des „Auftragsverarbeiters“ und deren jeweiligen Rollen geführt hat. Fragen wurden insbesondere zum Inhalt und zu den Auswirkungen des Konzepts der gemeinsamen Verantwortlichkeit (z. B. gemäß Artikel 26 DSGVO) und zu den spezifischen Verpflichtungen für Auftragsverarbeiter gemäß Kapitel IV (z. B. gemäß Artikel 28 DSGVO) gestellt. Der EDSA erkennt an, dass die konkrete Anwendung der Konzepte einer weiteren Klärung bedarf, und erachtet es nun für notwendig, ausführlichere und spezifischere Leitlinien vorzulegen, um einen kohärenten und harmonisierten Ansatz in der gesamten EU und im EWR zu gewährleisten. Die vorliegenden Leitlinien ersetzen die ältere Stellungnahme der Artikel 29-Datenschutzgruppe zu diesen Begriffen (WP 169).

5. In Teil I dieser Leitlinien werden die Definitionen der Begriffe „Verantwortlicher“, „gemeinsam Verantwortliche“, „Auftragsverarbeiter“ und „Dritter/Empfänger“ erörtert. In Teil II wird näher auf die Folgen eingegangen, die sich aus den unterschiedlichen Rollen von Verantwortlichem, gemeinsam Verantwortlichen und Auftragsverarbeiter ergeben.

TEIL I – BEGRIFFE

1 ALLGEMEINE BEMERKUNGEN

6. In Artikel 5 Absatz 2 DSGVO wird ausdrücklich der Grundsatz der Rechenschaftspflicht eingeführt; er bedeutet, dass

   - der Verantwortliche *für die Einhaltung* der in Artikel 5 Absatz 1 DSGVO festgelegten Grundsätze *verantwortlich ist*, und dass
   - der Verantwortliche *nachweisen* können muss, dass er die in Artikel 5 Absatz 1 DSGVO festgelegten Grundsätze *einhält*.

   Dieser Grundsatz wird in einer ausführlichen Stellungnahme der Artikel 29-Datenschutzgruppe[3] beschrieben und soll hier nicht im Einzelnen erörtert werden.

7. Mit der Aufnahme des Grundsatzes der Rechenschaftspflicht in die DSGVO und seiner Verankerung als zentraler Grundsatz sollte betont werden, dass Verantwortliche geeignete und wirksame Maßnahmen ergreifen müssen und in der Lage sein müssen, deren Einhaltung nachzuweisen. [4]

8. Der Grundsatz der Rechenschaftspflicht wird in Artikel 24 weiter ausgeführt, wonach der Verantwortliche geeignete technische und organisatorische Maßnahmen umsetzen muss, um sicherzustellen und den **Nachweis dafür erbringen** zu können, dass die Verarbeitung gemäß der DSGVO erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert. Der Grundsatz der Rechenschaftspflicht hat auch Eingang gefunden in Artikel 28, in dem die Pflichten des Verantwortlichen bei der Inanspruchnahme eines Auftragsverarbeiters festgelegt sind.

[2] Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, angenommen am 16. Februar 2010, WP 169.
[3] Stellungnahme 3/2010 der Artikel 29-Datenschutzgruppe zum Grundsatz der Rechenschaftspflicht, angenommen am 13. Juli 2010, 00062/10/DE WP 173.
[4] Erwägungsgrund 74 DSGVO.

9. Der Grundsatz der Rechenschaftspflicht wendet sich unmittelbar an den Verantwortlichen. Einige der spezifischeren Vorschriften gelten jedoch sowohl für Verantwortliche als auch für Auftragsverarbeiter, wie etwa die Bestimmungen über die Befugnisse der Aufsichtsbehörden in Artikel 58. Sowohl gegen Verantwortliche als auch gegen Auftragsverarbeiter können Geldbußen verhängt werden, wenn sie den ihnen obliegenden Verpflichtungen aus der DSGVO nicht nachkommen, und beide sind gegenüber den Aufsichtsbehörden unmittelbar rechenschaftspflichtig, weil sie verpflichtet sind, geeignete Unterlagen zu führen und auf Anfrage bereitzustellen, im Falle einer Untersuchung zu kooperieren und behördliche Anordnungen zu befolgen. Bei dieser Gelegenheit wird daran erinnert, dass Auftragsverarbeiter stets die Weisungen des Verantwortlichen befolgen müssen und nur auf diese hin handeln dürfen.

10. Der Grundsatz der Rechenschaftspflicht mitsamt den weiteren spezifischeren Regeln zur Einhaltung der DSGVO und zur Verteilung der Verantwortlichkeiten erfordert es daher, die unterschiedlichen Rollen der einzelnen an der Verarbeitung personenbezogener Daten beteiligten Akteure zu definieren.

11. Allgemein lässt sich zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO bemerken, dass sich an ihnen im Vergleich zur Richtlinie 95/46/EG nichts geändert hat und dass im Großen und Ganzen die Kriterien für die Zuweisung der verschiedenen Rollen unverändert geblieben sind.

12. Die Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“ sind *funktionelle* Begriffe: Sie zielen darauf ab, Verantwortlichkeiten entsprechend den tatsächlichen Rollen der Parteien zuzuweisen.[5] Das bedeutet, dass der rechtliche Status eines Akteurs als entweder „Verantwortlicher“ oder „Auftragsverarbeiter“ grundsätzlich anhand seiner tatsächlichen Tätigkeiten in einer bestimmten Situation zu bestimmen ist und nicht von der formellen Benennung eines Akteurs als „Verantwortlicher“ oder „Auftragsverarbeiter“ (z. B. in einem Vertrag) abhängig ist.[6] Das bedeutet, dass die Zuweisung der Rollen üblicherweise aus der Analyse der faktischen Elemente oder Umstände eines Falls abzuleiten ist und als solche nicht verhandelbar ist.

13. „Verantwortlicher“ und „Auftragsverarbeiter“ sind ferner insofern Konzepte *eigener Prägung*, als externe rechtliche Quellen zwar zur Ermittlung eines für die Verarbeitung Verantwortlichen beitragen können, sie aber in erster Linie anhand des EU-Datenschutzrechts ausgelegt werden sollten. Der Begriff des Verantwortlichen sollte unbeschadet anderer – manchmal kollidierender oder sich überschneidender – Begriffe in anderen Rechtsgebieten, wie etwa dem des Urhebers oder Rechteinhabers im Bereich des Rechts des geistigen Eigentums oder des Wettbewerbsrechts, ausgelegt werden.

14. Da das grundlegende Ziel der Zuweisung der Rolle des Verantwortlichen darin besteht, die Rechenschaftspflicht und den wirksamen und umfassenden Schutz der personenbezogenen Daten sicherzustellen, sollte der Begriff „Verantwortlicher“ hinreichend weit ausgelegt werden, womit ein möglichst wirksamer und vollständiger Schutz der betroffenen Personen gefördert werden soll[7], um

[5] Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010, WP 169, S. 12.

[6] Vgl. auch die Schlussanträge des Generalanwalts Mengozzi in *Zeugen Jehovas* (C-25/17, ECLI:EU:C:2018:57, Nr. 68) (*„Hinsichtlich der Bestimmung des „für die Verarbeitung Verantwortlichen“ im Sinne der Richtlinie 95/46 neige ich zu der Auffassung [….], dass ein übermäßiger Formalismus dazu führen könnte, dass die Bestimmungen der Richtlinie 95/46 leicht umgangen werden könnten, und daher von einer eher faktischen als formalen Betrachtung auszugehen ist [….]“).*

[7] EuGH, Rechtssache C-131/12, Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, Urteil vom 13. Mai 2014, Rn. 34; EuGH, Rechtssache C-210/16, Wirtschaftsakademie Schleswig-Holstein, Urteil vom 5. Juni 2018, Rn. 28; EuGH, Rechtssache C-40/17, Fashion ID GmbH & Co.KG gegen Verbraucherzentrale NRW e.V., Urteil vom 29. Juli 2019, Rn. 66.

die volle Wirksamkeit des EU-Datenschutzrechts zu gewährleisten, Lücken zu vermeiden und eine mögliche Umgehung der Vorschriften zu verhindern, ohne gleichzeitig die Rolle des Auftragsverarbeiters zu schmälern.

2 DEFINITION DES BEGRIFFS „VERANTWORTLICHER“

2.1 Definition des Begriffs „Verantwortlicher“

15. Der Verantwortliche ist in Artikel 4 Nr. 7 DSGVO definiert als

> *„**die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle**, die **allein oder gemeinsam mit anderen über** die **Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet**; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung **nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden**“.*

16. Die Definition des Begriffs „Verantwortlicher“ umfasst fünf Hauptkomponenten, die für die Zwecke dieser Leitlinien getrennt analysiert werden sollen. Dabei handelt es sich um folgende Elemente:

- „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle“
- „entscheidet“
- „allein oder gemeinsam mit anderen“
- „Zwecke und Mittel“
- „der Verarbeitung von personenbezogenen Daten“

2.1.1 „Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle“

17. Die erste Komponente bezieht sich auf die Art der Einrichtung, die Verantwortlicher sein kann. Gemäß DSGVO kann Verantwortlicher „*eine natürliche oder juristische Person, Behörde, Agentur oder andere Stelle*“ sein. Das bedeutet, dass es grundsätzlich keine Beschränkung hinsichtlich der Art der Stelle gibt, die als Verantwortlicher auftreten kann. Es kann sich dabei um eine Organisation, aber auch um eine Einzelperson oder eine Gruppe von Einzelpersonen handeln.[8] In der Praxis ist es jedoch in der Regel die Organisation als solche und nicht eine natürliche Person innerhalb der Organisation (wie der Geschäftsführer, ein Angestellter oder ein Mitglied des Leitungsorgans), die als Verantwortlicher im Sinne der DSGVO fungiert. Bei der Datenverarbeitung innerhalb einer Unternehmensgruppe ist besonders darauf zu achten, ob eine Niederlassung als Verantwortlicher oder als Auftragsverarbeiter tätig wird, z. B. bei der Verarbeitung von Daten im Auftrag der Muttergesellschaft.

18. Manchmal benennen Unternehmen und öffentliche Stellen eine bestimmte Person, die für die Durchführung der Verarbeitungstätigkeit verantwortlich ist. Selbst wenn eine bestimmte natürliche Person benannt wird, die die Einhaltung der Datenschutzvorschriften sicherstellen soll, wird diese Person nicht Verantwortlicher sein, sondern für die juristische Person (Unternehmen oder öffentliche

[8] So vertrat der EuGH beispielsweise in seinem Urteil in *Zeugen Jehovas* (C-25/17, ECLI:EU:C:2018:551, Rn. 75) die Auffassung, dass eine Religionsgemeinschaft wie die Zeugen Jehovas gemeinsam mit ihren einzelnen Mitgliedern als für die Verarbeitung Verantwortlicher angesehen werden kann. Urteil *Zeugen Jehovas*, C-25/17, ECLI:EU:C:2018:551, Rn. 75.

Stelle) handeln, die im Falle eines Verstoßes gegen die Vorschriften in ihrer Eigenschaft als Verantwortlicher letztlich verantwortlich ist. Auch wenn eine bestimmte Abteilung oder Einheit einer Organisation die operative Verantwortung für die Einhaltung der Vorschriften bei bestimmten Verarbeitungsvorgängen trägt, bedeutet dies nicht, dass diese Abteilung oder Einheit (und nicht die Organisation als Ganzes) zum Verantwortlichen wird.

Beispiel:

Die Marketingabteilung von Unternehmen ABC startet eine Werbekampagne für die Produkte von ABC. Die Marketingabteilung entscheidet über die Art der Kampagne, die einzusetzenden Mittel (E-Mail, soziale Medien usw.), die Zielgruppe unter den Kunden und die Daten, mit deren Hilfe die Kampagne so erfolgreich wie möglich gestaltet werden kann. Selbst wenn die Marketingabteilung weitgehend unabhängig gehandelt hat, gilt das Unternehmen ABC grundsätzlich als Verantwortlicher, da die Werbekampagne vom Unternehmen ins Leben gerufen wird und im Rahmen seiner Geschäftstätigkeit und für seine Zwecke stattfindet.

19. Grundsätzlich kann davon ausgegangen werden, dass jede Verarbeitung personenbezogener Daten durch Mitarbeiter im Tätigkeitsbereich einer Organisation unter der Kontrolle dieser Organisation erfolgt.[9] In Ausnahmesituationen kann es jedoch vorkommen, dass ein Beschäftigter beschließt, personenbezogene Daten für seine eigenen Zwecke zu verwenden, wodurch die ihm erteilte Befugnis unrechtmäßig überschritten wird. (z. B. Gründung eines eigenen Unternehmens o. ä.). Daher hat die Organisation als Verantwortlicher dafür zu sorgen, dass angemessene technische und organisatorische Maßnahmen, wie z. B. Schulungen und Informationen für Mitarbeiter, ergriffen werden, um die Einhaltung der DSGVO sicherzustellen.[10]

2.1.2 „entscheidet“

20. Die zweite Komponente des Konzepts des Verantwortlichen bezieht sich auf den *Einfluss* des Verantwortlichen auf die Verarbeitung im Wege der *Ausübung von Entscheidungsbefugnis*. Verantwortlicher ist eine Stelle, die über bestimmte Schlüsselelemente der Verarbeitung *entscheidet*. Diese Verantwortlichkeit kann gesetzlich festgelegt sein oder sich aus einer Analyse des Sachverhalts und der Umstände des Falls ergeben. Es geht darum, sich mit den konkret betroffenen Verarbeitungsvorgängen zu befassen und in Erfahrung zu bringen, wer über sie bestimmt, indem zunächst folgende Fragen geprüft werden: „*Warum findet diese Verarbeitung statt?*“ und „*Wer hat beschlossen, dass die Verarbeitung für einen bestimmten Zweck erfolgen sollte?*“

Umstände, die datenschutzrechtliche Verantwortlichkeit begründen

21. Da es sich bei dem Begriff des Verantwortlichen um ein funktionales Konzept handelt, stützt er sich auf eine **Analyse des Sachverhalts anstatt auf formale Aspekte**. Um die Prüfung zu erleichtern, können bestimmte Faustregeln und praktische Vermutungen herangezogen werden, um das Verfahren zu lenken und zu vereinfachen. In den meisten Fällen lässt sich die „Entscheidungen treffende Stelle“ anhand bestimmter rechtlicher und/oder tatsächlicher Umstände, aus denen normalerweise ein „Einfluss“ abgeleitet werden kann, leicht und eindeutig identifizieren, es sei denn, andere Anhaltspunkte deuten auf das Gegenteil hin. Es lassen sich zwei Kategorien von Situationen

[9] Beschäftigte, die innerhalb einer Organisation Zugang zu personenbezogenen Daten haben, gelten im Allgemeinen nicht als „Verantwortliche“ oder „Auftragsverarbeiter“, sondern als „Personen, die unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters handeln“ im Sinne von Artikel 29 DSGVO.
[10] Artikel 24 Absatz 1 DSGVO.

unterscheiden: 1) eine Verantwortlichkeit, die sich aus *Rechtsvorschriften* ergibt, und 2) eine Verantwortlichkeit, die aus *faktischem Einfluss* herrührt.

1) *Verantwortlichkeit, die sich aus Rechtsvorschriften ergibt*

22. Es gibt Fälle, in denen eine Verantwortlichkeit aus einer ausdrücklichen rechtlichen Zuständigkeit abgeleitet werden kann, wenn z. B. der Verantwortliche oder die spezifischen Kriterien für seine Benennung nach nationalem Recht oder Unionsrecht bestimmt sind. In Artikel 4 Nr. 7 heißt es : *„...; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.*" Zwar ist in Artikel 4 Nr. 7 nur von dem „Verantwortlichen" im Singular die Rede, doch könnte es nach Auffassung des EDSA nach dem Unionsrecht oder dem Recht der Mitgliedstaaten durchaus möglich sein, mehr als einen Verantwortlichen zu benennen, möglicherweise sogar als gemeinsam Verantwortliche.

23. Ist der Verantwortliche im Gesetz explizit festgelegt, ist dies für die Bestimmung, wer als Verantwortlicher handelt, maßgeblich. Dies setzt voraus, dass der Gesetzgeber diejenige Stelle als Verantwortlichen bestimmt hat, die in der Lage ist, echte Kontrolle auszuüben. In einigen Ländern sieht das nationale Recht vor, dass Behörden im Rahmen ihrer Aufgaben für die Verarbeitung personenbezogener Daten zuständig sind.

24. In der Regel wird jedoch, anstatt den Verantwortlichen direkt zu benennen oder die Kriterien für seine Benennung festzulegen, eine Rechtsvorschrift jemandem die Aufgabe zuweisen oder die Verpflichtung auferlegen, bestimmte Daten zu erheben und zu verarbeiten. In diesen Fällen ist der Zweck der Verarbeitung häufig im Gesetz bestimmt. Verantwortlicher ist normalerweise derjenige, der nach dem Gesetz diesen Zweck zu erreichen, diese öffentliche Aufgabe wahrzunehmen hat. Dies wäre beispielsweise der Fall, wenn eine Stelle, die mit bestimmten im öffentlichen Interesse liegenden Aufgaben (z. B. Sozialversicherung) betraut ist, die nicht ohne die Erhebung zumindest einiger personenbezogener Daten durchgeführt werden können, eine Datenbank oder ein Register zur Wahrnehmung dieser öffentlichen Aufgaben einrichtet. In diesem Fall legt das Gesetz, wenn auch mittelbar, fest, wer der Verantwortliche ist. Allgemein ausdrückt kann eine Rechtsvorschrift auch öffentliche oder private Stellen verpflichten, bestimmte Daten zu speichern oder bereitzustellen. Diese Stellen würden dann üblicherweise als Verantwortliche für die Verarbeitung gelten, die zur Erfüllung dieser Verpflichtung erforderlich ist.

Beispiel: Rechtsvorschriften

Das nationale Recht von Land A sieht für kommunale Behörden die Verpflichtung vor, Bürgern je nach deren finanzieller Situation Sozialleistungen wie monatliche Zahlungen zu gewähren. Um diese Zahlungen vornehmen zu können, muss die kommunale Behörde Daten über die finanzielle Situation der Antragsteller erheben und verarbeiten. Auch wenn das Gesetz nicht ausdrücklich vorsieht, dass die kommunalen Behörden für diese Verarbeitung Verantwortliche sind, ergibt sich dies implizit aus den Rechtsvorschriften.

2) *Verantwortlichkeit, die aus faktischem Einfluss herrührt*

25. Ergibt sich die datenschutzrechtliche Verantwortlichkeit nicht aus Rechtsvorschriften, ist über die Einstufung einer Partei als Verantwortlicher auf der Grundlage einer Beurteilung der tatsächlichen Umstände der Verarbeitung zu entscheiden. Um festzustellen, ob eine bestimmte Einrichtung einen

bestimmenden Einfluss auf die fragliche Verarbeitung personenbezogener Daten ausübt, sind alle relevanten tatsächlichen Gegebenheiten zu berücksichtigen.

26. Die Notwendigkeit einer Beurteilung der Faktenlage bedeutet auch, dass sich die Rolle des Verantwortlichen nicht aus der Art der Organisation ergibt, die Daten verarbeitet, sondern aus ihren konkreten Tätigkeiten in einem bestimmten Kontext. Anders ausgedrückt kann ein und dieselbe Organisation gleichzeitig hinsichtlich bestimmter Verarbeitungen als Verantwortlicher und hinsichtlich anderer Verarbeitungen als Auftragsverarbeiter handeln; die Einstufung als Verantwortlicher oder als Auftragsverarbeiter muss jeweils im Hinblick auf den konkreten Datenverarbeitungsvorgang bewertet werden.

27. In der Praxis kann davon ausgegangen werden, dass bestimmte Verarbeitungstätigkeiten als naturgemäß mit der Rolle oder den Tätigkeiten einer Organisation verknüpft gelten können, die letztendlich auch Verantwortlichkeiten hinsichtlich des Datenschutzes mit sich bringen. Dies kann auf allgemeine gesetzliche Bestimmungen oder geltende Rechtspraxis auf bestimmten Rechtsgebieten (Zivilrecht, Handelsrecht, Arbeitsrecht usw.) zurückzuführen sein. In diesem Fall sind für die Ermittlung des Verantwortlichen bestehende traditionelle Rollen und berufliche Fachkompetenz richtungsweisend, die üblicherweise eine bestimmte Verantwortlichkeit implizieren: z. B. Arbeitgeber in Bezug auf die Verarbeitung personenbezogener Daten über ihre Mitarbeiter, Verleger in Bezug auf die Verarbeitung personenbezogener Daten über Abonnenten oder Verbände in Bezug auf die Verarbeitung personenbezogener Daten über ihre Mitglieder oder Beitragszahler. Wenn eine Organisation im Rahmen ihrer Interaktion mit ihren eigenen Beschäftigten, Kunden und Kundinnen oder Mitgliedern personenbezogene Daten verarbeitet, bestimmt sie in der Regel den Zweck und die Mittel im Zusammenhang mit der Verarbeitung und handelt daher als Verantwortlicher im Sinne der DSGVO.

Beispiel: Anwaltskanzleien

Das Unternehmen ABC beauftragt eine Anwaltskanzlei mit seiner Vertretung in einem Rechtsstreit. Zur Erfüllung dieser Aufgabe muss die Anwaltskanzlei personenbezogene Daten im Zusammenhang mit dem Fall verarbeiten. Der Grund für die Verarbeitung der personenbezogenen Daten ist das Mandat für die Anwaltskanzlei, den Mandanten vor Gericht zu vertreten. Dieses Mandat zielt jedoch nicht speziell auf die Verarbeitung personenbezogener Daten ab. Die Anwaltskanzlei handelt weitgehend unabhängig, z. B. bei der Entscheidung darüber, welche Informationen zu verwenden sind und wie sie zu verwenden sind, und es liegen keine Weisungen des Mandanten bezüglich der Verarbeitung personenbezogener Daten vor. Die Verarbeitung, die die Anwaltskanzlei vornimmt, um die Aufgabe als Vertreter des Unternehmens vor Gericht wahrzunehmen, ist daher an die funktionale Rolle der Anwaltskanzlei gebunden, so dass sie als für diese Verarbeitung Verantwortlicher anzusehen ist.

Beispiel: Telekommunikationsdienstleister[11]:

Die Erbringung eines elektronischen Kommunikationsdienstes wie eines E-Mail-Dienstes beinhaltet die Verarbeitung personenbezogener Daten. Der Anbieter solcher Dienste gilt in der Regel als Verantwortlicher für die Verarbeitung personenbezogener Daten, die für den Betrieb des Dienstes als solchen erforderlich sind (z. B. Verkehrs- und Rechnungsdaten). Wenn Zweck und Rolle des Anbieters allein darin bestehen, die Übermittlung von E-Mails zu ermöglichen, gilt der Anbieter in Bezug auf die in der Nachricht selbst enthaltenen personenbezogenen Daten nicht als Verantwortlicher. Als

[11] Nach Ansicht des EDSA ist dieses Beispiel, das früher in Erwägungsgrund 47 der Richtlinie 95/46/EG enthalten war, auch im Rahmen der DSGVO weiterhin relevant.

Verantwortlicher in Bezug auf alle in der Nachricht enthaltenen personenbezogenen Daten gilt in der Regel die Person, von der die Nachricht stammt, und nicht der Diensteanbieter, der den Übermittlungsdienst anbietet.

28. In vielen Fällen kann eine Prüfung der Vertragsbestimmungen zwischen den verschiedenen beteiligten Parteien die Beantwortung der Frage erleichtern, welche Partei(en) als Verantwortliche(r) tätig ist/sind. Selbst wenn ein Vertrag keine Bestimmung darüber enthält, wer der Verantwortliche ist, kann er hinreichende Anhaltspunkte dafür bieten, wer in Bezug auf die Zwecke und Mittel der Verarbeitung eine Entscheidungsfunktion ausübt. Es kann auch sein, dass der Vertrag eine ausdrückliche Aussage zur Identität des Verantwortlichen enthält. Besteht kein Grund, daran zu zweifeln, dass dies die Realität zutreffend abbildet, spricht nichts dagegen, der Vertragsbestimmung zu folgen. Die Vertragsbestimmungen sind jedoch nicht in allen Fällen entscheidend, da dies den Parteien ermöglichen würde, die Verantwortlichkeit ganz nach eigenem Belieben zuzuweisen. Es ist nicht möglich, Verantwortlicher zu werden oder sich den Pflichten des Verantwortlichen einfach dadurch zu entziehen, dass der Vertrag in einer bestimmten Weise gestaltet wird, wenn die tatsächlichen Umstände etwas anderes sagen.

29. Entscheidet nämlich de facto eine Partei darüber, warum und wie personenbezogene Daten verarbeitet werden, so ist diese Partei selbst dann für die Verarbeitung verantwortlich, wenn es in einem Vertrag heißt, sie sei Auftragsverarbeiter. Ebenso wenig gilt eine Organisation aus datenschutzrechtlicher Sicht als Auftragsverarbeiter, weil in einem handelsrechtlichen Vertrag der Begriff „Unterauftragnehmer“ verwendet wird.[12]

30. Im Einklang mit dem faktischen Ansatz bedeutet das Wort „entscheidet“, dass die Organisation, die tatsächlich einen entscheidenden Einfluss auf die Zwecke und Mittel der Verarbeitung ausübt, der Verantwortliche ist. In der Regel wird in einer Auftragsverarbeitungsvereinbarung festgelegt, wer die bestimmende Partei (Verantwortlicher) und wer die beauftragte Partei (Auftragsverarbeiter) ist. Selbst wenn der Auftragsverarbeiter eine Dienstleistung anbietet, die vorab in einer bestimmten Weise definiert wurde, muss er dem Verantwortlichen eine ausführliche Beschreibung der Dienstleistung vorlegen und der Verantwortliche muss die endgültige Entscheidung treffen, die Art und Weise der Verarbeitung aktiv zu genehmigen und erforderlichenfalls Änderungen zu verlangen. Des Weiteren kann der Auftragsverarbeiter die wesentlichen Elemente der Verarbeitung zu einem späteren Zeitpunkt nicht ohne Zustimmung des Verantwortlichen ändern.

Beispiel: Standardisierter Cloud-Speicherdienst

Ein großer Anbieter von Cloud-Speicherdiensten bietet seinen Kunden die Möglichkeit, große Mengen personenbezogener Daten zu speichern. Die Dienstleistung ist vollständig standardisiert und die Kunden sind kaum oder gar nicht in der Lage, die Dienstleistung individuell zu gestalten. Die Vertragsbedingungen werden einseitig vom Cloud-Anbieter festgelegt und gestaltet und dem Kunden nach dem Motto „Nimm es oder lass es“ zur Verfügung gestellt. Das Unternehmen X beschließt, den Dienst des Cloud-Anbieters für die Speicherung personenbezogener Daten über seine Kunden zu nutzen. Unternehmen X gilt weiterhin als Verantwortlicher, da es sich dafür entschieden hat, diesen bestimmten Cloud-Diensteanbieter zu nutzen, um personenbezogene Daten für seine Zwecke zu verarbeiten. Solange der Cloud-Diensteanbieter die personenbezogenen Daten nicht für eigene

[12] Siehe z. B. Artikel 29 Datenschutzgruppe, Stellungnahme 10/2006 zur Verarbeitung personenbezogener Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22. November 2006, WP 128, S. 13.

Zwecke verarbeitet und die Daten ausschließlich im Auftrag seiner Kunden und weisungsgemäß speichert, gilt der Diensteanbieter als Auftragsverarbeiter.

2.1.3 „Allein oder gemeinsam mit anderen“

31. In Artikel 4 Nr. 7 wird anerkannt, dass über die „Zwecke und Mittel“ der Verarbeitung von mehr als einem Akteur entschieden werden kann. Dort heißt es, dass Verantwortlicher der Akteur ist, der „allein oder gemeinsam mit anderen“ über die Zwecke und Mittel der Verarbeitung entscheidet. Dies bedeutet, dass mehrere verschiedene Stellen bei ein und derselben Verarbeitung als Verantwortliche agieren können, wobei jede von ihnen dann den geltenden Datenschutzbestimmungen unterliegt. Dementsprechend kann eine Organisation auch dann Verantwortlicher sein, wenn sie nicht alle Entscheidungen über die Zwecke und Mittel trifft. Die Kriterien der gemeinsamen Verantwortlichkeit und das Ausmaß, in dem zwei oder mehr Akteure gemeinsam die Kontrolle ausüben, können unterschiedliche Formen annehmen, wie zu einem späteren Zeitpunkt erläutert wird.[13]

2.1.4 „Zwecke und Mittel“

32. Die vierte Hauptkomponente der Definition des Verantwortlichen bezieht sich auf den Gegenstand des Einflusses des Verantwortlichen, nämlich die „Zwecke und Mittel“ der Verarbeitung. Sie macht das Wesentliche des Konzepts des Verantwortlichen aus, nämlich: worüber eine Partei entscheiden muss, um als Verantwortlicher zu gelten.

33. In Wörterbüchern wird der Begriff „Zweck“ definiert als „ein erwartetes Ergebnis, an dem sich ihre geplanten Maßnahmen ausrichten“ und „wie ein Ergebnis erzielt oder ein Zielerreicht wird“.

34. Nach der DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Bestimmung der „Zwecke“ der Verarbeitung und der „Mittel“ zu ihrer Erreichung ist daher von besonderer Bedeutung.

35. Die Festlegung der Zwecke und der Mittel läuft darauf hinaus, jeweils zu entscheiden, „warum“ und „auf welche Weise“ die Verarbeitung erfolgt:[14] Bei einer bestimmten Verarbeitung ist der Verantwortliche der Akteur, der entschieden hat, *warum* die Verarbeitung erfolgt (also „mit welchem Ziel“ oder „wozu“), und *auf welche Weise* dieses Ziel erreicht werden soll (also welche Mittel eingesetzt werden, um das Ziel zu erreichen). Eine natürliche oder juristische Person, die einen solchen Einfluss auf die Verarbeitung personenbezogener Daten nimmt, ist somit gemäß der Definition in Artikel 4 Nr. 7 DSGVO an der Festlegung der Zwecke und Mittel dieser Verarbeitung beteiligt.[15]

36. Wie nachstehend beschrieben muss der Verantwortliche sowohl über den Zweck als auch über die Mittel der Verarbeitung entscheiden. Folglich kann der Verantwortliche sich nicht darauf beschränken, nur den Zweck zu bestimmen. Er muss auch Entscheidungen bezüglich der Mittel der Verarbeitung treffen. Umgekehrt kann die als Auftragsverarbeiter agierende Partei niemals den Zweck der Verarbeitung bestimmen.

37. Wenn ein Verantwortlicher einen Auftragsverarbeiter damit beauftragt, die Verarbeitung in seinem Namen durchzuführen, bedeutet dies in der Praxis häufig, dass der Auftragsverarbeiter in der Lage sein soll, selbst bestimmte Entscheidungen über die Durchführung der Verarbeitung zu treffen. Der EDSA

[13] Siehe Teil I Abschnitt 3 („Definition von gemeinsam Verantwortlichen“).
[14] Vgl. auch Schlussanträge des Generalanwalts Bot in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, Nr. 46).
[15] Urteil *Zeugen Jehovas*, C-25/17, ECLI:EU:C:2018:551, Rn. 68.

räumt ein, dass es einen gewissen Handlungsspielraum für den Auftragsverarbeiter geben kann, um auch einige Entscheidungen in Bezug auf die Verarbeitung treffen zu können. In diesem Zusammenhang ist es notwendig Hilfestellung zu geben, welches **Maß an Einfluss** auf das „Warum" und das „Auf welche Weise" die Einstufung einer Stelle als Verantwortlicher zur Folge haben sollte und in welchem Umfang ein Auftragsverarbeiter eigene Entscheidungen treffen kann.

38. Wenn eine Organisation eindeutig die Zwecke und Mittel festlegt und eine andere Organisation mit Verarbeitungstätigkeiten betraut, bei denen ihre detaillierten Weisungen befolgt werden, ist die Situation klar und besteht kein Zweifel daran, dass die zweite Organisation als Auftragsverarbeiter anzusehen ist, während die erste der Verantwortliche ist.

Wesentliche vs. nicht wesentliche Mittel

39. Es stellt sich die Frage, wo die Grenze zu ziehen ist zwischen Entscheidungen, die dem Verantwortlichen vorbehalten sind, und Entscheidungen, die dem Ermessen des Auftragsverarbeiters überlassen werden können. Entscheidungen über den Zweck der Verarbeitung sind eindeutig immer Sache des Verantwortlichen.

40. Bei der Festlegung der Mittel kann zwischen wesentlichen und nicht wesentlichen Mitteln unterschieden werden. „Wesentliche Mittel" sind traditionell und naturgemäß dem Verantwortlichen vorbehalten. Während nicht wesentliche Mittel auch vom Auftragsverarbeiter festgelegt werden können, muss über die wesentlichen Mittel der Verantwortliche entscheiden. „Wesentliche Mittel" sind solche, die in engem Zusammenhang mit dem Zweck und dem Umfang der Verarbeitung stehen, wie die Art der verarbeiteten personenbezogenen Daten („*welche Daten werden verarbeitet*?"), die Dauer der Verarbeitung („*wie lange werden sie verarbeitet*?"), die Kategorien von Empfängern („*wer hat Zugang zu ihnen*?") und die Kategorien betroffener Personen („*wessen personenbezogene Daten werden verarbeitet*?"). Neben dem Zweck der Verarbeitung sind die wesentlichen Mittel ferner eng verknüpft mit der Frage, ob die Verarbeitung rechtmäßig, erforderlich und verhältnismäßig ist. Bei den „nicht wesentlichen Mitteln" geht es eher um praktische Aspekte der Umsetzung, wie die Wahl einer bestimmten Hard- oder Software oder die detaillierten Sicherheitsmaßnahmen, über die der Auftragsverarbeiter entscheiden kann.

Beispiel: Lohnbuchhaltung

Arbeitgeber A überträgt einem anderen Unternehmen die Verwaltung der Löhne und Gehälter an seine Beschäftigten. Arbeitgeber A erteilt klare Weisungen dazu, an wen zu zahlen ist, welche Beträge, bis zu welchem Zeitpunkt, durch welche Bank, wie lange die Daten gespeichert werden sollen, welche Daten dem Finanzamt zu übermitteln sind usw. In diesem Fall erfolgt die Verarbeitung der Daten für den Zweck von Unternehmen A, seinen Beschäftigten ihre Löhne und Gehälter auszuzahlen, und das mit der Lohnbuchhaltung betraute Unternehmen darf die Daten nicht für eigene Zwecke verwenden. Die Art und Weise, in der die Lohn- und Gehaltsabrechnungsverwaltung die Verarbeitung durchführen sollte, ist im Wesentlichen klar und genau festgelegt. Die Lohn- und Gehaltsabrechnungsverwaltung kann jedoch über bestimmte Details im Zusammenhang mit der Verarbeitung entscheiden, wie z. B. welche Software eingesetzt wird, wie der Zugang innerhalb ihrer eigenen Organisation geregelt ist usw. Dies ändert nichts an ihrer Rolle als Auftragsverarbeiter, solange sie nicht gegen die Weisungen von Unternehmen A verstößt oder darüber hinausgeht.

Beispiel: Bankzahlungen

Gemäß den Weisungen von Arbeitgeber A übermittelt die das mit der Lohnbuchhaltung betraute Unternehmen der Bank B Informationen, damit diese die eigentliche Zahlung an die Beschäftigten von Arbeitgeber A tätigen kann. Zu dieser Tätigkeit gehört auch die Verarbeitung personenbezogener Daten durch die Bank B, die sie in Ausübung ihrer Banktätigkeit vornimmt. Im Rahmen dieser Tätigkeit entscheidet die Bank unabhängig von Arbeitgeber A, welche Daten zur Erbringung der Dienstleistung verarbeitet werden müssen, wie lange die Daten gespeichert werden müssen usw. Arbeitgeber A kann den Zweck und die Mittel der Datenverarbeitung von Bank B nicht beeinflussen. Bank B ist daher als für diese Verarbeitung Verantwortlicher anzusehen, und die Übermittlung personenbezogener Daten durch die Lohn- und Gehaltsabrechnungsverwaltung ist als Weitergabe von Informationen zwischen zwei Verantwortlichen, nämlich von Arbeitgeber A an Bank B, anzusehen.

Beispiel: Wirtschaftsprüfer

Arbeitgeber A beauftragt ferner Wirtschaftsprüfungsgesellschaft C mit der Prüfung seiner Buchführung und übermittelt daher Daten über Finanztransaktionen (einschließlich personenbezogener Daten) an C. Wirtschaftsprüfungsgesellschaft C verarbeitet diese Daten ohne detaillierte Weisungen von A. Wirtschaftsprüfungsgesellschaft C entscheidet gemäß den gesetzlichen Bestimmungen über ihre die Prüfungstätigkeiten selbst, dass die von ihr erhobenen Daten nur zum Zwecke der Prüfung von A verarbeitet werden, und legt fest, welche Daten sie benötigt, welche Kategorien von Personen erfasst werden müssen, wie lange die Daten gespeichert werden und welche technischen Mittel eingesetzt werden sollen. Unter diesen Umständen ist Wirtschaftsprüfungsgesellschaft C bei der Erbringung ihrer Wirtschaftsprüfungsleistungen für A als eigenständiger Verantwortlicher zu betrachten. Diese Einschätzung kann jedoch je nach dem Umfang der Weisungen von A auch anders ausfallen. Wenn nämlich das Gesetz keine besonderen Pflichten für die Wirtschaftsprüfungsgesellschaft vorsieht und das Kundenunternehmen sehr detaillierte Weisungen bezüglich der Verarbeitung erteilt, würde die Wirtschaftsprüfungsgesellschaft vielmehr als Auftragsverarbeiter handeln. Unterschieden werden könnte zwischen einer Situation, in der die Verarbeitung – im Einklang mit den für diesen Berufsstand geltenden Rechtsvorschriften – als Teil der Kerntätigkeit der Wirtschaftsprüfungsgesellschaft erfolgt, und Fällen, in denen es sich um eine eher begrenzte, untergeordnete Tätigkeit handelt, die im Rahmen der Tätigkeit des Kundenunternehmens durchgeführt wird.

Beispiel: Hosting-Dienstleistungen

Arbeitgeber A engagiert Hosting-Dienst H, der verschlüsselte Daten auf seinen Servern speichern soll. Hosting-Dienst H bestimmt weder, ob es sich bei den von ihm gehosteten Daten um personenbezogene Daten handelt, noch verarbeitet er Daten auf andere Weise als durch Speicherung auf seinen Servern. Da die Speicherung ein Beispiel für eine Verarbeitung personenbezogener Daten ist, verarbeitet Hosting-Dienst H personenbezogene Daten im Auftrag von Arbeitgeber A und ist daher Auftragsverarbeiter. Arbeitgeber A hat H die erforderlichen Weisungen zu erteilen und eine Auftragsverarbeitungsvereinbarung gemäß Artikel 28 zu schließen, mit der H zur Durchführung technischer und organisatorischer Sicherheitsmaßnahmen verpflichtet wird. H muss A dabei behilflich sein, sicherzustellen, dass die erforderlichen Sicherheitsmaßnahmen getroffen werden, und ihn im Falle einer Verletzung des Schutzes personenbezogener Daten benachrichtigen.

41. Auch wenn Entscheidungen über nicht wesentliche Mittel dem Auftragsverarbeiter überlassen werden können, muss der Verantwortliche dennoch bestimmte Elemente in der Auftragsverarbeitungsvereinbarung festlegen, wie etwa – in Bezug auf die Sicherheitsanforderungen

– z. B. eine Weisung, alle nach Artikel 32 DSGVO erforderlichen Maßnahmen zu ergreifen. In der Vereinbarung muss auch geregelt sein, dass der Auftragsverarbeiter den Verantwortlichen dabei unterstützt, die Einhaltung beispielsweise von Artikel 32 sicherzustellen. Der Verantwortliche bleibt in jedem Fall für die Durchführung geeigneter technischer und organisatorischer Maßnahmen verantwortlich, mit denen sichergestellt wird und nachgewiesen werden kann, dass die Verarbeitung im Einklang mit der Verordnung erfolgt (Artikel 24). Dabei muss der Verantwortliche die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Daher muss der Verantwortliche umfassend über die eingesetzten Mittel informiert werden, damit er in dieser Hinsicht eine fundierte Entscheidung treffen kann. Damit der Verantwortliche die Rechtmäßigkeit der Verarbeitung nachweisen kann, ist es ratsam, zumindest die erforderlichen technischen und organisatorischen Maßnahmen im Vertrag oder in einem anderen rechtsverbindlichen Instrument zwischen Verantwortlichem und Auftragsverarbeiter zu dokumentieren.

Beispiel: Callcenter

Unternehmen X beschließt, einen Teil seiner Kundenbetreuung an ein Callcenter auszulagern. Das Callcenter erhält identifizierbare Daten über Kundenkäufe sowie Kontaktangaben. Das Callcenter nutzt seine eigene Software und IT-Infrastruktur für die Verwaltung der personenbezogenen Daten der Kunden von Unternehmen X. Unternehmen X unterzeichnet eine Auftragsverarbeitungsvereinbarung mit dem Anbieter des Callcenters gemäß Artikel 28 DSGVO, nachdem es festgestellt hat, dass die vom Callcenter vorgeschlagenen technischen und organisatorischen Sicherheitsmaßnahmen den betreffenden Risiken angemessen sind und das Callcenter die personenbezogenen Daten nur für die Zwecke von Unternehmen X und gemäß seinen Weisungen verarbeiten wird. Unternehmen X erteilt dem Callcenter keine weiteren Weisungen hinsichtlich der zu verwendenden besonderen Software und auch keine detaillierten Weisungen zu den zu ergreifenden konkreten Sicherheitsmaßnahmen. In diesem Beispiel bleibt Unternehmen X Verantwortlicher, obwohl das Callcenter über bestimmte nicht wesentliche Verarbeitungsmittel entscheidet.

2.1.5 „Der Verarbeitung von personenbezogenen Daten“

42. Die vom Verantwortlichen festgelegten Zwecke und Mittel müssen mit der „Verarbeitung von personenbezogenen Daten“ zu tun haben. In Artikel 4 Nr. 2 DSGVO wird die Verarbeitung personenbezogener Daten definiert als *„jeder Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten*“. Folglich kann der Begriff eines Verantwortlichen entweder mit einem einzigen Verarbeitungsvorgang oder mit einer Reihe von Vorgängen verknüpft werden. In der Praxis kann dies bedeuten, dass sich die Kontrolle durch eine bestimmte Organisation auf die gesamte fragliche Verarbeitung erstrecken, sich aber auch auf einen bestimmten Verarbeitungsschritt beschränken kann.[16]

43. In der Praxis kann die Verarbeitung personenbezogener Daten, an der mehrere Akteure beteiligt sind, in mehrere kleinere Verarbeitungsvorgänge unterteilt werden, bei denen davon ausgegangen werden könnte, dass jeder Akteur den Zweck und die Mittel individuell bestimmt. Andererseits kann eine Abfolge oder Reihe von Verarbeitungsvorgängen, an denen mehrere Akteure beteiligt sind, auch für

[16]Urteil *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, Rn. 74: *„Daraus folgt, wie der Generalanwalt [...] ausgeführt hat, dass eine natürliche oder juristische Person offenbar nur für Vorgänge der Verarbeitung personenbezogener Daten, über deren Zwecke und Mittel sie – gemeinsam mit anderen – entscheidet, im Sinne von Art. 2 Buchst. d der Richtlinie gemeinsam mit anderen verantwortlich sein kann. Dagegen kann [...] diese natürliche oder juristische Person für vor- oder nachgelagerte Vorgänge in der Verarbeitungskette, für die sie weder die Zwecke noch die Mittel festlegt, nicht als im Sinne dieser Vorschrift verantwortlich angesehen werden“.*

denselben Zweck oder dieselben Zwecke erfolgen; in diesem Fall ist es möglich, dass an der Verarbeitung ein oder mehrere gemeinsam Verantwortliche beteiligt sind. Es ist also mit anderen Worten möglich, dass auf „Mikroebene“ die verschiedenen Verarbeitungsvorgänge der Kette als unabhängig voneinander erscheinen, da jeder von ihnen einen anderen Zweck haben kann. Es muss jedoch genau geprüft werden, ob diese Verarbeitungsvorgänge auf „Makroebene“ nicht als „Vorgangsreihe“ betrachtet werden sollten, mit der ein gemeinsamer Zweck mit gemeinsam festgelegten Mitteln verfolgt wird.

44. Wer beschließt, Daten zu verarbeiten, muss prüfen, ob dazu auch personenbezogene Daten gehören und, wenn ja, welche Verpflichtungen gemäß DSGVO bestehen. Ein Akteur gilt als für die Verarbeitung „Verantwortlicher“, auch wenn er dabei nicht bewusst auf personenbezogene Daten als solche abzielt oder fälschlicherweise angenommen hat, keine personenbezogenen Daten zu verarbeiten.

45. Es ist nicht erforderlich, dass der Verantwortliche tatsächlich Zugang zu den verarbeiteten Daten hat.[17] Wer eine Verarbeitungstätigkeit auslagert und dabei entscheidenden Einfluss auf den Zweck und die (wesentlichen) Mittel der Verarbeitung hat (z. B. durch Anpassung von Parametern eines Dienstes in einer Weise, dass er beeinflusst, wessen personenbezogene Daten verarbeitet werden), ist als Verantwortlicher anzusehen, auch wenn er nie tatsächlich auf die Daten zugreifen kann.

Beispiel: Marktforschung 1

Unternehmen ABC möchte wissen, welche Arten von Verbrauchern am ehesten an seinen Produkten interessiert sind, und beauftragt einen Dienstleister, XYZ, mit der Beschaffung entsprechender Informationen.

Unternehmen ABC weist XYZ an, an welcher Art von Informationen es interessiert ist, und stellt eine Liste von Fragen bereit, die den an der Marktstudie Teilnehmenden zu stellen sind.

Unternehmen ABC erhält von XYZ nur statistische Informationen (z. B. Ermittlung von Verbrauchertrends pro Region) und hat keinen Zugang zu den personenbezogenen Daten selbst. Dennoch entschied das Unternehmen ABC, die Verarbeitung solle stattfinden; die Verarbeitung erfolgt für seinen Zweck und seine Tätigkeit, und es erteilte XYZ detaillierte Weisungen bezüglich der zu erhebenden Informationen. Unternehmen ABC hat daher weiterhin als für die Verarbeitung personenbezogener Daten Verantwortlicher zu gelten, mit der die angeforderten Informationen geliefert werden sollen. XYZ darf die Daten nur für den von Unternehmen ABC vorgegebenen Zweck und nach dessen detaillierten Weisungen verarbeiten und ist daher als Auftragsverarbeiter zu betrachten.

Beispiel: Marktforschung 2

Unternehmen ABC möchte in Erfahrung bringen, welche Verbrauchergruppen am ehesten an seinen Produkten interessiert sind. Der Dienstleister XYZ ist eine Marktforschungsagentur, die mittels einer Vielzahl von Fragebögen zu einer breiten Palette von Produkten und Dienstleistungen Informationen über Verbraucherinteressen gesammelt hat. Der Dienstleister XYZ hat diese Daten unabhängig nach seiner eigenen Methodik erhoben und ausgewertet, ohne Weisungen von Unternehmen ABC erhalten zu haben. Auf Ersuchen von Unternehmen ABC stellt der Dienstleister XYZ statistische Informationen zusammen, ohne jedoch weitere Weisungen darüber zu erhalten, welche personenbezogenen Daten verarbeitet werden sollten oder wie sie verarbeitet werden sollten, um diese Statistiken zu erstellen.

[17] Urteil *Wirtschaftsakademie*, C-201/16, ECLI: EU: C: 2018: 388, Rn. 38.

In diesem Beispiel agiert der Dienstleister XYZ als einziger Verantwortlicher, der personenbezogene Daten für Marktforschungszwecke verarbeitet und die Mittel hierfür eigenständig festlegt. Unternehmen ABC hat in Bezug auf diese Verarbeitungstätigkeiten keine besondere datenschutzrechtliche Rolle oder Verantwortung, da Unternehmen ABC anonymisierte Statistiken erhält und nicht an der Festlegung der Zwecke und Mittel der Verarbeitung beteiligt ist.

3 DEFINITION DES BEGRIFFS „GEMEINSAM VERANTWORTLICHE“

3.1 Definition des Begriffs „gemeinsam Verantwortliche“

46. Die Einstufung als gemeinsam Verantwortliche kann geboten sein, wenn mehr als ein Akteur an der Verarbeitung beteiligt ist.

47. Obwohl das Konzept nicht neu ist und bereits in der Richtlinie 95/46/EG bestand, führt die DSGVO in Artikel 26 besondere Vorschriften für gemeinsam Verantwortliche ein und legt einen Rahmen für die Beziehungen zwischen ihnen fest. Darüber hinaus hat der Gerichtshof der Europäischen Union (EuGH) in jüngerer Zeit Klarstellungen zum Begriff der gemeinsam Verantwortlichen und seinen Auswirkungen vorgenommen.[18]

48. Wie in Teil II Abschnitt 2 näher ausgeführt, wird sich die Einstufung als gemeinsam Verantwortliche hauptsächlich auf die Zuweisung von Verpflichtungen zur Einhaltung der Datenschutzvorschriften und insbesondere in Bezug auf die Rechte des Einzelnen auswirken.

49. In diesem Zusammenhang soll der folgende Abschnitt Hilfestellung bei der Auslegung des Begriffs der gemeinsam Verantwortlichen im Einklang mit der DSGVO und der Rechtsprechung des EuGH geben, um Organisationen bei der Beantwortung der Frage, wo sie als gemeinsam Verantwortliche handeln könnten, und bei der Anwendung des Konzepts in der Praxis zu unterstützen.

3.2 Vorliegen gemeinsamer Verantwortlichkeit

3.2.1 Allgemeine Erwägungen

50. Ausgangspunkt für die Feststellung gemeinsamer Verantwortlichkeit ist die Definition des Begriffs „Verantwortlicher“ in Artikel 4 Nr. 7 DSGVO. Die Ausführungen in diesem Abschnitt stehen daher in unmittelbarem Zusammenhang mit denen im Abschnitt über den Begriff des Verantwortlichen und ergänzen diese. Folglich sollte die Beurteilung der gemeinsamen Verantwortlichkeit die oben vorgenommene Beurteilung der „alleinigen Verantwortlichkeit“ widerspiegeln.

51. In Artikel 26 DSGVO, der die Begriffsbestimmung in Artikel 4 Nr. 7 DSGVO aufgreift, heißt es: *„Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche.“* Im weitesten Sinne liegt also im Hinblick auf eine konkrete Verarbeitungstätigkeit eine gemeinsame Verantwortlichkeit vor, wenn verschiedene Parteien *gemeinsam* über den Zweck und die Mittel dieser Verarbeitungstätigkeit entscheiden. Zur Beurteilung der Frage, ob eine gemeinsame Verantwortlichkeit vorliegt, ist daher zu prüfen, ob über die Festlegung

[18] Vgl. insbesondere *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein gegen Wirtschaftsakademie* (C-210/16), *Tietosuojavaltuutettu gegen Jehovan todistajat – uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG gegen Verbraucherzentrale NRW e.V. (*C-40/17). Es sei darauf hingewiesen, dass diese Urteile zwar vom EuGH zur Auslegung des Begriffs „gemeinsam Verantwortliche“ gemäß der Richtlinie 95/46/EG erlassen wurden, sie aber vor dem Hintergrund der DSGVO weiterhin Gültigkeit haben, da sich an den Elementen, die diesen Begriff im Rahmen der DSGVO bestimmen, im Vergleich zur Richtlinie nichts geändert hat.

der Zwecke und der Mittel, die einen Verantwortlichen kennzeichnet, von mehr als einer Partei entschieden wird. Der Begriff „gemeinsam“ ist auszulegen als „zusammen mit“ oder „nicht allein“, und zwar in verschiedenen Formen und Kombinationen, wie nachstehend erläutert wird.

52. Die Prüfung gemeinsamer Verantwortlichkeit sollte auf der Grundlage einer tatsächlichen und nicht einer formalen Analyse des tatsächlichen Einflusses auf die Zwecke und Mittel der Verarbeitung erfolgen. Alle bestehenden oder geplanten Vereinbarungen sollten mit den tatsächlichen Umständen in Bezug auf die Beziehungen zwischen den Parteien abgeglichen werden. Ein rein formaler Maßstab wäre aus mindestens zwei Gründen nicht ausreichend: In einigen Fällen würde die formale Benennung von gemeinsam Verantwortlichen - beispielsweise gesetzlich oder vertraglich festgelegt - fehlen; in anderen Fällen könnte es sein, dass die formale Benennung nicht die Realität der Vereinbarungen widerspiegelt, wenn formal die Rolle des Verantwortlichen einer Stelle zugewiesen wird, die tatsächlich nicht in der Lage ist, über die Zwecke und Mittel der Verarbeitung zu „entscheiden“.

53. Nicht jede Verarbeitung, an der mehrere Stellen beteiligt sind, führt zu gemeinsamer Verantwortlichkeit. Das übergeordnete Kriterium für das Vorliegen gemeinsamer Verantwortlichkeit ist die **gemeinsame Beteiligung von zwei oder mehr Stellen an der Festlegung der Zwecke und Mittel** einer Verarbeitung. Genauer gesagt muss die gemeinsame Beteiligung einerseits die Festlegung der Zwecke und andererseits die Festlegung der Mittel umfassen. Entscheiden alle betroffenen Stellen über jedes dieser Elemente, sollten sie als gemeinsam Verantwortliche für die betreffende Verarbeitung betrachtet werden.

3.2.2 Beurteilung der gemeinsamen Beteiligung

54. Eine gemeinsame Beteiligung an der Festlegung der Zwecke und Mittel bedeutet, dass mehr als eine Stelle entscheidenden Einfluss darauf hat, ob und wie die Verarbeitung erfolgt. In der Praxis kann eine gemeinsame Beteiligung verschiedene Formen annehmen. Eine gemeinsame Beteiligung kann beispielsweise in Form einer **gemeinsam getroffenen Entscheidung** von zwei oder mehr Stellen vorliegen oder sich aus **konvergierenden Entscheidungen** von zwei oder mehr Stellen über die Zwecke und wesentlichen Mittel ergeben.

55. Eine gemeinsame Beteiligung im Wege einer *gemeinsamen Entscheidung* bedeutet, dass nach der gängigsten Lesart des in Artikel 26 DSGVO genannten Begriffs „gemeinsam“ eine gemeinsame Entscheidung getroffen wird und eine gemeinsame Absicht vorliegt.

Die Situation der gemeinsamen Beteiligung durch *konvergierende Entscheidungen* ergibt sich insbesondere aus der Rechtsprechung des EuGH zum Begriff der gemeinsam Verantwortlichen. Entscheidungen können im Hinblick auf Zwecke und Mittel als konvergierend angesehen werden, **wenn sie einander ergänzen und für die Verarbeitung in einer Weise erforderlich sind, , dass sie einen spürbaren Einfluss auf die Bestimmung der Zwecke und Mittel der Verarbeitung nehmen**. Es sollte hervorgehoben werden, dass der Begriff der konvergierenden Entscheidungen mit Blick auf die Zwecke und Mittel der Verarbeitung, nicht aber in Bezug auf andere Aspekte der Geschäftsbeziehung zwischen den Parteien zu betrachten ist.[19] Somit ist ein wichtiges Kriterium für die Feststellung konvergierender Entscheidungen in diesem Zusammenhang, **ob die Verarbeitung ohne Beteiligung beider Parteien an den Zwecken und Mitteln nicht möglich wäre in dem Sinne, dass die Verarbeitungsvorgänge beider Parteien untrennbar, d. h. unlösbar miteinander verbunden sind**. Die Situation von gemeinsam Verantwortlichen, die auf der Grundlage konvergierender Entscheidungen handeln, ist jedoch von dem Fall eines Auftragsverarbeiters zu unterscheiden, da letzterer – obwohl er an der Durchführung einer

[19] Tatsächlich beinhalten alle Geschäftsvereinbarungen konvergierende Entscheidungen im Zuge des Verfahrens, mit dem eine Einigung erzielt wird.

Verarbeitung beteiligt ist – die Daten nicht für eigene Zwecke verarbeitet, sondern die Verarbeitung im Auftrag des Verantwortlichen durchführt.

56. Die Tatsache, dass eine der Parteien keinen Zugang zu verarbeiteten personenbezogenen Daten hat, reicht nicht aus, um eine gemeinsame Verantwortlichkeit auszuschließen.[20] In *Zeugen Jehovas* beispielsweise vertrat der EuGH die Auffassung, dass eine Religionsgemeinschaft gemeinsam mit ihren als Verkündiger tätigen Mitgliedern als Verantwortliche für die Verarbeitungen personenbezogener Daten angesehen werden kann, die durch diese Mitglieder im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erfolgen.[21] Nach Ansicht des EuGH war es hierfür nicht erforderlich, dass die Gemeinschaft Zugriff auf die fraglichen Daten hatte oder dass sie ihren Mitgliedern schriftliche Leitlinien oder Weisungen für diese Datenverarbeitungen gegeben hatte.[22] Die Gemeinschaft beteiligte sich an der Festlegung der Zwecke und Mittel, indem sie die Aktivitäten ihrer Mitglieder organisierte und koordinierte, was dazu beitrug, das Ziel der Gemeinschaft der Zeugen Jehovas zu erreichen.[23] Überdies war der Gemeinschaft allgemein bekannt, dass solche Verarbeitungen zum Zweck der Verbreitung ihres Glaubens erfolgten.[24]

57. Es ist auch wichtig zu betonen, wie vom EuGH klargestellt, dass eine Stelle nur in Bezug auf diejenigen Vorgänge als gemeinsam Verantwortlicher gilt, für die sie gemeinsam mit anderen die Mittel und die Zwecke derselben Datenverarbeitung festlegt, insbesondere im Falle konvergierender Entscheidungen. Entscheidet eine dieser Stellen allein über die Zwecke und Mittel von Vorgängen, die in der Verarbeitungskette vor- oder nachgelagert sind, so ist diese Stelle als alleiniger Verantwortlicher für diesen vor- oder nachgelagerten Vorgang anzusehen.[25]

58. Das Vorliegen einer gemeinsamen Verantwortung impliziert nicht notwendigerweise das gleiche Maß an Verantwortung der verschiedenen an der Verarbeitung personenbezogener Daten beteiligten Akteure. Vielmehr hat der EuGH klargestellt, dass diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein können, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.

3.2.2.1 Gemeinsam festgelegte(r) Zweck(e)

59. Gemeinsame Verantwortlichkeit liegt vor, wenn Stellen, die an derselben Verarbeitung beteiligt sind, die Verarbeitung für gemeinsam festgelegte Zwecke durchführen. Dies ist der Fall, wenn die beteiligten Stellen die Daten für dieselben oder gemeinsame Zwecke verarbeiten.

60. Wenn die Stellen mit der Verarbeitung nicht denselben Zweck verfolgen, kann zudem im Lichte der Rechtsprechung des EuGH eine gemeinsame Verantwortlichkeit festgestellt werden, wenn die beteiligten Stellen eng miteinander verknüpfte oder sich ergänzende Zwecke verfolgen. Dies kann beispielsweise der Fall sein, wenn sich aus demselben Verarbeitungsvorgang beiderseitiger Nutzen ergibt, sofern jede der beteiligten Stellen an der Festlegung der Zwecke und Mittel des betreffenden Verarbeitungsvorgangs beteiligt ist. Der Begriff des beiderseitigen Nutzens ist jedoch nicht entscheidend und kann nur ein Indiz sein. In *Fashion ID* hat der EuGH beispielsweise klargestellt, dass

[20] Urteil *Wirtschaftsakademie*, C-210/16, ECLI: EU: C: 2018: 388, Rn. 38.
[21] Urteil *Zeugen Jehovas*, C-25/17, ECLI:EU:C:2018:551, Rn. 75.
[22] Ebenda.
[23] Ebenda., Rn. 71.
[24] Ebenda.
[25] Urteil *Fashion ID*, C-40/17, ECLI: EU: 2018: 1039, Rn. 74. „*Dagegen kann, unbeschadet einer etwaigen insoweit im nationalen Recht vorgesehenen zivilrechtlichen Haftung, diese natürliche oder juristische Person für vor- oder nachgelagerte Vorgänge in der Verarbeitungskette, für die sie weder die Zwecke noch die Mittel festlegt, nicht als im Sinne dieser Vorschrift verantwortlich angesehen werden*."

ein Website-Betreiber an der Festlegung der Zwecke (und Mittel) der Verarbeitung beteiligt ist, indem er ein Social Plug-in in eine Website einbindet, um die Werbung für seine Waren zu optimieren, indem er sie im sozialen Netzwerk sichtbarer macht. Nach Auffassung des EuGH wurden die fraglichen Verarbeitungsvorgänge im wirtschaftlichen Interesse sowohl des Betreibers der Website als auch des Anbieters des Social Plug-in durchgeführt.[26]

61. Ebenso soll, wie der EuGH in *Wirtschaftsakademie* festgestellt hat, die Verarbeitung personenbezogener Daten durch Statistiken über Besucher einer Fanpage Facebook in die Lage versetzen, sein über sein Netzwerk verbreitetes Werbesystem zu verbessern, und es dem Betreiber der Fanpage ermöglichen, Statistiken zu erhalten, um die Werbung für seine Tätigkeit zu verwalten.[27] In diesem Fall verfolgt jede Stelle ihr eigenes Interesse, aber beide Parteien beteiligen sich an der Festlegung der Zwecke (und Mittel) der Verarbeitung personenbezogener Daten in Bezug auf die Besucher der Fanpage.[28]

62. In diesem Zusammenhang ist hervorzuheben, dass die bloße Existenz eines beiderseitigen Vorteils (z. B. kommerzieller Art), der sich aus einer Verarbeitungstätigkeit ergibt, nicht zu einer gemeinsamen Verantwortlichkeit führt. Wenn die an der Verarbeitung beteiligte Stelle im Zusammenhang mit der Verarbeitungstätigkeit keine(n) eigenen Zweck(e) verfolgt, sondern lediglich für erbrachte Dienstleistungen bezahlt wird, handelt sie als Auftragsverarbeiter und nicht als gemeinsam Verantwortlicher.

3.2.2.2 Gemeinsam festgelegte Mittel

63. Gemeinsame Verantwortlichkeit erfordert ferner, dass zwei oder mehr Stellen Einfluss auf die Mittel der Verarbeitung ausgeübt haben. Das bedeutet nicht, dass für das Bestehen einer gemeinsamen Verantwortlichkeit jede beteiligte Stelle in jedem Fall alle Mittel bestimmen muss. Wie der EuGH klargestellt hat, können verschiedene Stellen in verschiedenen Phasen dieser Verarbeitung und in unterschiedlichem Ausmaß beteiligt sein. Verschiedene gemeinsam Verantwortliche können daher die Mittel der Verarbeitung in unterschiedlichem Maße festlegen, je nachdem, wer hierzu tatsächlich in der Lage ist.

64. Es kann auch vorkommen, dass eine der beteiligten Stellen die Mittel für die Verarbeitung bereitstellt und diese für die Verarbeitung personenbezogener Daten durch andere Stellen zur Verfügung stellt. Die Stelle, die beschließt, diese Mittel zu nutzen, damit personenbezogene Daten für einen bestimmten Zweck verarbeitet werden können, ist ebenfalls an der Festlegung der Mittel für die Verarbeitung beteiligt.

65. Dieses Szenario kann sich insbesondere bei Plattformen, standardisierten Tools oder anderen Infrastrukturen ergeben, die es den Parteien ermöglichen, dieselben personenbezogenen Daten zu verarbeiten, und die von einer der Parteien so eingerichtet wurden, dass sie von anderen verwendet werden, die auch entscheiden können, wie sie eingerichtet werden.[29] Die Nutzung eines bereits bestehenden technischen Systems schließt die gemeinsame Verantwortlichkeit nicht aus, wenn die Nutzer des Systems über die in diesem Zusammenhang durchzuführende Verarbeitung personenbezogener Daten entscheiden können.

---

[26] Urteil *Fashion ID,* C-40/17, ECLI: EU: 2018: 1039, Rn. 80.
[27] Urteil *Wirtschaftsakademie*, C-210/16, ECLI: EU: C: 2018: 388, Rn. 34.
[28] Urteil *Wirtschaftsakademie*, C-210/16, ECLI: EU: C: 2018: 388, Rn. 39.
[29] Anbieter des Systems kann ein gemeinsam Verantwortlicher sein, wenn die oben genannten Kriterien erfüllt sind, d. h. wenn der Anbieter an der Festlegung der Zwecke und Mittel beteiligt ist. Andernfalls sollte der Anbieter als Auftragsverarbeiter betrachtet werden.

66. Als Beispiel dafür hat der EuGH in *Wirtschaftsakademie* entschieden, dass der Betreiber einer auf Facebook gehosteten Fanpage durch die Festlegung von Parametern auf der Grundlage seiner Zielgruppe und der Ziele der Verwaltung und Förderung seiner Tätigkeiten als an der Festlegung der Mittel zur Verarbeitung personenbezogener Daten im Zusammenhang mit den Besuchern seiner Fanpage beteiligt anzusehen ist.

67. Darüber hinaus wird die Entscheidung einer Stelle, ein von einer anderen Stelle entwickeltes Instrument oder ein anderes System, das die Verarbeitung personenbezogener Daten ermöglicht, für eigene Zwecke zu nutzen, wahrscheinlich auf eine gemeinsame Entscheidung über die Mittel dieser Verarbeitung durch diese Stellen hinauslaufen. Dies folgt aus *Fashion ID*, wo der EuGH zu dem Schluss kam, dass Fashion ID durch die Einbettung des „Gefällt mir"-Button von Facebook, der den Website-Betreibern von Facebook zur Verfügung gestellt wurde, einen entscheidenden Einfluss auf die Vorgänge im Zusammenhang mit der Erhebung und Übermittlung der personenbezogenen Daten der Besucher seiner Website an Facebook ausgeübt und somit gemeinsam mit Facebook die Mittel dieser Verarbeitung bestimmt hat.[30]

68. Es sei nachdrücklich betont, dass **die Nutzung eines gemeinsamen Datenverarbeitungssystems oder einer gemeinsamen Datenverarbeitungsinfrastruktur nicht in allen Fällen dazu führen wird, dass die beteiligten Parteien als gemeinsam Verantwortliche eingestuft werden**, insbesondere wenn die von ihnen vorgenommene Verarbeitung abtrennbar ist und von einer Partei ohne Eingreifen der anderen durchgeführt werden könnte oder wenn der Anbieter in Ermangelung eines eigenen verfolgten Zwecks ein Auftragsverarbeiter ist (das Vorliegen eines reinen kommerziellen Nutzens für die beteiligten Parteien reicht nicht aus, um als Verarbeitungszweck zu gelten).

Beispiel: Reisebüro

Ein Reisebüro übermittelt der Fluggesellschaft und einer Hotelkette personenbezogene Daten seiner Kunden, um eine Pauschalreise zu buchen. Fluggesellschaft und Hotel bestätigen die Verfügbarkeit der angefragten Plätze und Zimmer. Das Reisebüro stellt die Reisedokumente und Gutscheine für seine Kunden aus. Jeder der Akteure verarbeitet die Daten für seine eigenen Tätigkeiten und mit eigenen Mitteln. In diesem Fall sind Reisebüro, Fluggesellschaft und Hotel drei verschiedene Verantwortliche, die die Daten für ihre eigenen und getrennten Zwecke verarbeiten; es besteht keine gemeinsame Verantwortlichkeit.

Das Reisebüro, die Hotelkette und die Fluggesellschaft beschließen dann, sich gemeinsam an der Einrichtung einer gemeinsamen Internet-Plattform für den gemeinsamen Zweck des Anbietens von Pauschalreisen zu beteiligen. Sie einigen sich auf die wesentlichen Mittel, die eingesetzt werden sollen, z. B. welche Daten gespeichert werden, wie Reservierungen zugewiesen und bestätigt werden und wer Zugang zu den gespeicherten Informationen haben kann. Darüber hinaus beschließen sie, die Daten ihrer Kunden gemeinsam zu nutzen, um gemeinsame Marketingmaßnahmen durchzuführen. In diesem Fall legen Reisebüro, Fluggesellschaft und Hotelkette gemeinsam fest, warum und wie personenbezogene Daten ihrer jeweiligen Kunden verarbeitet werden, und sind daher gemeinsam Verantwortliche für Verarbeitungen in Zusammenhang mit der gemeinsamen internetgestützten Buchungsplattform und den gemeinsamen Marketingmaßnahmen. Jede von ihnen würde jedoch weiterhin die alleinige Kontrolle über andere Verarbeitungstätigkeiten außerhalb der internetbasierten gemeinsamen Plattform behalten.

[30] Urteil *Fashion ID*, C-40/17, ECLI: EU: 2018: 1039, Rn. 77-79.

Beispiel: Forschungsprojekt von Instituten

Mehrere Forschungsinstitute beschließen, sich an einem konkreten gemeinsamen Forschungsprojekt zu beteiligen und zu diesem Zweck die bestehende Plattform eines der am Projekt beteiligten Institute zu nutzen. Jedes Institut gibt bereits in seinem Besitz befindliche personenbezogene Daten in die Plattform für Zwecke der gemeinsamen Forschung ein und nutzt für die Durchführung der Forschungsarbeiten die von anderen über die Plattform bereitgestellten Daten. In diesem Fall gelten alle Institute als gemeinsam Verantwortliche für die Verarbeitung personenbezogener Daten in Form von Speicherung und Weitergabe von Informationen aus dieser Plattform, da sie gemeinsam über den Zweck der Verarbeitung und die zu verwendenden Mittel (die bestehende Plattform) entschieden haben. Jedes Institut ist jedoch ein eigenständiger Verantwortlicher für jede andere Verarbeitung, die außerhalb der Plattform für seine jeweiligen Zwecke durchgeführt werden kann.

Beispiel: Werbekampagne

Die Unternehmen A und B haben gemeinsam ein Markenprodukt C auf den Markt gebracht und möchten zur Bewerbung dieses Produkts eine Veranstaltung organisieren. Zu diesem Zweck beschließen sie, Daten aus ihrer jeweiligen Datenbank zu aktuellen und künftigen Kunden gemeinsam zu nutzen und auf dieser Grundlage über die Liste der Teilnehmer an der Veranstaltung zu entscheiden. Ferner einigen sie sich auf die Modalitäten für die Versendung der Einladungen zu der Veranstaltung, die Art und Weise, wie Rückmeldungen während der Veranstaltung eingeholt werden können, und die nachfolgenden Vermarktungsmaßnahmen. Die Unternehmen A und B können als gemeinsam Verantwortliche für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Organisation der Werbeveranstaltung betrachtet werden, da sie gemeinsam über den gemeinsam festgelegten Zweck und die wesentlichen Mittel der Datenverarbeitung in diesem Zusammenhang entscheiden.

Beispiel: Klinische Studien[31]

Ein Gesundheitsdienstleister (der Prüfer) und eine Hochschule (der Sponsor) beschließen, gemeinsam eine klinische Studie zu demselben Zweck einzuleiten. Sie arbeiten gemeinsam an der Ausarbeitung des Studienprotokolls (d. h. Zweck, Methodik/Konzeption der Studie, zu erhebende Daten, Kriterien für den Ausschluss/die Einbeziehung der Probanden, ggf. Weiterverwendung der Datenbank usw.). Sie können als gemeinsam Verantwortliche für diese klinische Studie betrachtet werden, da sie gemeinsam denselben Zweck und die wesentlichen Mittel für die Verarbeitung festlegen und vereinbaren. Die Erhebung personenbezogener Daten aus der Patientenakte zu Forschungszwecken ist von der Speicherung und Verwendung derselben Daten für die Zwecke der Patientenversorgung zu unterscheiden, für die der Gesundheitsdienstleister weiterhin der Verantwortliche bleibt.

Nimmt der Prüfer nicht an der Ausarbeitung des Prüfplans teil (er akzeptiert lediglich den vom Sponsor bereits ausgearbeiteten Prüfplan), und wird der Prüfplan nur vom Sponsor konzipiert, so sollte der Prüfer als Auftragsverarbeiter und der Sponsor als Verantwortlicher für diese klinische Prüfung betrachtet werden.

[31] Der EDSA plant, im Zusammenhang mit seinen künftigen Leitlinien für die Verarbeitung personenbezogener Daten für medizinische und wissenschaftliche Forschungszwecke weitere Leitlinien für klinische Prüfungen bereitzustellen.

Beispiel: Headhunter

Unternehmen X hilft Unternehmen Y bei der Einstellung neuer Mitarbeiter – mit seinem berühmten Mehrwertdienst „global matchz“. Unternehmen X sucht geeignete Bewerber sowohl unter den Lebensläufen, die es vom Unternehmen Y direkt erhalten hat, als auch denjenigen, die es bereits in seiner eigenen Datenbank hat. Diese Datenbank wird von Unternehmen X allein erstellt und verwaltet. Dadurch wird sichergestellt, dass Unternehmen X Stellenangebote und Arbeitssuchende besser miteinander abgleichen kann und so seine Einnahmen erhöht. Auch wenn sie keine förmliche gemeinsame Entscheidung getroffen haben, beteiligen sich die Unternehmen X und Y gemeinsam an der Verarbeitung, um geeignete Kandidaten auf der Grundlage konvergierender Entscheidungen zu finden: der Entscheidung von Unternehmen X, den Dienst „global matchz“ ins Leben zu rufen und zu verwalten, und der Entscheidung des Unternehmens Y, die direkt bei ihm eingehenden Lebensläufe in die Datenbank einzupflegen. Diese Entscheidungen ergänzen einander, sind nicht voneinander zu trennen und für die Suche nach geeigneten Bewerbern erforderlich. Daher sollten sie in diesem besonderen Fall als gemeinsam Verantwortliche für eine solche Verarbeitung betrachtet werden. Unternehmen X ist jedoch der alleinige Verantwortliche für die Verarbeitung, die für die Verwaltung seiner Datenbank erforderlich ist, und Unternehmen Y ist der alleinige Verantwortliche für das anschließende Einstellungsverfahren für seinen eigenen Zweck (Organisation von Vorstellungsgesprächen, Abschluss des Vertrags und Verwaltung von Personaldaten).

Beispiel: Analyse von Gesundheitsdaten

Unternehmen ABC, Entwickler einer App für Blutdrucküberwachung, und Unternehmen XYZ, Anbieter von Apps für medizinische Fachkräfte, möchten beide untersuchen, wie Blutdruckveränderungen zur Vorhersage bestimmter Krankheiten beitragen können. Die Unternehmen beschließen, ein gemeinsames Projekt ins Leben zu rufen und beim Krankenhaus DEF anzufragen, ob es sich ebenfalls beteiligen möchte.

Bei den personenbezogenen Daten, die im Rahmen dieses Projekts verarbeitet werden, handelt es sich um personenbezogene Daten, die das Unternehmen ABC, das Krankenhaus DEF und das Unternehmen XYZ jeweils als einzelne für die Verarbeitung Verantwortliche verarbeiten. Die Entscheidung, diese Daten zur Beurteilung von Blutdruckänderungen zu verarbeiten, wird von den drei Akteuren gemeinsam getroffen. Das Unternehmen ABC, das Krankenhaus DEF und das Unternehmen XYZ haben die Zwecke der Verarbeitung gemeinsam festgelegt. Unternehmen XYZ ergreift die Initiative und schlägt die wesentlichen Mittel zur Verarbeitung vor. Sowohl das Unternehmen ABC als auch das Krankenhaus DEF akzeptieren diese wesentlichen Mittel, nachdem sie ebenfalls an der Entwicklung einiger Funktionen der App beteiligt waren, sodass die Ergebnisse von ihnen ausreichend genutzt werden können. Die drei Organisationen einigen sich somit auf einen gemeinsamen Zweck für die Verarbeitung, nämlich die Beurteilung, inwieweit Veränderungen des Blutdrucks zur Vorhersage bestimmter Krankheiten beitragen können. Nach Abschluss der Forschungsarbeiten können das Unternehmen ABC, das Krankenhaus DEF und das Unternehmen XYZ von der Beurteilung profitieren, indem sie deren Ergebnisse im Rahmen ihrer eigenen Tätigkeiten verwenden. Aus all diesen Gründen gelten sie für diese konkrete gemeinsame Verarbeitung als gemeinsam Verantwortliche.

Wäre Unternehmen XYZ von den anderen lediglich gebeten worden, diese Beurteilung vorzunehmen, ohne einen eigenen Zweck zu verfolgen, und hätte es lediglich Daten für die anderen verarbeitet, würde das Unternehmen XYZ als Auftragsverarbeiter gelten, selbst wenn es mit der Festlegung der nicht wesentlichen Mittel betraut worden wäre.

3.2.3 Situationen, in denen keine gemeinsame Verantwortlichkeit vorliegt

69. Die Tatsache, dass mehrere Akteure an ein und derselben Verarbeitung beteiligt sind, bedeutet nicht, dass sie zwangsläufig als für diese Verarbeitung gemeinsam Verantwortliche handeln. Nicht alle Arten von Partnerschaft, Kooperation oder Zusammenarbeit implizieren eine Einstufung als gemeinsam Verantwortliche, da eine solche Einstufung eine Einzelfallanalyse der jeweiligen Verarbeitung und der genauen Rolle jeder Stelle in Bezug auf die einzelnen Verarbeitungen erfordert. Die nachstehend geschilderten Fälle sind nicht abschließende Beispiele für Situationen, in denen es keine gemeinsame Verantwortlichkeit gibt.

70. So sollte beispielsweise der Austausch derselben Daten oder desselben Datensatzes zwischen zwei Stellen ohne gemeinsam festgelegte Zwecke oder gemeinsam festgelegte Mittel der Verarbeitung als Übermittlung von Daten zwischen getrennten Verantwortlichen betrachtet werden.

Beispiel: Übermittlung von Arbeitnehmerdaten an die Steuerbehörden

Ein Unternehmen erhebt und verarbeitet personenbezogene Daten seiner Mitarbeiter zum Zweck der Verwaltung von Gehältern, Krankenversicherungsbeiträgen usw. Ein Gesetz verpflichtet das Unternehmen, alle Gehaltsdaten an die Steuerbehörden zu übermitteln, um die Steuerkontrolle zu stärken.

Obwohl in diesem Fall sowohl das Unternehmen als auch die Steuerbehörden dieselben Gehaltsdaten verarbeiten, führt das Fehlen gemeinsam festgelegter Zwecke und Mittel in Bezug auf diese Datenverarbeitung dazu, dass die beiden Stellen als zwei getrennte für die Verarbeitung Verantwortliche eingestuft werden.

71. Eine gemeinsame Verantwortlichkeit kann auch dann ausgeschlossen werden, wenn mehrere Stellen eine gemeinsame Datenbank oder eine gemeinsame Infrastruktur nutzen, sofern jede Stelle ihre eigenen Zwecke eigenständig festlegt.

Beispiel: Marketingmaßnahmen in einer Unternehmensgruppe, die eine gemeinsame Datenbank nutzt:

Eine Unternehmensgruppe nutzt dieselbe Datenbank für die Verwaltung von aktuellen und künftigen Kunden. Diese Datenbank wird auf den Servern der Muttergesellschaft gehostet, die somit in Bezug auf die Speicherung der Daten als Auftragsverarbeiter der einzelnen Unternehmen fungiert. Jedes Unternehmen der Gruppe gibt die Daten seiner eigenen aktuellen und künftigen Kunden ein und verarbeitet diese Daten ausschließlich für eigene Zwecke. Ferner entscheidet jedes Unternehmen unabhängig über den Zugang, die Speicherfristen, die Berichtigung oder Löschung ihrer Daten von aktuellen und künftigen Kunden. Keines der Unternehmen kann auf die Daten des jeweils anderen zugreifen oder sie nutzen. Die bloße Tatsache, dass diese Unternehmen eine gemeinsame Konzerndatenbank nutzen, hat als solche keine gemeinsame Verantwortlichkeit zur Folge. Unter diesen Umständen ist jedes Unternehmen somit ein getrennter Verantwortlicher.

Beispiel: Unabhängige Verantwortliche bei der Nutzung gemeinsamer Infrastruktur

Das Unternehmen XYZ unterhält eine Datenbank und stellt sie anderen Unternehmen für die Verarbeitung und Speicherung personenbezogener Daten über ihre Beschäftigten zur Verfügung. Das Unternehmen XYZ ist im Zusammenhang mit der Verarbeitung und Speicherung der Daten von Beschäftigten anderer Unternehmen Auftragsverarbeiter, da diese Vorgänge im Auftrag und nach den Weisungen dieser anderen Unternehmen durchgeführt werden. Darüber hinaus verarbeiten die

anderen Unternehmen die Daten ohne Beteiligung des Unternehmens XYZ und für Zwecke, die in keiner Weise vom Unternehmen XYZ geteilt werden.

72. Es kommt ferner vor, dass verschiedene Akteure nacheinander in einer Verarbeitungskette dieselben personenbezogenen Daten verarbeiten, wobei jeder dieser Akteure in seinem Teil der Kette einen unabhängigen Zweck verfolgt und unabhängige Mittel einsetzt. In Ermangelung einer gemeinsamen Beteiligung an der Festlegung der Zwecke und Mittel desselben Verarbeitungsvorgangs oder derselben Reihe von Verarbeitungsvorgängen ist eine gemeinsame Verantwortlichkeit auszuschließen und sind die verschiedenen Akteure als aufeinanderfolgende unabhängige Verantwortliche anzusehen.

Beispiel: Statistische Analyse für eine Aufgabe von öffentlichem Interesse

Eine Behörde (Behörde A) hat nach dem Gesetz die Aufgabe, einschlägige Analysen und Statistiken über die Entwicklung der Beschäftigungsquote des Landes zu erstellen. Zu diesem Zweck sind viele andere öffentliche Stellen rechtlich verpflichtet, der Behörde A bestimmte Daten offenzulegen. Behörde A beschließt, für die Verarbeitung der Daten, einschließlich der Erhebung, ein spezielles System zu verwenden. Das bedeutet auch, dass die anderen Stellen verpflichtet sind, für die Offenlegung von Daten dieses System zu verwenden. In diesem Fall wird Behörde A unbeschadet der im Gesetz zugewiesenen Rollen der einzige Verantwortliche sein für die in diesem System erfolgende Datenverarbeitung zum Zweck der Analyse und Statistik hinsichtlich der Beschäftigungsquote, da Behörde A den Zweck der Verarbeitung bestimmt und entschieden hat, wie die Verarbeitung organisiert wird. Selbstverständlich sind die anderen öffentlichen Stellen als Verantwortliche für ihre eigenen Verarbeitungstätigkeiten dafür verantwortlich, die Richtigkeit der zuvor von ihnen verarbeiteten Daten zu gewährleisten, die sie dann an die Behörde A weitergeben.

4 DEFINITION DES AUFTRAGSVERARBEITERS

73. „Auftragsverarbeiter“ ist nach Artikel 4 Nr. 8 DSGVO „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Ähnlich wie bei der Definition des Begriffs des „Verantwortlichen“ sieht die Definition des Begriffs „Auftragsverarbeiter“ ein breites Spektrum von Akteuren vor – es kann sich um „*eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle*“ handeln. Das bedeutet, dass es grundsätzlich keine Beschränkung hinsichtlich der Art des Akteurs gibt, der die Rolle eines Auftragsverarbeiters übernehmen kann. Es kann sich um eine Organisation, aber auch um eine Einzelperson handeln.

74. In der DSGVO sind Verpflichtungen festgelegt, die speziell für Auftragsverarbeiter gelten, wie in Teil II Abschnitt 1 dieser Leitlinien näher ausgeführt wird. Ein Auftragsverarbeiter kann haftbar gemacht oder mit einer Geldbuße belegt werden, wenn er seinen Pflichten nicht nachkommt oder wenn er außerhalb der rechtmäßigen Anweisungen des Verantwortlichen handelt oder gegen diese verstößt.

75. An der Verarbeitung personenbezogener Daten können mehrere Auftragsverarbeiter beteiligt sein. So kann beispielsweise ein Verantwortlicher selbst entscheiden, mehrere Auftragsverarbeiter direkt zu beauftragen, indem er verschiedene Auftragsverarbeiter in verschiedenen Phasen der Verarbeitung einbezieht (mehrere Auftragsverarbeiter). Ein Verantwortlicher kann aber auch beschließen, einen Auftragsverarbeiter zu beauftragen, der seinerseits – mit Zustimmung des Verantwortlichen – einen oder mehrere andere Auftragsverarbeiter („Unterauftragsverarbeiter“) beauftragt. Die einem Auftragsverarbeiter übertragene Verarbeitungstätigkeit kann auf eine ganz konkrete Aufgabe oder einen ganz bestimmten Kontext beschränkt oder auch allgemeiner und umfassender sein.

76. Es bestehen zwei grundlegende Voraussetzungen für die Einstufung als Auftragsverarbeiter:

a) Er muss eine vom Verantwortlichen *getrennte Stelle* sein und

b) er muss personenbezogene Daten *im Auftrag des Verantwortlichen* verarbeiten.

77. Der Ausdruck *getrennte Stelle* bedeutet, dass der Verantwortliche beschließt, die Verarbeitungstätigkeiten ganz oder teilweise an eine externe Organisation zu delegieren. Innerhalb einer Unternehmensgruppe kann ein Unternehmen Auftragsverarbeiter für ein anderes Unternehmen sein, das als Verantwortlicher fungiert, da es sich bei beiden Unternehmen um getrennte Einheiten handelt. Dagegen kann eine Abteilung innerhalb eines Unternehmens nicht Auftragsverarbeiter für eine andere Abteilung innerhalb desselben Unternehmens sein.

78. Beschließt der Verantwortliche, Daten selbst zu verarbeiten, indem er seine eigenen Ressourcen innerhalb seiner Organisation nutzt, beispielsweise sein eigenes Personal, kann hier nicht von Auftragsverarbeitung gesprochen werden. Beschäftigte und andere Personen, die unter der unmittelbaren Aufsicht des Verantwortlichen handeln, wie z. B. vorübergehend angestellte Mitarbeiter, gelten nicht als Auftragsverarbeiter, da sie personenbezogene Daten als Teil der Einheit des Verantwortlichen verarbeiten. Gemäß Artikel 29 sind auch sie an die Weisungen des Verantwortlichen gebunden.

79. *Die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen* setzt zunächst voraus, dass die getrennte Stelle personenbezogene Daten zugunsten des Verantwortlichen verarbeitet. In Artikel 4 Nr. 2 wird der Begriff „Verarbeitung“ definiert als ein breites Spektrum von Vorgängen, die vom Erheben, der Speicherung und dem Abfragen bis zur Verwendung, Verbreitung oder anderen Form der Bereitstellung und der Vernichtung reichen. Auf den Begriff „Verarbeitung“ wird weiter oben unter 2.1.5 näher eingegangen.

80. Zweitens muss die Verarbeitung im Auftrag eines Verantwortlichen erfolgen, nicht jedoch unter seiner unmittelbaren Aufsicht oder Kontrolle. Handeln „im Auftrag“ bedeutet, dem Interesse eines anderen zu dienen, und erinnert an das Rechtskonzept der „Delegation“. Im Bereich des Datenschutzrechts muss ein Auftragsverarbeiter die Weisungen des Verantwortlichen zumindest in Bezug auf den Zweck der Verarbeitung und die wesentlichen Elemente der Mittel umsetzen. Die Rechtmäßigkeit der Verarbeitung gemäß Artikel 6 und gegebenenfalls Artikel 9 der Verordnung leitet sich aus der Tätigkeit des Verantwortlichen ab, und der Auftragsverarbeiter darf die Daten nicht anders als nach den Weisungen des Verantwortlichen verarbeiten. Dennoch können, wie oben beschrieben, die Weisungen des Verantwortlichen einen gewissen Ermessensspielraum hinsichtlich der Frage lassen, wie den Interessen des Verantwortlichen am besten gedient werden kann, so dass der Auftragsverarbeiter die geeignetsten technischen und organisatorischen Mittel auswählen kann.[32]

81. Das Handeln „im Auftrag von“ bedeutet auch, dass der Auftragsverarbeiter keine Verarbeitung für seine(n) eigene(n) Zweck(e) vornehmen darf. Gemäß Artikel 28 Absatz 10 verstößt ein Auftragsverarbeiter gegen die DSGVO, wenn er über die Weisungen des Verantwortlichen hinausgeht und beginnt, seine eigenen Zwecke und Mittel der Verarbeitung zu bestimmen. Der Auftragsverarbeiter gilt dann in Bezug auf diese Verarbeitung als Verantwortlicher und kann wegen der Überschreitung der Weisungen des Verantwortlichen mit Sanktionen belegt werden.

Beispiel: Diensteanbieter, der als Datenverarbeiter bezeichnet wird, aber als Verantwortlicher handelt

[32] Siehe Teil I Unterabschnitt 2.1.4 zur Unterscheidung zwischen wesentlichen und nicht wesentlichen Mitteln.

Der Dienstleister MarketinZ erbringt Dienstleistungen im Bereich Werbung und Direktmarketing für verschiedene Unternehmen. Das Unternehmen GoodProductZ schließt einen Vertrag mit MarketinZ, dem zufolge das letztgenannte Unternehmen kommerzielle Werbung für GoodProductZ-Kunden anbietet und als Datenverarbeiter bezeichnet wird. MarketinZ beschließt jedoch, die Kundendatenbank von GoodProducts auch für andere Zwecke als die Werbung für GoodProducts zu nutzen, wie z. B. den Ausbau der eigenen Geschäftstätigkeit. Durch die Entscheidung, dem Zweck, für den die personenbezogenen Daten übermittelt wurden, einen weiteren Zweck hinzuzufügen, wird MarketinZ für diese Reihe von Verarbeitungen zum Verantwortlichen, und seine Verarbeitungstätigkeit zu diesem Zweck wäre ein Verstoß gegen die DSGVO.

82. Der EDSA erinnert daran, dass nicht jeder Diensteanbieter, der im Zuge der Erbringung einer Dienstleistung personenbezogene Daten verarbeitet, ein „Auftragsverarbeiter" im Sinne der DSGVO ist. Die Rolle eines Auftragsverarbeiters ergibt sich nicht aus der Art einer Stelle, die Daten verarbeitet, sondern aus ihren konkreten Tätigkeiten in einem bestimmten Kontext. Mit anderen Worten: Ein und dieselbe Stelle kann gleichzeitig bei bestimmten Verarbeitungsvorgängen als Verantwortlicher und bei anderen als Auftragsverarbeiter fungieren, und die Einstufung als Verantwortlicher oder als Auftragsverarbeiter muss mit Blick auf konkrete Datensätze oder Vorgänge geprüft werden. Die Art der Dienstleistung bestimmt, ob die Verarbeitungstätigkeit eine Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen im Sinne der DSGVO darstellt. In der Praxis kann der Diensteanbieter in Fällen, in denen die erbrachte Dienstleistung nicht speziell auf die Verarbeitung personenbezogener Daten abzielt oder diese Verarbeitung kein Schlüsselelement der Dienstleistung darstellt, in der Lage sein, die Zwecke und Mittel dieser Verarbeitung, die für die Erbringung der Dienstleistung erforderlich sind, selbst zu bestimmen. In diesem Fall ist der Diensteanbieter als eigenständiger Verantwortlicher und nicht als Auftragsverarbeiter anzusehen.[33] Eine Einzelfallanalyse ist jedoch weiterhin erforderlich, um festzustellen, in welchem Maße jede Stelle tatsächlich Einfluss auf die Zwecke und Mittel der Verarbeitung hat.

Beispiel: Taxidienst

Ein Taxidienst bietet eine Online-Plattform an, auf der Unternehmen ein Taxi buchen können, um Mitarbeiter oder Gäste zum und vom Flughafen zu befördern. Bei der Buchung eines Taxis gibt das Unternehmen ABC den Namen des Mitarbeiters an, der am Flughafen abgeholt werden soll, damit der Fahrer die Identität des Mitarbeiters zum Zeitpunkt der Abholung bestätigen kann. In diesem Fall verarbeitet der Taxidienst personenbezogene Daten des Mitarbeiters als Teil seiner Dienstleistung für das Unternehmen ABC, doch ist die Verarbeitung als solche nicht Ziel der Dienstleistung. Der Taxidienst hat die Online-Buchungsplattform als Teil der Entwicklung seiner eigenen Geschäftstätigkeit für die Erbringung von Beförderungsdienstleistungen ohne jegliche Weisungen von Unternehmen ABC konzipiert. Ferner legt der Taxidienst selbständig fest, welche Kategorien von Daten er erhebt und wie lange er die Daten speichert. Der Taxidienst handelt daher eigenständig als Verantwortlicher, ungeachtet der Tatsache, dass die Verarbeitung nach einem Serviceersuchen von Unternehmen ABC erfolgt.

83. Der EDSA stellt fest, dass ein Diensteanbieter auch dann als Auftragsverarbeiter handeln kann, wenn die Verarbeitung personenbezogener Daten nicht der hauptsächliche oder vorrangige Gegenstand der Dienstleistung ist, sofern der Dienstleistungsempfänger weiterhin über die Zwecke und Mittel der

[33] Siehe auch Erwägungsgrund 81 DSGVO, der von der *Betrauung eines Auftragsverarbeiters mit Verarbeitungstätigkeiten* spricht und darauf hinweist, dass die Verarbeitungstätigkeit als solche ein wichtiger Bestandteil der Entscheidung des Verantwortlichen ist, von einem Auftragsverarbeiter zu verlangen, personenbezogene Daten in seinem Auftrag zu verarbeiten.

Verarbeitung in der Praxis entscheidet. Bei der Prüfung der Frage, ob ein bestimmter Diensteanbieter mit der Verarbeitung personenbezogener Daten betraut werden soll, sollten Verantwortliche sorgfältig prüfen, ob der betreffende Diensteanbieter ihnen unter Berücksichtigung der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der potenziellen Risiken für betroffene Personen ein ausreichendes Maß an Kontrolle ermöglicht.

Beispiel: Callcenter

Unternehmen X lagert seine Kundenbetreuung an Unternehmen Y aus, das ein Callcenter bereitstellt, das den Kunden von Unternehmen X bei ihren Fragen weiterhilft. Die Kundenbetreuung bringt es mit sich, dass Unternehmen Y Zugang zu den Kundendatenbanken von Unternehmen X haben muss. Unternehmen Y kann nur auf Daten zugreifen, um die von Unternehmen X in Auftrag gegebene Betreuung zu leisten, und es darf keine Daten für andere als die von Unternehmen X angegebenen Zwecke verarbeiten. Unternehmen Y ist als Auftragsverarbeiter für personenbezogene Daten zu betrachten, und die Unternehmen X und Y müssen eine Auftragsverarbeitungsvereinbarung schließen.

Beispiel: Allgemeine IT-Dienstleistungen

Unternehmen Z beauftragt einen IT-Dienstleister mit dem allgemeinen Support seiner IT-Systeme, die große Mengen personenbezogener Daten enthalten. Der Zugang zu personenbezogenen Daten ist nicht Hauptgegenstand der Support-Dienstleistung, doch ist es unvermeidlich, dass der IT-Dienstleister bei der Erbringung der Dienstleistung systematisch Zugang zu personenbezogenen Daten hat. Unternehmen Z kommt daher zu dem Schluss, dass der IT-Dienstleister – ein eigenständiges Unternehmen, das zwangsläufig personenbezogene Daten verarbeiten muss, obwohl dies nicht der Hauptzweck der Dienstleistung ist – als Auftragsverarbeiter anzusehen ist. Daher wird mit dem IT-Dienstleister eine Auftragsverarbeitungsvereinbarung geschlossen.

Beispiel: IT-Berater, der einen Software-Fehler behebt

Unternehmen ABC engagiert einen IT-Spezialisten eines anderen Unternehmens, um einen Fehler in einer Software zu beheben, die von dem Unternehmen verwendet wird. Der IT-Berater ist nicht engagiert, um personenbezogene Daten zu verarbeiten, und das Unternehmen ABC stellt fest, dass ein Zugriff auf personenbezogene Daten nur zufällig erfolgt und daher in der Praxis sehr begrenzt sein wird. ABC kommt daher zu dem Schluss, dass der IT-Spezialist weder Auftragsverarbeiter (noch eigenständiger Verantwortlicher) ist und dass das Unternehmen ABC geeignete Maßnahmen gemäß Artikel 32 DSGVO ergreifen wird, um den IT-Berater daran zu hindern, personenbezogene Daten auf unbefugte Weise zu verarbeiten.

84. Wie bereits erwähnt, hindert nichts den Auftragsverarbeiter daran, eine im Voraus festgelegte Dienstleistung anzubieten, doch muss der Verantwortliche die endgültige Entscheidung treffen, die Art und Weise der Verarbeitung aktiv zu billigen, zumindest was die wesentlichen Mittel der Verarbeitung betrifft. Wie bereits erwähnt, verfügt ein Auftragsverarbeiter über einen Handlungsspielraum in Bezug auf die nicht wesentlichen Mittel (siehe weiter oben Abschnitt 2.1.4).

Beispiel: Cloud-Dienstleister

Eine Gemeinde hat beschlossen, einen Cloud-Dienstleister für die Informationsverarbeitung in ihrem Schul- und Bildungsangebot einzusetzen. Der Cloud-Dienst bietet Messaging-Services, Videokonferenzen, Speicherung von Dokumenten, Kalenderverwaltung, Textverarbeitung usw. und

beinhaltet die Verarbeitung personenbezogener Daten über Schüler und Lehrkräfte. Der Cloud-Dienstleister hat einen standardisierten Dienst angeboten, der weltweit angeboten wird. Die Gemeinde muss jedoch sicherstellen, dass die bestehende Vereinbarung mit Artikel 28 Absatz 3 DSGVO in Einklang steht und dass die personenbezogenen Daten, für die sie verantwortlich ist, ausschließlich für die Zwecke der Gemeinde verarbeitet werden. Sie muss außerdem sicherstellen, dass ihre konkreten Weisungen zu Speicherfristen, Löschung von Daten usw. vom Cloud-Dienstleister eingehalten werden, unabhängig davon, was im Rahmen des standardisierten Dienstes allgemein angeboten wird.

5 DEFINITION DES BEGRIFFS „DRITTER/EMPFÄNGER“

85. In der Verordnung werden nicht nur die Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“ definiert, sondern auch die Begriffe „Empfänger“ und „Dritter“. Im Gegensatz zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ legt die Verordnung keine besonderen Verpflichtungen oder Verantwortlichkeiten für Empfänger und Dritte fest. Dabei handelt es sich um relative Begriffe in dem Sinne, dass sie eine Beziehung zu einem Verantwortlichen oder Auftragsverarbeiter aus einer bestimmten Perspektive beschreiben, z. B. wenn ein Verantwortlicher oder ein Auftragsverarbeiter Daten gegenüber einem Empfänger offenlegt. Ein Empfänger personenbezogener Daten und ein Dritter können aus anderen Blickwinkeln durchaus gleichzeitig als Verantwortlicher oder Auftragsverarbeiter angesehen werden. Beispielsweise sind Stellen, die aus einer Perspektive als Empfänger oder Dritte zu betrachten sind, Verantwortliche für die Verarbeitung, für die sie den Zweck und die Mittel bestimmen.

Dritter

86. In Artikel 4 Nr. 10 wird der Begriff „*Dritter*“ definiert als „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle außer

- der betroffenen Person,
- dem Verantwortlichen,
- dem Auftragsverarbeiter und
- den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

87. Die Definition entspricht insgesamt der früheren Definition des Begriffs „*Dritter*“ in der Richtlinie 95/46/EG.

88. Während die Begriffe „*personenbezogene Daten*“, „*betroffene Person*“, „*Verantwortlicher*“ und „*Auftragsverarbeiter*“ in der Verordnung definiert sind, ist der Begriff „*Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, personenbezogene Daten zu verarbeiten*“ nicht definiert. Er wird jedoch im Allgemeinen so verstanden, dass er sich auf Personen bezieht, die zur rechtlichen Einheit des Verantwortlichen oder des Auftragsverarbeiters gehören (also Beschäftigter sind oder eine mit der Rolle von Beschäftigten in hohem Maße vergleichbare Rolle haben, z. B. Zeitarbeitskräfte, die über ein Leiharbeitsunternehmen bereitgestellt werden), jedoch nur insoweit, als sie zur Verarbeitung personenbezogener Daten befugt sind. Ein Beschäftigter usw., der Zugang zu Daten erlangt, zu denen er keinen Zugang haben darf, und dies für andere Zwecke als denen des Arbeitgebers, fällt nicht unter diese Kategorie. Vielmehr sollte dieser Beschäftigte mit Blick auf die vom Arbeitgeber vorgenommene Verarbeitung als Dritter betrachtet werden. Soweit der Beschäftigte personenbezogene Daten für eigene Zwecke verarbeitet,

die sich von denen seines Arbeitgebers unterscheiden, wird er als Verantwortlicher betrachtet und übernimmt alle sich daraus ergebenden Konsequenzen und Pflichten in Bezug auf die Verarbeitung personenbezogener Daten.[34]

89. Der Ausdruck „Dritter" bezeichnet somit eine Person, die in der konkreten Situation weder eine betroffene Person noch ein Verantwortlicher, Auftragsverarbeiter oder Beschäftigter ist. Beispielsweise kann der Verantwortliche einen Auftragsverarbeiter beauftragen und ihn anweisen, personenbezogene Daten an einen Dritten zu übermitteln. Dieser Dritte gilt dann als eigenständiger Verantwortlicher für die Verarbeitung, die er für seine eigenen Zwecke durchführt. Es sei darauf hingewiesen, dass innerhalb einer Unternehmensgruppe ein anderes Unternehmen als der Verantwortliche oder der Auftragsverarbeiter ein Dritter ist, auch wenn es zur selben Unternehmensgruppe gehört wie das Unternehmen, das als Verantwortlicher oder Auftragsverarbeiter tätig ist.

Beispiel: Reinigungsdienstleistungen

Unternehmen A schließt mit einem Reinigungsunternehmen einen Vertrag über die Reinigung seiner Büros ab. Die Reinigungskräfte sollen nicht auf personenbezogene Daten zugreifen oder sie anderweitig verarbeiten. Auch wenn sie gelegentlich beim Reinigen der Büros auf solche Daten stoßen, können sie ihre Aufgabe erfüllen, ohne auf Daten zuzugreifen, und es ist ihnen vertraglich untersagt, auf personenbezogene Daten, die Unternehmen A als Verantwortlicher aufbewahrt, zuzugreifen oder sie anderweitig zu verarbeiten. Die Reinigungskräfte sind weder bei Unternehmen A angestellt noch gelten sie als diesem Unternehmen direkt unterstellt. Es besteht keine Absicht, das Reinigungsunternehmen oder seine Mitarbeiter mit der Verarbeitung personenbezogener Daten im Namen von Unternehmen A zu beauftragen. Das Reinigungsunternehmen und seine Mitarbeiter sind daher als Dritte anzusehen, und der Verantwortliche muss sicherstellen, dass angemessene Sicherheitsmaßnahmen ergriffen werden, um den Zugang zu Daten zu verhindern, und er muss eine Vertraulichkeitspflicht für den Fall vorsehen, dass die Reinigungskräfte zufällig auf personenbezogene Daten stoßen.

Beispiel: Unternehmensgruppen – Muttergesellschaft und Tochtergesellschaften

Die Unternehmen X und Y sind Teil der Gruppe Z. Die Unternehmen X und Y verarbeiten Daten über ihre jeweiligen Beschäftigten für Zwecke der Personalverwaltung. Zu einem bestimmten Zeitpunkt beschließt die Muttergesellschaft ZZ, für die Erstellung gruppenweiter Statistiken Beschäftigtendaten von allen Tochtergesellschaften anzufordern. Bei der Übermittlung von Daten von den Gesellschaften X und Y an die Muttergesellschaft ZZ ist letztere unabhängig davon, ob alle Gesellschaften derselben Gruppe angehören, als Dritter anzusehen. Das Unternehmen ZZ gilt als für die Verarbeitung der Daten für statistische Zwecke Verantwortlicher.

Empfänger

90. In Artikel 4 Nr. 9 ist „*Empfänger*" definiert als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden gelten jedoch nicht als Empfänger,

[34] Der Arbeitgeber (als ursprünglich Verantwortlicher) könnte dennoch eine gewisse Verantwortung behalten, falls die neue Verarbeitung aufgrund mangelnder angemessener Sicherheitsmaßnahmen erfolgt.

wenn sie personenbezogene Daten im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erhalten (z. B. Steuer- und Zollbehörden, Finanzermittlungsstellen usw.).[35]

91. Die Definition entspricht im Großen und Ganzen der früheren Definition des Begriffs *Empfänger* in der Richtlinie 95/46/EG.

92. Die Definition erfasst jeden, der personenbezogene Daten erhält, unabhängig davon, ob es sich um einen Dritten handelt oder nicht. Übermittelt ein Verantwortlicher beispielsweise personenbezogene Daten an eine andere Stelle, sei es ein Auftragsverarbeiter oder ein Dritter, so ist diese Stelle Empfänger. Ein Dritter, der Daten empfängt, gilt als Verantwortlicher für jede Verarbeitung, die er für (einen) eigene(n) Zweck(e) durchführt, nachdem er die Daten erhalten hat.

Beispiel: Offenlegung von Daten zwischen Unternehmen

Das Reisebüro ExploreMore organisiert auf Wunsch seiner Kunden Reisen. Im Rahmen dieser Dienstleistung übermittelt es personenbezogene Daten von Kunden an Fluggesellschaften, Hotels und Anbieter von Ausflügen, damit diese ihre jeweiligen Dienstleistungen erbringen können. ExploreMore, die Hotels, die Fluggesellschaften und die Anbieter von Ausflügen sind jeweils als Verantwortliche für die Verarbeitung anzusehen, die sie im Rahmen ihrer jeweiligen Dienstleistung durchführen. Es gibt keine Beziehung zwischen einem Verantwortlichem und einem Auftragsverarbeiter. Fluggesellschaften, Hotels und Anbieter von Ausflügen sind jedoch als Empfänger anzusehen, wenn sie die personenbezogenen Daten von ExploreMore erhalten.

TEIL II – FOLGEN DER ZUWEISUNG UNTERSCHIEDLICHER ROLLEN

1 BEZIEHUNG ZWISCHEN VERANTWORTLICHEM UND AUFTRAGSVERARBEITER

93. Ein eigenständiges neues Merkmal der DSGVO sind die Bestimmungen, die Auftragsverarbeitern unmittelbar Verpflichtungen auferlegen. So muss beispielsweise ein Auftragsverarbeiter sicherstellen, dass zur Verarbeitung personenbezogener Daten befugte Personen sich zur Vertraulichkeit verpflichtet haben (Artikel 28 Absatz 3); er muss ein Verzeichnis zu allen Kategorien von Verarbeitungstätigkeiten führen (Artikel 30 Absatz 2), und er muss geeignete technische und organisatorische Maßnahmen treffen (Artikel 32). Ein Auftragsverarbeiter muss ferner unter bestimmten Bedingungen einen Datenschutzbeauftragten benennen (Artikel 37) und ist verpflichtet, den Verantwortlichen unverzüglich zu benachrichtigen, nachdem er Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erlangt hat (Artikel 33 Absatz 2). Darüber hinaus gelten die Vorschriften für die Übermittlung von Daten an Drittländer (Kapitel V) sowohl für Auftragsverarbeiter als auch für Verantwortliche. In diesem Zusammenhang vertritt der EDSA die Auffassung, dass Artikel 28 Absatz 3 DSGVO zwar einen konkreten Inhalt für den erforderlichen Vertrag zwischen Verantwortlichen und Auftragsverarbeiter vorschreibt, den Auftragsverarbeitern aber auch unmittelbar Verpflichtungen auferlegt, einschließlich der Pflicht, den Verantwortlichen bei der Sicherstellung der Einhaltung der Vorschriften zu unterstützen.[36]

[35] Siehe auch Erwägungsgrund 31 DSGVO.

[36] So sollte der Auftragsverarbeiter erforderlichenfalls den Verantwortlichen auf Anfrage bei der Einhaltung der Auflagen im Zusammenhang mit Datenschutz-Folgenabschätzungen unterstützen (Erwägungsgrund 95 DSGVO).

1.1 Auswahl des Auftragsverarbeiters

94. Der Verantwortliche **hat die Pflicht, „nur mit Auftragsverarbeitern zu arbeiten, die hinreichende Garantien für die Anwendung geeigneter technischer und organisatorischer Maßnahmen bieten“**, so dass die Verarbeitung den Anforderungen der DSGVO – auch in Bezug auf die Sicherheit der Verarbeitung – entspricht und den Schutz der Rechte der betroffenen Personen gewährleistet.[37] Es obliegt daher dem Verantwortlichen zu beurteilen, ob die Garantien des Auftragsverarbeiters ausreichend sind, und er sollte nachweisen können, dass er alle in der DSGVO vorgesehenen Elemente ernsthaft berücksichtigt hat.

95. Die Garantien, die der Auftragsverarbeiter „bietet“, sind diejenigen, die der Auftragsverarbeiter **zur Zufriedenheit des Verantwortlichen nachweisen** kann, da diese die einzigen Garantien sind, die der Verantwortliche bei der Prüfung der Erfüllung seiner Pflichten wirksam berücksichtigen kann. Häufig erfordert dies einen Austausch einschlägiger Unterlagen (z. B. Datenschutzerklärung, Dienstleistungsbedingungen, Verzeichnis von Verarbeitungstätigkeiten, Richtlinien zum Dokumentenmanagement, Informationssicherheitskonzept, Berichte über externe Datenschutzaudits, anerkannte internationale Zertifizierungen wie die ISO 27000-Reihe).

96. Die Beurteilung durch den Verantwortlichen, ob die Garantien hinreichend sind, ist eine Form der RisikoBeurteilung, die in hohem Maße von der Art der dem Auftragsverarbeiter anvertrauten Verarbeitung abhängt und von Fall zu Fall unter Berücksichtigung der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen erfolgen muss. Folglich kann der EDSA keine abschließende Liste der Dokumente oder Maßnahmen bereitstellen, die der Auftragsverarbeiter in einem bestimmten Szenario vorlegen oder nachweisen muss, da dies weitgehend von den besonderen Umständen der Verarbeitung abhängt.

97. Folgende Elemente [38] sollte der Verantwortliche berücksichtigen, wenn er der Frage nachgeht, ob die Garantien hinreichend sind: das **Fachwissen** des Auftragsverarbeiters (z. B. technisches Fachwissen im Hinblick auf Sicherheitsmaßnahmen und Verletzungen des Schutzes personenbezogener Daten); die **Zuverlässigkeit** des Auftragsverarbeiters; die **Ressourcen** des Auftragsverarbeiters. Auch der Ruf des Auftragsverarbeiters auf dem Markt kann für den Verantwortlichen ein wichtiger Faktor sein.

98. Darüber hinaus kann die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens als Faktor herangezogen werden, um ausreichende Garantien nachzuweisen.[39] Auftragsverarbeitern wird daher empfohlen, den Verantwortlichen über diesen Umstand sowie über jede Änderung in diesem Zusammenhang in Kenntnis zu setzen.

99. Die in Artikel 28 Absatz 1 DSGVO enthaltene Verpflichtung, ausschließlich Auftragsverarbeiter heranzuziehen, „die hinreichende Garantien bieten“, ist eine kontinuierliche Verpflichtung. Sie endet nicht zu dem Zeitpunkt, zu dem der Verantwortliche und der Auftragsverarbeiter einen Vertrag oder ein anderes Rechtsinstrument abschließen. Vielmehr sollte der Verantwortliche die Garantien des Auftragsverarbeiters in angemessenen Abständen kontrollieren, gegebenenfalls auch durch Überprüfungen und Inspektionen.[40]

Dies muss seinen Niederschlag in dem Vertrag zwischen Verantwortlichem und Auftragsverarbeiter gemäß Artikel 28 Absatz 3 Buchstabe f DSGVO finden.

[37] Artikel 28 Absatz 1 und Erwägungsgrund 81 DSGVO.

[38] Erwägungsgrund 81 DSGVO.

[39] Artikel 28 Absatz 5 und Erwägungsgrund 81 DSGVO.

[40] Siehe auch Artikel 28 Absatz 3 Buchstabe h DSGVO.

1.2 Form des Vertrags oder sonstigen Rechtsinstruments

100. Jede Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zwischen dem Verantwortlichen und dem Auftragsverarbeiter, wie in Artikel 28 Absatz 3 DSGVO vorgeschrieben.

101. Ein solches Rechtsinstrument ist **schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann**.[41] Daher können nicht schriftliche Vereinbarungen (unabhängig davon, wie durchdacht oder wirksam sie sind) nicht als ausreichend gelten, um den Anforderungen von Artikel 28 DSGVO zu genügen. Um Schwierigkeiten beim Nachweis zu vermeiden, dass der Vertrag oder ein anderes Rechtsinstrument tatsächlich in Kraft ist, empfiehlt der EDSA, dafür zu sorgen, dass das Rechtsinstrument mit den nach dem geltenden Recht (z. B. dem Vertragsrecht) erforderlichen Unterschriften versehen ist.

102. Darüber hinaus muss der Vertrag oder das andere Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten **für den Auftragsverarbeiter** in Bezug auf den Verantwortlichen **verbindlich** sein, d. h. er muss dem Auftragsverarbeiter Verpflichtungen auferlegen, die nach dem Unionsrecht oder dem Recht der Mitgliedstaaten verbindlich sind. Außerdem müssen darin die Pflichten des Verantwortlichen niedergelegt werden. In den meisten Fällen wird es sich um einen Vertrag handeln, doch ist in der Verordnung auch von einem „anderen Rechtsinstrument" die Rede, beispielsweise einem Rechtsinstrument nach nationalem (Primär- oder Sekundär-)Recht oder einem anderen Rechtsinstrument. Enthält das Rechtsinstrument nicht den geforderten Mindestinhalt, so muss es durch einen Vertrag oder ein anderes Rechtsinstrument ergänzt werden, das die fehlenden Elemente enthält.

103. Da in der Verordnung eine eindeutige Verpflichtung zum Abschluss eines schriftlichen Vertrags festgelegt ist, wenn kein anderes einschlägiges Rechtsinstrument in Kraft ist, stellt das Fehlen eines solchen Vertrags einen Verstoß gegen die DSGVO dar.[42] Sowohl der Verantwortliche als auch der Auftragsverarbeiter sind dafür verantwortlich, dass die Verarbeitung durch einen Vertrag oder ein anderes Rechtsinstrument geregelt wird.[43] Vorbehaltlich der Bestimmungen von Artikel 83 DSGVO kann die zuständige Aufsichtsbehörde unter Berücksichtigung der Umstände des jeweiligen Einzelfalls sowohl gegen den Verantwortlichen als auch gegen den Auftragsverarbeiter eine Geldbuße verhängen. Verträge, die vor dem Geltungsbeginn der DSGVO geschlossen wurden, hätten im Hinblick auf Artikel 28 Absatz 3 aktualisiert werden müssen. Das Fehlen einer solchen Aktualisierung, um einen

[41] Artikel 28 Absatz 9 DSGVO.

[42] Das Vorhandensein (oder Fehlen) einer schriftlichen Vereinbarung ist jedoch für das Bestehen einer Beziehung zwischen Verantwortlichem und Auftragsverarbeiter nicht entscheidend. Besteht Grund zu der Annahme, dass der Vertrag in Bezug auf die tatsächliche Kontrolle nicht der Realität entspricht, so kann die Vereinbarung auf der Grundlage einer faktischen Analyse der Umstände der Beziehung zwischen den Parteien und der durchgeführten Verarbeitung personenbezogener Daten aufgehoben werden. Umgekehrt kann auch ohne eine schriftliche Verarbeitungsvereinbarung davon ausgegangen werden, dass ein Auftragsverarbeitungsverhältnis besteht. Dies würde jedoch einen Verstoß gegen Artikel 28 Absatz 3 DSGVO bedeuten. Darüber hinaus kann das Fehlen einer klar definierten Beziehung zwischen Verantwortlichem und Auftragsverarbeiter unter bestimmten Umständen das Problem des Fehlens einer Rechtsgrundlage aufwerfen, auf der jede Verarbeitung beruhen sollte, z. B. in Bezug auf die Übermittlung von Daten zwischen dem Verantwortlichen und dem mutmaßlichen Auftragsverarbeiter.

[43] Artikel 28 Absatz 3 gilt nicht nur für Verantwortliche. Wenn nur der Auftragsverarbeiter dem räumlichen Anwendungsbereich der DSGVO unterliegt, gilt die Verpflichtung nur unmittelbar für den Auftragsverarbeiter, siehe auch EDSA-Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO, S. 13.

bereits bestehenden Vertrag mit den Anforderungen der DSGVO in Einklang zu bringen, stellt einen Verstoß gegen Artikel 28 Absatz 3 dar.

Ein schriftlicher Vertrag gemäß Artikel 28 Absatz 3 DSGVO kann in einen umfassenderen Vertrag, beispielsweise eine Dienstleistungsvereinbarung, eingebettet sein. Um den Nachweis der Einhaltung der DSGVO zu erleichtern, empfiehlt der EDSA, dass die Vertragselemente, mit denen Artikel 28 DSGVO umgesetzt werden soll, an einem Ort (z. B. in einem Anhang) eindeutig als solche gekennzeichnet werden.

104. Um der Pflicht zum Abschluss eines Vertrags nachzukommen, können der Verantwortliche und der Auftragsverarbeiter beschließen, ihren eigenen Vertrag auszuhandeln, der alle obligatorischen Elemente enthält**, oder sich in Bezug auf Verpflichtungen nach Artikel 28 ganz oder teilweise auf Standardvertragsklauseln** stützen.[44]

105. Standardvertragsklauseln können alternativ von der Kommission[45] oder einer Aufsichtsbehörde im Einklang mit dem Kohärenzverfahren angenommen werden.[46] Diese Klauseln könnten Teil einer Zertifizierung sein, die dem Verantwortlichen oder dem Auftragsverarbeiter nach den Artikeln 42 oder 43 erteilt wird.[47]

106. Der EDSA möchte klarstellen, dass Verantwortliche und Auftragsverarbeiter weder verpflichtet sind, einen Vertrag auf der Grundlage von Standardvertragsklauseln abzuschließen, noch dass diese zwangsläufig der Aushandlung eines individuellen Vertrags vorzuziehen sind. Beide Optionen sind je nach den besonderen Umständen zum Zweck der Einhaltung des Datenschutzrechts möglich, sofern sie die Anforderungen des Artikel 28 Absatz 3 erfüllen.

107. Wenn die Parteien von Standardvertragsklauseln Gebrauch machen wollen, müssen die Datenschutzklauseln ihrer Vereinbarung mit denen der Standardvertragsklauseln übereinstimmen. Standardvertragsklauseln lassen häufig einige Leerstellen, die von den Parteien ausgefüllt bzw. Optionen, die von den Parteien ausgewählt werden können. Wie bereits erwähnt, dürften Standardvertragsklauseln im Allgemeinen in eine umfassendere Vereinbarung eingebettet sein, in der der Vertragsgegenstand, die finanziellen Bedingungen und andere vereinbarte Klauseln niedergelegt sind: So können die Parteien zusätzliche Klauseln hinzufügen (z. B. zum anwendbaren Recht und zum Gerichtsstand), sofern diese nicht mittelbar oder unmittelbar den Standardvertragsklauseln

[44] Artikel 28 Absatz 6 DSGVO. Der EDSA erinnert daran, dass die Standardvertragsklauseln für die Zwecke der Einhaltung von Artikel 28 DSGVO nicht dieselben sind wie die Standardvertragsklauseln gemäß Artikel 46 Absatz 2. In ersteren wird näher festgelegt und präzisiert, wie die Bestimmungen von Artikel 28 Absätze 3 und 4 erfüllt werden, letztere hingegen sehen geeignete Garantien für den Fall vor, dass personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt werden, wenn kein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt.

[45] Artikel 28 Absatz 7 DSGVO. Artikel 28 Absatz 7 DSGVO. Artikel 28 Absatz 7 DSGVO. Artikel 28 Absatz 7 DSGVO. Siehe Gemeinsame Stellungnahme 1/2021 des EDSA und des EDSB zu Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_de.

[46] Artikel 28 Absatz 8 DSGVO. Das Register für Entscheidungen von Aufsichtsbehörden und Gerichten zu Fragen, die im Rahmen des Kohärenzverfahrens behandelt werden, einschließlich Standardvertragsklauseln für die Zwecke der Einhaltung von Artikel 28 DSGVO, ist hier abrufbar: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en.

[47] Artikel 28 Absatz 6 DSGVO.

widersprechen[48] und sie nicht den durch die DGSVO und die Datenschutzgesetze der EU oder der Mitgliedstaaten gewährten Schutz unterlaufen.

108. Verträge zwischen Verantwortlichen und Auftragsverarbeitern können bisweilen einseitig von einer der Parteien abgefasst werden. Welche Partei bzw. welche Parteien den Vertrag abfasst/abfassen, kann von mehreren Faktoren abhängen, darunter die Stellung der Parteien auf dem Markt und ihre Vertragsmacht, ihr technisches Fachwissen sowie ihr Zugang zu Rechtsberatung. So neigen einige Diensteanbieter tendenziell dazu, Standardbedingungen festzulegen, zu denen auch Datenverarbeitungsvereinbarungen gehören.

109. Eine Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter muss den Anforderungen von Artikel 28 DSGVO genügen, damit sichergestellt ist, dass der Auftragsverarbeiter personenbezogene Daten im Einklang mit der DSGVO verarbeitet. Eine solche Vereinbarung sollte den konkreten Verantwortlichkeiten von Verantwortlichen und Auftragsverarbeitern Rechnung tragen. Artikel 28 enthält zwar eine Liste von Punkten, die in jedem Vertrag behandelt werden müssen, der das Verhältnis zwischen Verantwortlichen und Auftragsverarbeitern regelt, doch lässt er den Parteien solcher Verträge Raum für Verhandlungen. Mitunter kommt es vor, dass sich ein Verantwortlicher oder ein Auftragsverarbeiter bei der Anpassung der Datenschutzvereinbarung in einer schwächeren Verhandlungsposition befindet. Der Rückgriff auf die Standardvertragsklauseln, die gemäß Artikel 28 (Absätze 7 und 8) angenommen wurden, kann dazu beitragen, die Verhandlungspositionen wieder ins Gleichgewicht zu bringen und sicherzustellen, dass die Verträge im Einklang mit der DSGVO stehen.

110. Die Tatsache, dass der Vertrag und seine detaillierten Geschäftsbedingungen vom Diensteanbieter und nicht vom Verantwortlichen ausgearbeitet werden, ist für sich genommen nicht problematisch und stellt allein keine ausreichende Grundlage für die Schlussfolgerung dar, dass der Diensteanbieter als Verantwortlicher angesehen werden sollte. Außerdem sollte das Ungleichgewicht bei der Vertragsmacht eines kleinen Verantwortlichen gegenüber großen Diensteanbietern weder als Rechtfertigung dafür betrachtet werden, dass der Verantwortliche Klauseln und Vertragsbedingungen akzeptiert, die nicht mit dem Datenschutzrecht vereinbar sind, noch kann es den Verantwortlichen von seinen Datenschutzpflichten entbinden. Der Verantwortliche muss die Bedingungen prüfen, und soweit er sie freiwillig akzeptiert und die Dienstleistung in Anspruch nimmt, hat er auch die volle Verantwortung für die Einhaltung der DSGVO übernommen. Jede von einem Auftragsverarbeiter vorgeschlagene Änderung von Datenverarbeitungs-Vereinbarungen, die in allgemeinen Vertragsbedingungen enthalten sind, sollte dem Verantwortlichen direkt mitgeteilt und von ihm genehmigt werden, wobei zu berücksichtigen ist, über welchen Spielraum der Auftragsverarbeiter in Bezug auf nicht wesentliche Elemente der Mittel verfügt (siehe weiter oben die Ziffern 40-41). Die

[48] Der EDSA erinnert daran, dass das gleiche Maß an Flexibilität zulässig ist, wenn sich die Parteien dafür entscheiden, Standardvertragsklauseln als geeignete Schutzklauseln für Übermittlungen an Drittländer gemäß Artikel 46 Absatz 2 Buchstabe c oder Artikel 46 Absatz 2 Buchstabe d DSGVO zu verwenden. In Erwägungsgrund 109 DSGVO heißt es: *„Die dem Verantwortlichen oder dem Auftragsverarbeiter offenstehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde festgelegten Standard-Datenschutzklauseln zurückzugreifen, sollte den Verantwortlichen oder den Auftragsverarbeiter weder daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen, wie zum Beispiel Verträgen zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, zu verwenden, noch ihn daran hindern, ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standarddatenschutzklauseln stehen oder die Grundrechte und Grundfreiheiten der betroffenen Personen beschneiden. Die Verantwortlichen und die Auftragsverarbeiter sollten ermutigt werden, mit vertraglichen Verpflichtungen, die die Standard-Schutzklauseln ergänzen, zusätzliche Garantien zu bieten*“.

bloße Veröffentlichung dieser Änderungen auf der Website des Auftragsverarbeiters steht nicht im Einklang mit Artikel 28.

1.3 Inhalt des Vertrags oder des sonstigen Rechtsinstruments

111. Bevor wir näher auf die einzelnen Anforderungen der DSGVO in Bezug auf den Inhalt des Vertrags oder eines anderen Rechtsinstruments eingehen, sind einige allgemeine Anmerkungen angebracht.

112. Zwar sollten die in Artikel 28 der Verordnung festgelegten Elemente den wesentlichen Inhalt des Vertrags ausmachen, doch sollte er dem Verantwortlichen und dem Auftragsverarbeiter die Möglichkeit bieten, genauer zu erläutern, wie diese Kernelemente mit detaillierten Weisungen umgesetzt werden sollen. Daher **sollten in der Auftragsverarbeitungsvereinbarung nicht lediglich die Bestimmungen der DSGVO wiederholt werden**: vielmehr sollte sie spezifischere, konkrete Angaben dazu enthalten, wie die Vorgaben eingehalten werden und welches Sicherheitsniveau für die Verarbeitung personenbezogener Daten, die Gegenstand der Verarbeitungsvereinbarung ist, erforderlich ist. Das Aushandeln und Festlegen des Vertrags ist keineswegs eine Pro-forma-Übung, sondern eine Gelegenheit, Einzelheiten der Verarbeitung festzulegen.[49] „Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es [...] einer klaren Zuteilung der Verantwortlichkeiten“ durch die DSGVO.[50]

113. Gleichzeitig sollte der Vertrag ***„die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person“*** **berücksichtigen**.[51] Generell sollte der Vertrag zwischen den Parteien unter Berücksichtigung der konkreten Datenverarbeitung abgefasst werden. So ist es beispielsweise nicht erforderlich, einem Auftragsverarbeiter, der mit einer Verarbeitungstätigkeit betraut ist, von der nur geringe Risiken ausgehen, besonders strenge Schutzmaßnahmen und Verfahren aufzuerlegen: Zwar muss jeder Auftragsverarbeiter die Anforderungen der Verordnung erfüllen, doch sollten die Maßnahmen und Verfahren auf die jeweilige Situation zugeschnitten sein. In jedem Fall müssen alle in Artikel 28 Absatz 3 genannten Elemente durch den Vertrag abgedeckt werden. Gleichzeitig sollte der Vertrag Elemente enthalten, die dem Auftragsverarbeiter helfen können, die Risiken für die Rechte und Freiheiten der betroffenen Personen zu verstehen, die sich aus der Verarbeitung ergeben: Weil die Verarbeitung im Auftrag des Verantwortlichen erfolgt, kennt der Verantwortliche häufig die durch diese Verarbeitung entstehenden Risiken besser, weil er die Umstände kennt, unter denen die Verarbeitung stattfindet.

114. Wir kommen nunmehr zum **erforderlichen Inhalt** des Vertrags oder des sonstigen Rechtsinstruments, und hier legt der EDSA Artikel 28 Absatz 3 so aus, dass er Folgendes enthalten muss:

- den **Gegenstand** der Verarbeitung (z. B. Videoüberwachungsaufnahmen von Personen, die eine Hochsicherheitseinrichtung betreten und verlassen). Obwohl der Gegenstand der Verarbeitung ein weit gefasster Begriff ist, muss er hinreichend präzise formuliert werden, damit klar ist, was der Hauptgegenstand der Verarbeitung ist;

[49] Vgl. ferner EDSA, Stellungnahme 14/2019 zu dem von der dänischen Aufsichtsbehörde vorgelegten Entwurf für Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO), S. 5.
[50] Erwägungsgrund 79 DSGVO.
[51] Erwägungsgrund 81 DSGVO.

- die **Dauer**[52] der Verarbeitung: Es sollten hier der genaue Zeitraum oder die Kriterien für seine Festlegung angegeben werden; es könnte beispielsweise die Laufzeit der Auftragsverarbeitungsvereinbarung angeführt werden;

- die **Art** der Verarbeitung; die Art der im Rahmen der Verarbeitung durchgeführten Vorgänge (z. B.: „Filmaufnahmen", „Aufzeichnung", „Archivierung von Bildern"...) **und der Zweck** der Verarbeitung (z. B.: Erfassen unberechtigter Zutritte). Diese Beschreibung sollte je nach der konkreten Verarbeitungstätigkeit so umfassend wie möglich sein, damit externe Parteien (z. B. Aufsichtsbehörden) den Inhalt und die Risiken der dem Auftragsverarbeiter anvertrauten Verarbeitung verstehen können;

- die **Art der personenbezogenen Daten**: sie sollte so detailliert wie möglich angegeben werden (beispielsweise: Videobilder von Personen beim Betreten und Verlassen der Einrichtung). Die bloße Angabe, dass es sich um „personenbezogene Daten gemäß Artikel 4 Nr. 1 DSGVO" oder um „besondere Kategorien personenbezogener Daten gemäß Artikel 9" handelt, wäre nicht ausreichend. Bei besonderen Kategorien personenbezogener Daten sollte im Vertrag oder im Rechtsinstrument zumindest angegeben werden, um welche Arten von Daten es sich handelt, z. B. „Informationen bezüglich Patientenakten" oder „Informationen darüber, ob die betroffene Person Mitglied in einer Gewerkschaft ist";

- die **Kategorien betroffener Personen**: Auch hier sollte die Angabe recht spezifisch sein (beispielsweise: „Besucher", „Beschäftigte", „Zustelldienste" usw.);

- die **Pflichten und Rechte des Verantwortlichen**: Die Rechte des Verantwortlichen werden in den folgenden Abschnitten näher behandelt (z. B. in Bezug auf das Recht des Verantwortlichen, Inspektionen und Prüfungen durchzuführen). Zu den Pflichten des Verantwortlichen gehören beispielsweise seine Pflicht, dem Auftragsverarbeiter die im Vertrag genannten Daten zur Verfügung zu stellen, Weisungen im Zusammenhang mit der Verarbeitung der Daten durch den Auftragsverarbeiter zu erteilen und zu dokumentieren, um vor und während der gesamten Verarbeitung sicherzustellen, dass der Auftragsverarbeiter seinen in der DSGVO festgelegten Pflichten nachkommt, die Verarbeitung zu überwachen, unter anderem durch Überprüfungen und Inspektionen beim Auftragsverarbeiter.

115. Während die DSGVO Elemente aufführt, die stets in die Vereinbarung aufzunehmen sind, müssen gegebenenfalls je nach Kontext und Risiken der Verarbeitung weitere relevante Informationen sowie etwaige zusätzlich geltende Anforderungen aufgenommen werden.

1.3.1 Der Auftragsverarbeiter darf Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten (Artikel 28 Absatz 3 Buchstabe a DSGVO)

116. Die Notwendigkeit dieser Verpflichtung ergibt sich daraus, dass der Auftragsverarbeiter Daten im Auftrag des Verantwortlichen verarbeitet. Verantwortliche müssen ihren Auftragsverarbeitern Weisungen zu jeder Verarbeitungstätigkeit erteilen. Diese Weisungen können den zulässigen bzw. unzulässigen Umgang mit personenbezogenen Daten, detailliertere Verfahren, Möglichkeiten der Sicherung von Daten usw. umfassen. Der Auftragsverarbeiter darf nicht über die Weisungen des Verantwortlichen hinausgehen. Der Auftragsverarbeiter kann jedoch Elemente vorschlagen, die, wenn sie von dem Verantwortlichen akzeptiert werden, Teil der erteilten Weisungen werden.

[52] Die Dauer der Verarbeitung entspricht nicht unbedingt der Laufzeit der Vereinbarung (es können gesetzliche Verpflichtungen bestehen, die Daten über einen längeren oder kürzeren Zeitraum zu speichern).

117. Verarbeitet ein Auftragsverarbeiter Daten außerhalb oder über die Weisungen des Verantwortlichen hinaus und kommt dies einer Entscheidung über die Zwecke und Mittel der Verarbeitung gleich, verstößt der Auftragsverarbeiter gegen seine Pflichten und gilt gemäß Artikel 28 Absatz 10 in Bezug auf diese Verarbeitung sogar als Verantwortlicher (siehe weiter unten Unterabschnitt 1.5[53]).

118. Die Weisungen des Verantwortlichen sind zu **dokumentieren**. Zu diesem Zweck wird empfohlen, ein Verfahren und eine Vorlage für die Erteilung weiterer Weisungen in einen Anhang des Vertrags oder anderen Rechtsinstruments aufzunehmen. Alternativ können die Weisungen in schriftlicher Form (z. B. per E-Mail) sowie in jeder anderen dokumentierten Form erteilt werden, sofern es möglich ist, Aufzeichnungen über diese Weisungen zu führen. Um Schwierigkeiten beim Nachweis e zu vermeiden, dass die Weisungen des Verantwortlichen ordnungsgemäß dokumentiert wurden, empfiehlt der EDSA in jedem Fall, diese Weisungen zusammen mit dem Vertrag oder anderen Rechtsinstrument aufzubewahren.

119. Die Pflicht des Auftragsverarbeiters, jede Verarbeitungstätigkeit zu unterlassen, die nicht auf den Weisungen des Verantwortlichen beruht, gilt auch für die **Übermittlung** personenbezogener Daten an ein Drittland oder eine internationale Organisation. In dem Vertrag sollten unter Berücksichtigung der Bestimmungen von Kapitel V der DSGVO die Anforderungen an die Übermittlung an Drittländer oder internationale Organisationen festgelegt werden.

120. Der EDSA empfiehlt Verantwortlichen, diesem konkreten Punkt gebührende Aufmerksamkeit zu schenken, insbesondere wenn der Auftragsverarbeiter bestimmte Verarbeitungstätigkeiten an andere Auftragsverarbeiter delegieren wird und wenn der Auftragsverarbeiter über Abteilungen oder Einheiten in Drittländern verfügt. Wenn die Weisungen des Verantwortlichen keine Übermittlung oder Offenlegung an Drittländer zulassen, darf der Auftragsverarbeiter weder einen Unterauftragsverarbeiter in einem Drittland mit der Verarbeitung beauftragen, noch darf er die Daten in einer seiner Abteilungen außerhalb der EU verarbeiten lassen.

121. Ein Auftragsverarbeiter darf Daten auf andere Weise als auf dokumentierte Weisung des Verantwortlichen verarbeiten, **wenn der Auftragsverarbeiter verpflichtet ist, personenbezogene Daten auf der Grundlage des Unionsrechts oder des Rechts des Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, zu verarbeiten und/oder zu übermitteln**. Diese Bestimmung zeigt ferner, wie wichtig es ist, Datenverarbeitungsvereinbarungen sorgfältig auszuhandeln und abzufassen, beispielsweise kann es für jede Partei in Bezug auf das Bestehen einer solchen rechtlichen Verpflichtung erforderlich sein, sich rechtlich beraten zu lassen. Dies muss rechtzeitig geschehen, da der Auftragsverarbeiter verpflichtet ist, den Verantwortlichen vor Beginn der Verarbeitung über eine solche Anforderung zu informieren. Nur wenn es dem Auftragsverarbeiter aufgrund desselben (EU- oder mitgliedstaatlichen) Rechts untersagt ist, den Verantwortlichen aus „wichtigen Gründen des öffentlichen Interesses“ zu informieren, besteht keine solche Informationspflicht. In jedem Fall darf eine Übermittlung oder Offenlegung nur erfolgen, wenn dies nach dem Unionsrecht einschließlich Artikel 48 DSGVO zulässig ist.

1.3.2 Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Artikel 28 Absatz 3 Buchstabe b DSGVO)

[53] Siehe Teil II Unterabschnitt 1.5 („Bestimmung der Zwecke und Mittel der Verarbeitung durch den Auftragsverarbeiter“).

122. Im Vertrag muss festgelegt werden, dass der Auftragsverarbeiter sicherzustellen hat, dass jede Person, die er zur Verarbeitung der personenbezogenen Daten ermächtigt, zur Vertraulichkeit verpflichtet ist. Dies kann entweder durch eine konkrete vertragliche Vereinbarung oder aufgrund bereits bestehender gesetzlicher Verpflichtungen geschehen.

123. Der weit gefasste Begriff „zur Verarbeitung personenbezogener Daten befugte Personen“ umfasst Arbeitnehmer und Zeitarbeitskräfte. Generell sollte der Auftragsverarbeiter die personenbezogenen Daten nur Arbeitnehmern zur Verfügung stellen, die sie tatsächlich benötigen, um Aufgaben wahrzunehmen, mit denen der Auftragsverarbeiter von dem Verantwortlichen betraut wurde.

124. Die Zusage der oder Verpflichtung zur Vertraulichkeit muss „angemessen“ sein, d. h. sie muss der befugten Person effektiv untersagen, vertrauliche Informationen unbefugt offenzulegen, und sie muss so weit gefasst sein, dass sie alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten sowie die Bedingungen, unter denen die personenbezogenen Daten verarbeitet werden, umfasst.

1.3.3 Der Auftragsverarbeiter muss alle nach Artikel 32 erforderlichen Maßnahmen ergreifen (Artikel 28 Absatz 3 Buchstabe c DSGVO).

125. Artikel 32 verpflichtet Verantwortlichen und Auftragsverarbeiter, geeignete technische und organisatorische Sicherheitsmaßnahmen zu treffen. Auch wenn diese Verpflichtung für den Auftragsverarbeiter, dessen Verarbeitungsvorgänge in den Anwendungsbereich der DSGVO fallen, bereits unmittelbar besteht, muss die Pflicht, alle nach Artikel 32 erforderlichen Maßnahmen zu ergreifen, dennoch in den Vertrag über die von dem Verantwortlichen übertragenen Verarbeitungstätigkeiten aufgenommen werden.

126. Wie bereits erwähnt, sollte der Verarbeitungsvertrag die Bestimmungen der DSGVO nicht nur wiederholen. Der Vertrag muss Informationen zu folgenden Punkten enthalten oder auf solche Informationen verweisen: die zu ergreifenden Sicherheitsmaßnahmen, **eine Verpflichtung des Auftragsverarbeiters, die Zustimmung des Verantwortlichen einzuholen, bevor er Änderungen vornimmt**, und eine regelmäßige Überprüfung der Sicherheitsmaßnahmen, um deren Angemessenheit im Hinblick auf Risiken, die sich im Laufe der Zeit entwickeln können, zu gewährleisten. Die Informationen über die in den Vertrag aufzunehmenden Sicherheitsmaßnahmen müssen so detailliert sein, dass der Verantwortliche die Angemessenheit der Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO beurteilen kann. Darüber hinaus ist die Beschreibung auch erforderlich, damit der Verantwortliche seiner Rechenschaftspflicht gemäß Artikel 5 Absatz 2 und Artikel 24 DSGVO in Bezug auf die dem Auftragsverarbeiter auferlegten Sicherheitsmaßnahmen nachkommen kann. Eine entsprechende Verpflichtung des Auftragsverarbeiters, den Verantwortlichen zu unterstützen und alle für den Nachweis der Einhaltung erforderlichen Informationen zur Verfügung zu stellen, kann aus Artikel 28 Absatz 3 Buchstaben f und h DSGVO abgeleitet werden.

127. Der Umfang der Weisungen, die der Verantwortliche dem Auftragsverarbeiter hinsichtlich der durchzuführenden Maßnahmen erteilt, hängt von den konkreten Umständen ab. In einigen Fällen kann der Verantwortliche eine klare und detaillierte Beschreibung der durchzuführenden Sicherheitsmaßnahmen vorlegen. In anderen Fällen kann der Verantwortliche die mindestens zu erreichenden Sicherheitsziele beschreiben und den Auftragsverarbeiter auffordern, die Umsetzung konkreter Sicherheitsmaßnahmen vorzuschlagen. In jedem Fall muss der Verantwortliche dem Auftragsverarbeiter eine Beschreibung der Verarbeitungstätigkeiten und der Sicherheitsziele (auf der Grundlage der RisikoBeurteilung des Verantwortlichen) zur Verfügung stellen und die vom Auftragsverarbeiter vorgeschlagenen Maßnahmen genehmigen. Dies könnte dem Vertrag als Anhang

beigefügt werden. Der Verantwortliche übt seine Entscheidungsbefugnis über die wesentlichen Merkmale der Sicherheitsmaßnahmen aus, sei es durch eine explizite Auflistung der Maßnahmen oder durch Genehmigung der vom Auftragsverarbeiter vorgeschlagenen Maßnahmen.

1.3.4 Der Auftragsverarbeiter muss die in Artikel 28 Absätze 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhalten (Artikel 28 Absatz 3 Buchstabe d DSGVO).

128. In der Vereinbarung muss festgelegt sein, dass der Auftragsverarbeiter ohne vorherige schriftliche Genehmigung des Verantwortlichen keinen anderen Auftragsverarbeiter beauftragen darf, und ob es sich hierbei um eine gesonderte oder allgemeine Genehmigung handeln muss. Im Falle einer allgemeinen Genehmigung muss der Auftragsverarbeiter den Verantwortlichen über jede Änderung bei den Unterauftragsverarbeitern schriftlich informieren und dem Verantwortlichen die Möglichkeit geben, Einspruch zu erheben. Es wird empfohlen, das entsprechende Verfahren im Vertrag festzulegen. Es sei darauf hingewiesen, dass die Pflicht des Auftragsverarbeiters, den Verantwortlichen über jede Änderung bei den Unterauftragsverarbeitern zu informieren, impliziert, dass der Auftragsverarbeiter solche Änderungen gegenüber dem Verantwortlichen aktiv anzeigt oder kennzeichnet.[54] Wenn eine gesonderte Genehmigung erforderlich ist, sollte im Vertrag auch das Verfahren für die Erteilung einer solchen Genehmigung festgelegt werden.

129. Wenn der Auftragsverarbeiter einen weiteren Auftragsverarbeiter einsetzt, muss zwischen ihnen ein Vertrag geschlossen werden, der dieselben Datenschutzverpflichtungen vorsieht, wie sie dem ursprünglichen Auftragsverarbeiter auferlegt werden, oder diese Verpflichtungen müssen durch ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten auferlegt werden (siehe auch den nachstehenden Absatz 160). Dazu gehört auch die Verpflichtung nach Artikel 28 Absatz 3 Buchstabe h, Überprüfungen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen.[55] Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für die Einhaltung der Datenschutzpflichten durch die anderen Auftragsverarbeiter (weitere Einzelheiten zum empfohlenen Inhalt der Vereinbarung siehe weiter unten Abschnitt 1.6[56]).

1.3.5 Der Auftragsverarbeiter unterstützt den Verantwortlichen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person nachzukommen (Artikel 28 Absatz 3 Buchstabe e DSGVO).

130. Zwar obliegt die Bearbeitung der Anträge betroffener Personen dem Verantwortlichen, doch muss im Vertrag festgelegt werden, dass der Auftragsverarbeiter verpflichtet ist, dabei „nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen Unterstützung zu leisten“. Die Art dieser Unterstützung kann „angesichts der Art der Verarbeitung“ und je nach Art der dem Auftragsverarbeiter übertragenen Tätigkeit sehr unterschiedlich sein. Die Einzelheiten der vom Auftragsverarbeiter zu

[54] In diesem Zusammenhang reicht es hingegen z. B. nicht aus, dass der Auftragsverarbeiter dem Verantwortlichen lediglich allgemeinen Zugang zu einer Liste der Unterauftragsverarbeiter gewährt, die möglicherweise von Zeit zu Zeit aktualisiert wird, ohne auf jeden neuen vorgesehenen Unterauftragsverarbeiter hinzuweisen. Mit anderen Worten: Der Auftragsverarbeiter muss den Verantwortlichen aktiv über jede Änderung in der Liste informieren (d. h. insbesondere über jeden neuen geplanten Unterauftragsverarbeiter).
[55] Vgl. Stellungnahme des EDSA 14/2019 zu dem von der dänischen Aufsichtsbehörde vorgelegten Entwurf für Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO), 9. Juli 2019.
[56] Siehe Teil II Unterabschnitt 1.6 („Unterauftragsverarbeiter“).

leistenden Unterstützung sollten im Vertrag oder in einem Anhang zu diesem Vertrag aufgeführt werden.

131. Während die Unterstützung lediglich darin bestehen kann, alle eingegangenen Anfragen umgehend weiterzuleiten und/oder dem Verantwortlichen die Möglichkeit zu geben, die einschlägigen personenbezogenen Daten direkt zu extrahieren und zu verwalten, werden dem Auftragsverarbeiter unter bestimmten Umständen spezifischere technische Aufgaben übertragen, insbesondere wenn er in der Lage ist, die personenbezogenen Daten zu extrahieren und zu verwalten.

132. Es darf nicht vergessen werden, dass die praktische Bearbeitung einzelner Anfragen zwar an den Auftragsverarbeiter ausgelagert werden kann, der Verantwortliche jedoch die Verantwortung für die Beantwortung solcher Anträge trägt. Daher sollte die Beurteilung der Frage, ob Anträge betroffener Personen zulässig sind und/oder die in der DSGVO festgelegten Anforderungen erfüllt sind, vom Verantwortlichen vorgenommen werden, und zwar entweder von Fall zu Fall oder mittels klarer Weisungen, die dem Auftragsverarbeiter im Vertrag vor Beginn der Verarbeitung erteilt werden. Außerdem kann der Verantwortliche die in Kapitel III festgelegten Fristen nicht aufgrund der Tatsache verlängern, dass die erforderlichen Informationen vom Auftragsverarbeiter bereitgestellt werden müssen.

1.3.6 Der Auftragsverarbeiter muss den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützen (Artikel 28 Absatz 3 Buchstabe f DSGVO).

133. Der Vertrag darf sich nicht darauf beschränken, diese Unterstützungspflichten nur zu wiederholen: **In der Vereinbarung sollte detailliert dargestellt werden, wie der Auftragsverarbeiter aufgefordert wird, dem Verantwortlichen bei der Erfüllung der aufgelisteten Pflichten zu helfen**. So können beispielsweise Verfahren und Musterformulare in die Anhänge der Vereinbarung aufgenommen werden, damit der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen kann.

134. Art und Umfang der vom Auftragsverarbeiter zu leistenden Unterstützung können „*unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen*“ sehr unterschiedlich sein. Der Verantwortliche muss den Auftragsverarbeiter angemessen über das mit der Verarbeitung verbundene Risiko und über alle sonstigen Umstände informieren, die dem Auftragsverarbeiter bei der Erfüllung seiner Pflichten helfen könnten.

135. Bei den besonderen Pflichten hat der Auftragsverarbeiter zunächst die Pflicht, den Verantwortlichen bei der Erfüllung seiner Pflicht zu unterstützen, angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu ergreifen.[57] Zwar kann sich dies bis zu einem gewissen Grad mit der Anforderung überschneiden, dass der Auftragsverarbeiter selbst angemessene Sicherheitsmaßnahmen ergreift, wenn die Verarbeitungsvorgänge des Auftragsverarbeiters in den Anwendungsbereich der DSGVO fallen, doch handelt es sich um zwei unterschiedliche Pflichten, da sich die eine auf die eigenen Maßnahmen des Auftragsverarbeiters und die andere auf den Verantwortlichen bezieht.

136. Zweitens muss der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung seiner Pflicht unterstützen, der Aufsichtsbehörde und den betroffenen Personen Verletzungen des Schutzes personenbezogener Daten zu melden. Der Auftragsverarbeiter muss den Verantwortlichen benachrichtigen, wenn er eine Verletzung des Schutzes personenbezogener Daten feststellt, die die

[57] Artikel 32 DSGVO.

Einrichtungen/IT-Systeme des Auftragsverarbeiters oder eines Unterauftragsverarbeiters betrifft, und dem Verantwortlichen behilflich sein, die Informationen zu erhalten, die in der Meldung an die Aufsichtsbehörde anzugeben sind.[58] Nach der DSGVO muss der Verantwortliche einen Verstoß unverzüglich melden, um den Schaden für den Einzelnen so gering wie möglich zu halten und die Möglichkeit zu maximieren, die Verletzung in angemessener Weise zu beheben. Daher sollte die Benachrichtigung des Auftragsverarbeiters an den Verantwortlichen unverzüglich erfolgen.[59] Je nach den Besonderheiten der dem Auftragsverarbeiter anvertrauten Verarbeitung kann es angebracht sein, dass die Parteien in den Vertrag einen bestimmten Zeitrahmen (z. B. eine bestimmte Anzahl von Stunden) aufnehmen, innerhalb dessen der Auftragsverarbeiter den Verantwortlichen benachrichtigen sollte, sowie die Kontaktstelle für solche Meldungen, die Modalitäten und die vom Verantwortlichen erwarteten Mindestinformationen.[60] Die vertragliche Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter kann auch eine Ermächtigung und eine Verpflichtung für den Auftragsverarbeiter beinhalten, eine Verletzung des Schutzes personenbezogener Daten im Einklang mit den Artikeln 33 und 34 direkt zu melden, doch bleibt die rechtliche Verantwortung für die Meldung nach wie vor beim Verantwortlichen.[61] Meldet der Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten direkt der Aufsichtsbehörde und unterrichtet er die betroffenen Personen gemäß Artikel 33 und 34, so muss der Auftragsverarbeiter auch den Verantwortlichen unterrichten und ihm Kopien der Meldung und der Information der betroffenen Personen zur Verfügung stellen.

137. Darüber hinaus muss der Auftragsverarbeiter den Verantwortlichen bei Bedarf bei der Durchführung von Datenschutz-Folgenabschätzungen und bei der Konsultation der Aufsichtsbehörde unterstützen, wenn sich aus dem Ergebnis ergibt, dass ein hohes Risiko besteht, das nicht gemindert werden kann.

138. Die Pflicht zur Unterstützung besteht nicht in einer Verlagerung der Verantwortung, da diese Pflichten dem Verantwortlichen auferlegt werden. Obwohl beispielsweise die Datenschutz-Folgenabschätzung in der Praxis von einem Auftragsverarbeiter durchgeführt werden kann, bleibt der Verantwortliche für seine Pflicht zur Durchführung der Abschätzung verantwortlich[62], und der Auftragsverarbeiter ist nur verpflichtet, den Verantwortlichen „erforderlichenfalls und auf Anfrage“ zu unterstützen.[63] Folglich muss der Verantwortliche die Initiative zur Durchführung einer Datenschutz-Folgenabschätzung ergreifen, nicht der Auftragsverarbeiter.

1.3.7 Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen löschen oder zurückgeben (Artikel 28 Absatz 3 Buchstabe g DSGVO).

139. Die Vertragsbedingungen sollen gewährleisten, dass die personenbezogenen Daten nach Abschluss der „Erbringung der Verarbeitungsleistungen“ angemessen geschützt werden: Es ist daher Sache des

[58] Artikel 33 Absatz 3 DSGVO.
[59] Weitere Informationen finden Sie in den Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP250rev.01, 6. Februar 2018, S. 16-17.
[60] Vgl. ferner die Stellungnahme des EDSA 14/2019 zu dem von der dänischen Aufsichtsbehörde vorgelegten Entwurf für Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO), 9. Juli 2019, Ziffer 40.
[61] Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP250rev.01, 6. Februar 2018, S. 16.
[62] Artikel 29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev. 01, 4. Oktober 2017, S. 14.
[63] Erwägungsgrund 95 DSGVO.

Verantwortlichen, zu entscheiden, wie der Auftragsverarbeiter im Hinblick auf die personenbezogenen Daten verfahren soll.

140. Der Verantwortliche kann zu Beginn entscheiden, ob personenbezogene Daten gelöscht oder zurückgegeben werden müssen, indem er dies im Vertrag festlegt und dem Auftragsverarbeiter zeitnah schriftlich mitteilt. Der Vertrag oder das andere Rechtsinstrument sollte für den Verantwortlichen die Möglichkeit vorsehen, seine getroffene Entscheidung vor Abschluss der Erbringung der Verarbeitungsleistungen zu ändern. Im Vertrag sollte das Verfahren für die Erteilung solcher Weisungen festgelegt werden.

141. Entscheidet sich der Verantwortliche für die Löschung der personenbezogenen Daten, sollte der Auftragsverarbeiter sicherstellen, dass die Löschung auf sichere Weise erfolgt, auch um Artikel 32 DSGVO zu genügen. Der Auftragsverarbeiter sollte dem Verantwortlichen bestätigen, dass die Löschung innerhalb der vereinbarten Frist und in der vereinbarten Weise abgeschlossen wurde.

142. Der Auftragsverarbeiter muss alle vorhandenen Kopien der Daten löschen, es sei denn, das EU-Recht oder das Recht der Mitgliedstaaten verlangt eine längere Speicherung. Ist dem Auftragsverarbeiter oder dem Verantwortlichen eine solche rechtliche Verpflichtung bekannt, sollte er die andere Partei so bald wie möglich davon in Kenntnis setzen.

1.3.8 Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 niedergelegten Pflichten zur Verfügung und ermöglicht und trägt zu Überprüfungen – einschließlich Inspektionen – bei, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden (Artikel 28 Absatz 3 Buchstabe h DSGVO).

143. Der Vertrag muss Einzelheiten darüber enthalten, wie oft und auf welche Weise der Informationsfluss zwischen dem Auftragsverarbeiter und dem Verantwortlichen stattfinden sollte, damit der Verantwortliche umfassend über die Einzelheiten der Verarbeitung informiert ist, die für den Nachweis der Einhaltung der in Artikel 28 DSGVO festgelegten Pflichten relevant sind. So können beispielsweise die maßgeblichen Teile des Verzeichnisses von Verarbeitungstätigkeiten des Auftragsverarbeiters an den Verantwortlichen weitergegeben werden. Der Auftragsverarbeiter sollte alle Informationen darüber bereitstellen, wie die Verarbeitungstätigkeit im Auftrag des Verantwortlichen durchgeführt wird. Diese Informationen sollten folgende Angaben umfassen: Funktionsweise der verwendeten Systeme, Sicherheitsmaßnahmen, Gewährleistung der Speicher-/ Aufbewahrungspflichten, Speicherort der Daten, Datenübermittlungen, Personen, die Zugriff auf die Daten haben, Empfänger der Daten, eingesetzte Unterauftragsverarbeiter usw.

144. Ferner sollten im Vertrag nähere Einzelheiten zur Durchführung von Inspektionen und Überprüfungen durch den Verantwortlichen oder einen vom Verantwortlichen beauftragten Prüfer sowie in Bezug auf die Pflicht zur Mitwirkung an Inspektionen und Überprüfungen festgelegt werden.

In der DSGVO ist festgelegt, dass Inspektionen und Überprüfungen von dem Verantwortlichen oder einem vom Verantwortlichen beauftragten Dritten durchgeführt werden. Mit solchen Überprüfungen soll sichergestellt werden, dass der Verantwortliche über alle Informationen über die in seinem Auftrag durchgeführte Verarbeitungstätigkeit und die vom Auftragsverarbeiter gebotenen Garantien verfügt. Der Auftragsverarbeiter kann zwar einen bestimmten Prüfer vorschlagen, die endgültige Entscheidung muss jedoch gemäß Artikel 28 Absatz 3 Buchstabe h DSGVO dem Verantwortlichen überlassen

bleiben.[64] Darüber hinaus behält der Verantwortliche auch dann, wenn die Inspektion von einem vom Auftragsverarbeiter vorgeschlagenen Prüfer durchgeführt wird, das Recht, den Umfang, die Methodik und die Ergebnisse der Inspektion anzufechten.[65]

Die Parteien sollten nach Treu und Glauben zusammenarbeiten und prüfen, ob und wann in den Räumlichkeiten des Auftragsverarbeiters Überprüfungen durchzuführen sind und welche Art von Überprüfung oder Inspektion (Fern-/Vor-Ort-Kontrolle/sonstige Art der Einholung der erforderlichen Informationen) im konkreten Fall erforderlich und angemessen wäre, wobei auch Sicherheitsbedenken zu berücksichtigen sind; das Letztentscheidungsrecht liegt beim Verantwortlichen. Je nach den Ergebnissen der Inspektion sollte der Verantwortliche den Auftragsverarbeiter auffordern können, weitere Maßnahmen zu ergreifen, z. B. um festgestellte Mängel zu beheben und Lücken zu schließen.[66] Desgleichen sollten besondere Verfahren für die Inspektion von Unterauftragsverarbeitern durch den Auftragsverarbeiter und den Verantwortlichen festgelegt werden (siehe weiter unten Abschnitt 1.6[67]).

145. Die Frage der Kostenverteilung zwischen einem Verantwortlichen und einem Auftragsverarbeiter im Zusammenhang mit Überprüfungen fällt nicht unter die DSGVO und unterliegt wirtschaftlichen Erwägungen. Artikel 28 Absatz 3 Buchstabe h sieht jedoch vor, dass der Vertrag den Auftragsverarbeiter verpflichtet, dem Verantwortlichen alle erforderlichen Informationen zur Verfügung zu stellen, und dass er verpflichtet ist, Überprüfungen einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen vom Verantwortlichen beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen. In der Praxis bedeutet dies, dass die Vertragsparteien keine Klauseln vereinbaren sollten, die die Zahlung eindeutig unangemessener oder unverhältnismäßig hoher Kosten und Gebühren zum Gegenstand habenund dadurch eine abschreckende Wirkung auf eine der Parteien ausüben würden. Solche Klauseln würden in der Tat bedeuten, dass die in Artikel 28 Absatz 3 Buchstabe h festgelegten Rechte und Pflichten in der Praxis nie ausgeübt würden und rein theoretisch wären, obwohl sie integraler Bestandteil der Datenschutzgarantien nach Artikel 28 DSGVO sind.

1.4 Weisungen, die gegen das Datenschutzrecht verstoßen

146. Gemäß Artikel 28 Absatz 3 informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

147. Der Auftragsverarbeiter ist zwar verpflichtet, die Weisungen des Verantwortlichen zu befolgen, er hat aber auch eine allgemeine Verpflichtung zur Einhaltung der Gesetze. Eine Weisung, die gegen das Datenschutzrecht verstößt, führt scheinbar zu einem Konflikt zwischen den beiden genannten Verpflichtungen.

148. Sobald der Verantwortliche darüber informiert ist, dass eine seiner Weisungen möglicherweise gegen das Datenschutzrecht verstößt, muss er die Situation prüfen und feststellen, ob die Weisung tatsächlich gegen das Datenschutzrecht verstößt.

[64] Vgl. Gemeinsame Stellungnahme 1/2021 des EDSA und des EDSB zu Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern, Ziffer 43.
[65] Vgl. Stellungnahme 14/2019 zu dem von der dänischen Aufsichtsbehörde vorgelegten Entwurf für Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO), Ziffer 43.
[66] Vgl. Stellungnahme 14/2019 zu dem von der dänischen Aufsichtsbehörde vorgelegten Entwurf für Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO), Ziffer 43.
[67] Siehe Teil II Unterabschnitt 1.6 („Unterauftragsverarbeiter“).

149. Der EDSA empfiehlt den Parteien, im Vertrag die Folgen einer vom Auftragsverarbeiter übermittelten Mitteilung einer rechtswidrigen Weisung und gegebenenfalls der Untätigkeit des Verantwortlichen in diesem Zusammenhang auszuhandeln und zu regeln. Ein Beispiel wäre die Aufnahme einer Klausel über die Beendigung des Vertragsverhältnisses für den Fall, dass der Verantwortliche an einer rechtswidrigen Weisung festhält. Ein weiteres Beispiel wäre eine Klausel, die dem Auftragsverarbeiter die Möglichkeit eröffnet, die Durchführung der betreffenden Weisung auszusetzen, bis der Verantwortliche seine Weisung bestätigt, ändert oder zurückzieht.[68]

1.5 Auftragsverarbeiter, der die Verarbeitungszwecke und -mittel bestimmt

150. Verstößt der Auftragsverarbeiter gegen die Verordnung, indem er die Zwecke und Mittel der Verarbeitung bestimmt, gilt er in Bezug auf diese Verarbeitung als Verantwortlicher (Artikel 28 Absatz 10 DSGVO).

1.6 Unterauftragsverarbeiter

151. Datenverarbeitungstätigkeiten werden häufig von einer großen Zahl von Akteuren durchgeführt, und die Ketten der Unterauftragsvergabe werden immer komplexer. Mit der DSGVO werden besondere Pflichten eingeführt, die ausgelöst werden, wenn ein (Unter-)Auftragsverarbeiter beabsichtigt, einen weiteren Akteur in Anspruch zu nehmen, womit ein weiteres Glied in die Kette eingefügt wird, indem ihm Tätigkeiten übertragen werden, die die Verarbeitung personenbezogener Daten erfordern. Die Prüfung der Frage, ob der Diensteanbieter als Unterauftragsverarbeiter handelt, sollte im Einklang mit den obigen Ausführungen zum Begriff des Auftragsverarbeiters durchgeführt werden (siehe oben, Absatz 83).

152. Obwohl die Kette recht lang sein mag, behält der Verantwortliche seine zentrale Rolle bei der Bestimmung des Zwecks und der Mittel der Verarbeitung. Gemäß Artikel 28 Absatz 2 DSGVO darf der Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen (auch in elektronischer Form) keinen weiteren Auftragsverarbeiter in Anspruch nehmen. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen stets über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. In beiden Fällen muss der Auftragsverarbeiter die schriftliche Genehmigung des Verantwortlichen einholen, bevor der Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten betraut wird. Zum Zweck der Prüfung und Entscheidung über die Genehmigung einer Unterauftragsvergabe muss der Auftragsverarbeiter dem Verantwortlichen eine Liste potenzieller Unterauftragsverarbeiter (jeweils mit Angabe des Standorts, ihrer künftigen Aufgabe und einem Nachweis für die von ihnen durchgeführten Sicherheitsmaßnahmen) vorlegen.[69]

153. Die vorherige schriftliche Genehmigung kann gesondert sein, d. h. sich auf einen konkreten Unterauftragsverarbeiter für eine bestimmte Verarbeitungstätigkeit zu einem bestimmten Zeitpunkt beziehen, oder allgemein gehalten sein. Dies sollte im Vertrag oder einem anderen Rechtsinstrument zur Regelung der Verarbeitung festgelegt werden.

154. Beschließt der Verantwortliche zum Zeitpunkt der Vertragsunterzeichnung bestimmte Unterauftragsverarbeiter zu akzeptieren, so sollte eine Liste der zugelassenen

[68] Vgl. Gemeinsame Stellungnahme 1/2021 des EDSA und des EDSB zu Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern, Ziffer 39.

[69] Diese Informationen sind erforderlich, damit der Verantwortliche dem Grundsatz der Rechenschaftspflicht gemäß Artikel 24 und den Bestimmungen von Artikel 28 Absatz 1, Artikel 32 und Kapitel V DSGVO genügen kann.

Unterauftragsverarbeiter in den Vertrag oder einen Anhang zum Vertrag aufgenommen werden. Die Liste sollte dann entsprechend der allgemeinen oder gesonderten Genehmigung des Verantwortlichen auf dem neuesten Stand gehalten werden.

155. Entscheidet sich der Verantwortliche für die Erteilung einer **gesonderten Genehmigung**, sollte er schriftlich angeben, auf welchen Unterauftragsverarbeiter und auf welche Verarbeitungstätigkeit er sich bezieht. Spätere Änderungen bedürfen vor ihrer Umsetzung einer weiteren Genehmigung durch den Verantwortlichen. Wird der Antrag des Auftragsverarbeiters auf Erteilung einer gesonderten Genehmigung nicht innerhalb der gesetzten Frist beantwortet, sollte er als abgelehnt betrachtet werden. Der Verantwortliche sollte seine Entscheidung über die Erteilung oder Verweigerung der Genehmigung unter Berücksichtigung seiner Verpflichtung treffen, nur Auftragsverarbeiter heranzuziehen, die „hinreichende Garantien" bieten (siehe weiter oben Unterabschnitt 1.1[70]).

156. Alternativ kann der Verantwortliche seine **allgemeine Genehmigung** zur Inanspruchnahme von Unterauftragsverarbeitern erteilen (im Vertrag, einschließlich einer Liste mit diesen Unterauftragsverarbeitern in einem Anhang), die um Kriterien als Richtschnur für die Entscheidung des Auftragsverarbeiters ergänzt werden sollte (z. B. Garantien in Bezug auf technische und organisatorische Maßnahmen, Fachwissen, Zuverlässigkeit und Ressourcen).[71] In diesem Fall muss der Auftragsverarbeiter den Verantwortlichen rechtzeitig über jede beabsichtigte Hinzufügung oder Ersetzung von Unterauftragsverarbeitern informieren, damit der Verantwortliche die Möglichkeit erhält, Einspruch zu erheben.

157. Daher liegt der Hauptunterschied zwischen der gesonderten Genehmigung und der allgemeinen Genehmigung in der Bedeutung des Schweigens des Verantwortlichen: Bei der allgemeinen Genehmigung kann sein unterlassener Einspruch innerhalb einer bestimmten Frist als Genehmigung gedeutet werden.

158. In beiden Szenarien sollte der Vertrag Einzelheiten zum Zeitrahmen für die Zustimmung oder Ablehnung durch den Verantwortlichen und zu der Art und Weise enthalten, wie die Parteien zu diesem Thema kommunizieren wollen (z. B. Muster). Ein solcher Zeitrahmen muss im Hinblick auf die Art der Verarbeitung, die Komplexität der dem Auftragsverarbeiter (und den Unterauftragsverarbeitern) übertragenen Tätigkeiten und die Beziehungen zwischen den Parteien angemessen sein. Darüber hinaus sollte der Vertrag Einzelheiten zu den praktischen Schritten enthalten, die auf den Einspruch des Verantwortlichen folgen (z. B. durch Angabe des Zeitrahmens, innerhalb dessen der Verantwortliche und der Auftragsverarbeiter entscheiden sollten, ob die Verarbeitung beendet werden soll).

159. Unabhängig von den vom Verantwortlichen vorgeschlagenen Kriterien für die Auswahl der Dienstleister bleibt der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Erfüllung der Verpflichtungen der Unterauftragsverarbeiter uneingeschränkt haftbar (Artikel 28 Absatz 4 DSGVO). Daher sollte der Auftragsverarbeiter sicherstellen, dass er Unterauftragsverarbeiter vorschlägt, die hinreichende Garantien bieten.

160. Darüber hinaus muss ein Auftragsverarbeiter, der beabsichtigt, einen (genehmigten) Unterauftragsverarbeiter zu beschäftigen, mit diesem einen Vertrag schließen, der diesem dieselben Verpflichtungen auferlegt, wie sie der Verantwortliche dem ersten Auftragsverarbeiter auferlegt, oder die Verpflichtungen müssen nach dem Unionsrecht oder dem Recht der Mitgliedstaaten durch ein

[70] Siehe Teil II – Unterabschnitt 1.1 („Auswahl des Auftragsverarbeiters").

[71] Diese Pflicht des Verantwortlichen ergibt sich aus dem Grundsatz der Rechenschaftspflicht in Artikel 24 und aus der Verpflichtung, den Bestimmungen von Artikel 28 Absatz 1, Artikel 32 und Kapitel V DSGVO zu genügen.

anderes Rechtsinstrument auferlegt werden. Die gesamte Verarbeitungskette muss durch schriftliche Vereinbarungen geregelt werden. Die Auferlegung „derselben“ Verpflichtungen sollte vielmehr funktional als formal ausgelegt werden: Es ist nicht erforderlich, dass der Vertrag denselben Wortlaut hat wie der Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter, aber er sollte sicherstellen, dass die Verpflichtungen materiell identisch sind. Dies bedeutet auch, dass für den Fall, dass der Auftragsverarbeiter dem Unterauftragsverarbeiter einen bestimmten Teil der Verarbeitung überträgt, für den einige der Verpflichtungen nicht gelten können, diese Verpflichtungen nicht „standardmäßig“ in den Vertrag mit dem Unterauftragsverarbeiter aufgenommen werden sollten, da dies nur zu Unsicherheit führen würde. So könnte beispielsweise als Unterstützung bei Verpflichtungen im Zusammenhang mit Verletzungen des Schutzes personenbezogener Daten die Meldung einer Verletzung des Schutzes personenbezogener Daten durch einen Unterauftragsverarbeiter direkt an den Verantwortlichen erfolgen, wenn alle drei zustimmen. Im Falle einer solchen direkten Meldung sollte der Auftragsverarbeiter jedoch informiert werden und eine Kopie der Meldung erhalten.

2 FOLGEN GEMEINSAMER VERANTWORTLICHKEIT

2.1 Transparente Festlegung der jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen für die Erfüllung der Verpflichtungen aus der DSGVO

161. Artikel 26 Absatz 1 DSGVO sieht vor, dass gemeinsam Verantwortliche in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtungen gemäß der Verordnung erfüllt.

162. Gemeinsam Verantwortliche müssen also festlegen, „wer was tut“, indem sie untereinander entscheiden, wer welche Aufgaben auszuführen hat, um sicherzustellen, dass die Verarbeitung den geltenden Verpflichtungen aus der DSGVO in Bezug auf die betreffende gemeinsame Verarbeitung entspricht. Mit anderen Worten: Es ist eine Aufteilung der Verantwortlichkeiten für die Einhaltung der Vorschriften vorzunehmen, wie sich aus der Verwendung des Begriffs *jeweilige* in Artikel 26 Absatz 1 ergibt. Dies schließt nicht aus, dass das Unionsrecht oder das Recht der Mitgliedstaaten bereits bestimmte Zuständigkeiten für jeden der gemeinsam Verantwortlichen festlegen kann. Ist dies der Fall, sollte die Vereinbarung der gemeinsam Verantwortlichen auch alle zusätzlichen Zuständigkeiten regeln, die für die Einhaltung der DSGVO erforderlich sind und in den Rechtsvorschriften nicht geregelt sind.[72]

163. Mit diesen Vorschriften soll sichergestellt werden, dass in Fällen, an denen mehrere Akteure beteiligt sind, insbesondere in komplexen Datenverarbeitungsumgebungen, die Verantwortung für die Einhaltung der Datenschutzvorschriften eindeutig zugewiesen wird, um zu vermeiden, dass der Schutz personenbezogener Daten eingeschränkt wird oder dass ein negativer Kompetenzkonflikt zu Schlupflöchern führt, wodurch bestimmte Verpflichtungen von keiner der an der Verarbeitung beteiligten Parteien eingehalten werden. An dieser Stelle sollte klargestellt werden, dass alle Zuständigkeiten entsprechend den tatsächlichen Gegebenheiten zugewiesen werden müssen, um zu einer funktionierenden Vereinbarung zu gelangen. Der EDSA stellt fest, dass es Situationen gibt, in denen die Einflussmöglichkeiten eines der gemeinsamen Verantwortlichen und seine tatsächliche Einflussnahme den Abschluss einer Vereinbarung erschweren. Diese Umstände stehen jedoch der

[72] „In jedem Fall sollte die Vereinbarung der gemeinsam Verantwortlichen umfassend auf alle Zuständigkeiten der gemeinsam Verantwortlichen eingehen, einschließlich derjenigen, die möglicherweise bereits im einschlägigen Recht der EU oder der Mitgliedstaaten festgelegt sind, und unbeschadet der Verpflichtung der gemeinsam Verantwortlichen, das Wesentliche der Vereinbarung zwischen den gemeinsam Verantwortlichen gemäß Artikel 26 Absatz 2 DSGVO zur Verfügung zu stellen.“

gemeinsamen Verantwortlichkeit nicht entgegen und können nicht dazu dienen, eine der Parteien von ihren Verpflichtungen gemäß der DSGVO zu befreien.

164. Konkret heißt es in Artikel 26 Absatz 1, dass die Festlegung ihrer jeweiligen Verpflichtungen (d.h. Aufgaben) von den gemeinsam Verantwortlichen „*insbesondere*" im Hinblick auf die Wahrnehmung der Rechte der betroffenen Person und die Erfüllung der Informationspflichten gemäß den Artikeln 13 und 14 vorzunehmen ist, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind.

165. Aus dieser Bestimmung geht ganz klar hervor, dass gemeinsam Verantwortliche festlegen müssen, wer jeweils für die Beantwortung von Anträgen zuständig ist, wenn betroffene Personen ihre durch die DSGVO gewährten Rechte ausüben, und wer ihnen Informationen gemäß den Artikeln 13 und 14 DSGVO zur Verfügung stellt. Dies bezieht sich nur darauf, dass sie in ihrem Innenverhältnis festzulegen haben, welche der Parteien verpflichtet ist, auf welche Anträge betroffener Personen zu antworten. Ungeachtet einer solchen Vereinbarung kann sich die betroffene Person gemäß Artikel 26 Absatz 3 DSGVO an jeden einzelnen der gemeinsam Verantwortlichen wenden. Die Verwendung des Begriffs *insbesondere* weist jedoch darauf hin, dass die Verpflichtungen, die Gegenstand der in dieser Bestimmung genannten Aufteilung der Zuständigkeiten zwecks Einhaltung durch jede beteiligte Partei sind, nicht erschöpfend sind. Daraus folgt, dass sich die Aufteilung der Zuständigkeiten für die Einhaltung unter den gemeinsam Verantwortlichen nicht auf die in Artikel 26 Absatz 1 genannten Themen beschränkt, sondern sich auch auf andere Verpflichtungen des Verantwortlichen im Rahmen der DSGVO erstreckt. Gemeinsam Verantwortliche müssen nämlich sicherstellen, dass die gesamte gemeinsame Verarbeitung in vollem Umfang mit der DSGVO im Einklang steht.

166. Daher sollten gemeinsam Verantwortliche bei der Festlegung ihrer jeweiligen Zuständigkeiten neben den in Artikel 26 Absatz 1 ausdrücklich genannten Verpflichtungen unter anderem folgende Compliance-Maßnahmen und damit verbundene Verpflichtungen berücksichtigen:

- die Umsetzung der allgemeinen Datenschutzgrundsätze (Artikel 5)
- die Rechtsgrundlage der Verarbeitung[73] (Artikel 6)
- Sicherheitsmaßnahmen (Artikel 32)
- die Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde und die betroffene Person[74] (Artikel 33 und 34)
- Datenschutz-Folgenabschätzungen (Artikel 35 und 36)[75]

[73] Obwohl die DSGVO gemeinsam Verantwortliche nicht daran hindert, für von ihnen durchgeführte unterschiedliche Verarbeitungsvorgänge unterschiedliche Rechtsgrundlagen zu verwenden, wird doch empfohlen, für einen bestimmten Zweck soweit möglich dieselbe Rechtsgrundlage zu verwenden.

[74] Vgl. auch die Leitlinien des EDSA zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung 2016/679, WP250.rev.01, in denen festgelegt ist, dass bei gemeinsam Verantwortlichen „*auch die für die Einhaltung der Verpflichtungen aus den Artikeln 33 und 34 verantwortliche Partei benannt werden muss. Die Artikel 29-Datenschutzgruppe empfiehlt, in den vertraglichen Vereinbarungen zwischen gemeinsam für die Verarbeitung Verantwortlichen ausdrücklich zu regeln, welcher Verantwortliche in Bezug auf die Einhaltung der Pflicht zur Meldung von Datenschutzverletzungen die führende Rolle übernimmt bzw. die Verantwortung trägt*" (S. 15).

[75] Vgl. auch die Leitlinien des EDSA zur Datenschutz-Folgenabschätzung, WP248.rev01, in denen es heißt: „*Sollten für den fraglichen Verarbeitungsvorgang mehrere Verantwortliche gemeinsam für die Verarbeitung zuständig sein, müssen deren jeweilige Aufgaben genau festgelegt sein. In ihrer DSFA müssen sie angeben, welcher*

- der Einsatz eines Auftragsverarbeiters (Artikel 28)
- Datenübermittlungen an Drittländer (Kapitel V)
- die Organisation des Kontakts mit betroffenen Personen und Aufsichtsbehörden

167. Weitere Themen, die je nach der betreffenden Verarbeitung und der Absicht der Parteien in Betracht gezogen werden könnten, sind beispielsweise die Beschränkungen bei der Verwendung personenbezogener Daten für einen anderen Zweck durch einen der gemeinsam Verantwortlichen. In dieser Hinsicht sind beide Verantwortlichen stets verpflichtet sicherzustellen, dass beide über eine Rechtsgrundlage für die Verarbeitung verfügen. Es kommt vor, dass im Rahmen gemeinsamer Verantwortlichkeit personenbezogene Daten von einem Verantwortlichen an einen anderen weitergegeben werden. Aus Gründen der Rechenschaftspflicht hat jeder Verantwortliche die Pflicht, dafür zu sorgen, dass die Daten nicht in einer Weise weiterverarbeitet werden, die mit den Zwecken unvereinbar ist, für die sie ursprünglich von dem Verantwortlichen, der die Daten teilt, erhoben wurden.[76]

168. Gemeinsam Verantwortliche können ein gewisses Maß an Flexibilität bei der Verteilung und Zuweisung der Pflichten untereinander haben, solange sie die vollständige Einhaltung der DSGVO in Bezug auf eine bestimmte Verarbeitung gewährleisten. Bei der Zuweisung sollte berücksichtigt werden, wer kompetent und in der Lage ist, die Rechte der betroffenen Person wirksam zu gewährleisten und die einschlägigen Verpflichtungen aus der DSGVO zu erfüllen. Der EDSA empfiehlt, die relevanten Faktoren und die interne Beurteilung zu dokumentieren, die durchgeführt wurde, um die verschiedenen Verpflichtungen zuzuweisen. Diese Beurteilung ist Teil der Dokumentation nach dem Grundsatz der Rechenschaftspflicht.

169. Die Pflichten müssen nicht gleichmäßig auf die gemeinsam Verantwortlichen verteilt werden. In diesem Zusammenhang hat der EuGH kürzlich klargestellt, „*dass das Bestehen einer gemeinsamen Verantwortlichkeit (...) aber nicht zwangsläufig eine gleiche Verantwortlichkeit der verschiedenen Akteure zur Folge hat, die an einer Verarbeitung personenbezogener Daten beteiligt sind*".[77] Es kann jedoch Fälle geben, in denen nicht alle Pflichten verteilt werden können und alle gemeinsam Verantwortlichen unter Berücksichtigung der Art und des Kontexts der gemeinsamen Verarbeitung dieselben Anforderungen aus der DSGVO erfüllen müssen. Beispielsweise müssen gemeinsam Verantwortliche, die gemeinsame Datenverarbeitungsinstrumente oder -systeme verwenden, beide sicherstellen, dass insbesondere der Grundsatz der Zweckbindung eingehalten wird, und geeignete Maßnahmen ergreifen, um die Sicherheit der mit den gemeinsamen Instrumenten verarbeiteten personenbezogenen Daten zu gewährleisten.

Beteiligte für die verschiedenen Maßnahmen zuständig ist, mit denen die Risiken angegangen und die Rechte und Freiheiten der Betroffenen geschützt werden. Jeder für die Datenverarbeitung Verantwortliche muss angeben, was er benötigt, und den anderen Beteiligten hilfreiche Informationen bereitstellen, ohne Geheimnisse (z. B. Schutz von Betriebsgeheimnissen, von geistigem Eigentum, von vertraulichen Geschäftsinformationen) oder Schwachstellen preiszugeben" (S. 8).

[76] Jede Offenlegung durch einen für die Verarbeitung Verantwortlichen erfordert eine Rechtsgrundlage und eine Beurteilung der Vereinbarkeit, unabhängig davon, ob es sich bei dem Empfänger um einen getrennt Verantwortlichen oder einen gemeinsam Verantwortlichen handelt. Mit anderen Worten bedeutet das Bestehen einer gemeinsamen Verantwortlichkeit nicht automatisch, dass der gemeinsam Verantwortliche, der die Daten erhält, die Daten auch für weitere Zwecke, die außerhalb des Bereichs der gemeinsamen Verantwortlichkeit liegen, rechtmäßig verarbeiten kann.

[77] Urteil *Wirtschaftsakademie*, C-210/16, ECLI: EU: C: 2018: 388, Rn. 43.

170. Ein weiteres Beispiel ist die Anforderung, dass jeder der gemeinsam Verantwortlichen ein Verzeichnis der Verarbeitungstätigkeiten führen oder einen Datenschutzbeauftragten (DSB) benennen muss, wenn die Bedingungen von Artikel 37 Absatz 1 erfüllt sind. Solche Anforderungen stehen nicht im Zusammenhang mit der gemeinsamen Verarbeitung, sondern gelten für sie in ihrer Funktion als für die Verarbeitung Verantwortliche.

2.2 Die Zuweisung der Zuständigkeiten muss im Wege einer Vereinbarung erfolgen

2.2.1 Form der Vereinbarung

171. Artikel 26 Absatz 1 DSGVO sieht als neue Verpflichtung für gemeinsam Verantwortliche vor, dass sie *in einer Vereinbarung* ihre jeweiligen Zuständigkeiten festlegen. Die rechtliche Form einer solchen Vereinbarung wird in der DSGVO nicht vorgegeben. Daher steht es den gemeinsam Verantwortlichen frei, sich auf die Form der Vereinbarung zu einigen.

172. Darüber hinaus ist die Vereinbarung über die Aufteilung der Zuständigkeiten für jeden der gemeinsam Verantwortlichen verbindlich. Sie vereinbaren und verpflichten sich *gegenseitig*, die jeweiligen Verpflichtungen, die in ihrer Vereinbarung als ihre Zuständigkeit festgelegt sind, einzuhalten.

173. Daher empfiehlt der EDSA im Interesse der Rechtssicherheit, auch wenn die DSGVO keinen Vertrag oder ein anderes Rechtsinstrument vorschreibt, eine solche Vereinbarung in Form eines bindenden Dokuments wie eines Vertrags oder eines anderen bindenden Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem die Verantwortlichen unterliegen, zu treffen. Dies würde Sicherheit schaffen und könnte dazu genutzt werden, Transparenz nachzuweisen und der Rechenschaftspflicht nachzukommen. Wird nämlich die in der Vereinbarung niedergelegte Zuweisung nicht eingehalten, kann ein Verantwortlicher aufgrund des verbindlichen Charakters der Vereinbarung die Haftung des anderen Verantwortlichen für das, was in der Vereinbarung als in dessen Zuständigkeitsbereich fallend festgelegt ist, geltend machen. Im Einklang mit dem Grundsatz der Rechenschaftspflicht wird die Verwendung eines Vertrags oder eines anderen Rechtsinstruments es den gemeinsam Verantwortlichen zudem ermöglichen nachzuweisen, dass sie die ihnen durch die DSGVO auferlegten Verpflichtungen erfüllen.

174. Die Art und Weise, wie die Zuständigkeiten, d. h. die Aufgaben, zwischen den einzelnen gemeinsam für die Verarbeitung Verantwortlichen aufgeteilt werden, muss in der Vereinbarung klar und eindeutig angegeben werden.[78] Diese Anforderung ist wichtig, da sie Rechtssicherheit gewährleistet und mögliche Konflikte nicht nur in der Beziehung zwischen den gemeinsam Verantwortlichen, sondern auch gegenüber den betroffenen Personen und den Datenschutzbehörden verhindert.

175. Im Sinne einer reibungslosen Zuweisung der Zuständigkeiten an die Parteien empfiehlt der EDSA, dass die Vereinbarung auch allgemeine Informationen über die gemeinsame Verarbeitung enthält, insbesondere zum Gegenstand und Zweck der Verarbeitung, zur Art der personenbezogenen Daten und zu den Kategorien betroffener Personen.

[78] In Erwägungsgrund 79 der DSGVO heißt es: *„(...) bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung, einschließlich der Fälle, in denen ein Verantwortlicher die Verarbeitungszwecke und -mittel gemeinsam mit anderen Verantwortlichen festlegt“*.

2.2.2 Pflichten gegenüber betroffenen Personen

176. Die DSGVO sieht mehrere Pflichten der gemeinsam Verantwortlichen gegenüber betroffenen Personen vor:

Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln

177. Ergänzend zu den Ausführungen in Abschnitt 2.1 dieser Leitlinien sei unterstrichen, dass es wichtig ist, dass die gemeinsam für die Verarbeitung Verantwortlichen in der Vereinbarung ihre jeweilige Rolle, *insbesondere* in Bezug auf die Ausübung der Rechte der betroffenen Person und ihre Informationspflichten nach den Artikeln 13 und 14, klarstellen. In Artikel 26 DSGVO wird die Bedeutung dieser besonderen Verpflichtungen hervorgehoben. Die gemeinsam Verantwortlichen müssen daher organisieren und vereinbaren, wie und von wem die Informationen bereitgestellt werden und wie und von wem die Antworten auf die Anfragen der betroffenen Person erteilt werden. Unabhängig vom Inhalt der Vereinbarung zu diesem besonderen Punkt kann sich die betroffene Person gemäß Artikel 26 Absatz 3 an jeden einzelnen der gemeinsam Verantwortlichen wenden, um ihre Rechte, wie nachstehend näher erläutert, wahrzunehmen.

178. Die Art und Weise, wie diese Verpflichtungen in der Vereinbarung umgesetzt sind, sollte *gebührend*, d. h. genau, die Realität der zugrunde liegenden gemeinsamen Verarbeitung widerspiegeln. Wenn beispielsweise nur einer der gemeinsam Verantwortlichen mit den betroffenen Personen für die Zwecke der gemeinsamen Verarbeitung kommuniziert, könnte dieser Verantwortliche besser in der Lage sein, die betroffenen Personen zu informieren und gegebenenfalls ihre Anträge zu beantworten.

Das Wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt

179. Mit dieser Bestimmung soll sichergestellt werden, dass der betroffenen Person das „*Wesentliche der Vereinbarung*“ bekannt ist. So muss beispielsweise für die betroffene Person völlig klar sein, welcher Verantwortliche als Ansprechpartner für die Ausübung der Rechte betroffener Personen dient (ungeachtet der Tatsache, dass sie ihre Rechte bei und gegenüber jedem der gemeinsam Verantwortlichen geltend machen kann). Die Verpflichtung, den betroffenen Personen das Wesentliche der Vereinbarung zur Verfügung zu stellen, ist im Falle einer gemeinsamen Verantwortlichkeit wichtig, damit die betroffene Person weiß, welcher der Verantwortlichen wofür zuständig ist.

180. Was unter den Begriff *das Wesentliche der Vereinbarung* fallen sollte, wird in der DSGVO nicht definiert. Der EDSA empfiehlt, dass das Wesentliche zumindest alle Elemente der in den Artikeln 13 und 14 genannten Informationen umfasst, die der betroffenen Person bereits zugänglich sein sollten, und für jedes dieser Elemente sollte in der Vereinbarung festgelegt werden, welcher der gemeinsam Verantwortlichen für die Gewährleistung der Einhaltung dieser Elemente zuständig ist. Das Wesentliche der Vereinbarung muss auch die Anlaufstelle umfassen, falls eine solche benannt wurde.

181. Auf welche Weise diese Informationen der betroffenen Person zur Verfügung gestellt werden, ist nicht geregelt. Im Gegensatz zu anderen Bestimmungen der DSGVO (wie Artikel 30 Absatz 4 für das Verzeichnis von Verarbeitungstätigkeiten oder Artikel 40 Absatz 11 für das Register genehmigter Verhaltensregeln) enthält Artikel 26 keinen Hinweis darauf, dass die Informationen *auf Anfrage* verfügbar sein oder *in geeigneter Weise veröffentlicht werden* sollten. Daher ist es Sache der gemeinsam Verantwortlichen, zu entscheiden, wie das Wesentliche der Vereinbarung den betroffenen Personen am wirksamsten zur Verfügung gestellt werden kann (z. B. zusammen mit den Informationen gemäß Artikel 13 oder 14, in der Datenschutzerklärung oder auf Anfrage beim Datenschutzbeauftragten, falls vorhanden, oder bei der gegebenenfalls benannten Kontaktstelle).

Gemeinsam Verantwortliche sollten dafür sorgen, dass die Informationen in übereinstimmender Weise bereitgestellt werden.

In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden

182. Artikel 26 Absatz 1 sieht für gemeinsam Verantwortliche die Möglichkeit vor, in der Vereinbarung eine Anlaufstelle für die betroffenen Personen anzugeben. Eine solche Angabe ist nicht zwingend vorgeschrieben.

183. Wenn betroffene Personen über eine einzige Möglichkeit informiert werden, sich mit mehreren gemeinsam Verantwortlichen in Verbindung zu setzen, wissen sie, an wen sie sich in allen Fragen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten wenden können. Darüber hinaus können auf diese Weise mehrere gemeinsam Verantwortliche ihre Beziehungen zu den betroffenen Personen und ihre Kommunikation mit ihnen effizienter koordinieren.

184. Aus diesen Gründen empfiehlt der EDSA gemeinsam Verantwortlichen, eine solche Anlaufstelle anzugeben, um die Ausübung der Rechte der betroffenen Personen gemäß der DSGVO zu erleichtern.

185. Bei der Anlaufstelle kann es sich um den Datenschutzbeauftragten, falls vorhanden, um den Vertreter in der Union (bei gemeinsam Verantwortlichen, die nicht in der Union niedergelassen sind) oder jede andere Anlaufstelle, bei der Informationen erhältlich sind, handeln.

Ungeachtet der Einzelheiten der Vereinbarung können betroffene Personen ihre Rechte bei und gegenüber jedem der gemeinsam Verantwortlichen geltend machen

186. Nach Artikel 26 Absatz 3 ist eine betroffene Person nicht an die Bestimmungen der Vereinbarung gebunden und kann ihre Rechte aus der DSGVO bei und gegenüber jedem einzelnen der gemeinsam für die Verarbeitung Verantwortlichen geltend machen.

187. Beispielsweise kann sich die betroffene Person bei gemeinsam Verantwortlichen, die in verschiedenen Mitgliedstaaten niedergelassen sind, oder wenn nur einer der gemeinsam Verantwortlichen in der Union niedergelassen ist, nach ihrer Wahl entweder an den Verantwortlichen wenden, der in dem Mitgliedstaat niedergelassen ist, in dem die betroffenen Person ihren gewöhnlichen Aufenthalt oder ihren Arbeitsplatz hat, oder an den Verantwortlichen, der in einem anderen Mitgliedstaat der EU oder des EWR niedergelassen ist.

188. Selbst wenn die Vereinbarung und ihre wesentlichen Bestimmungen eine Anlaufstelle für die Entgegennahme und Bearbeitung der Anträge aller betroffenen Personen vorsehen, können sich die betroffenen Personen trotzdem für einen anderen Weg entscheiden.

189. Daher ist es wichtig, dass gemeinsam für die Verarbeitung Verantwortliche im Voraus in ihrer Vereinbarung regeln, wie sie die Beantwortung von Anfragen, die sie möglicherweise von betroffenen Personen erhalten, handhaben wollen. In diesem Zusammenhang wird empfohlen, dass gemeinsam Verantwortliche die anderen Verantwortlichen oder die angegebene Anlaufstelle über die eingegangenen Anfragen informieren, damit sie effizient bearbeitet werden können. Betroffene Personen zu verpflichten, sich an die angegebene Anlaufstelle oder den für die Verarbeitung Verantwortlichen zu wenden, würde für die betroffene Person einen übermäßigen Aufwand bedeuten, der dem Ziel zuwiderliefe, die Wahrnehmung ihrer Rechte aus der DSGVO zu erleichtern.

2.3 Pflichten gegenüber den Datenschutzbehörden

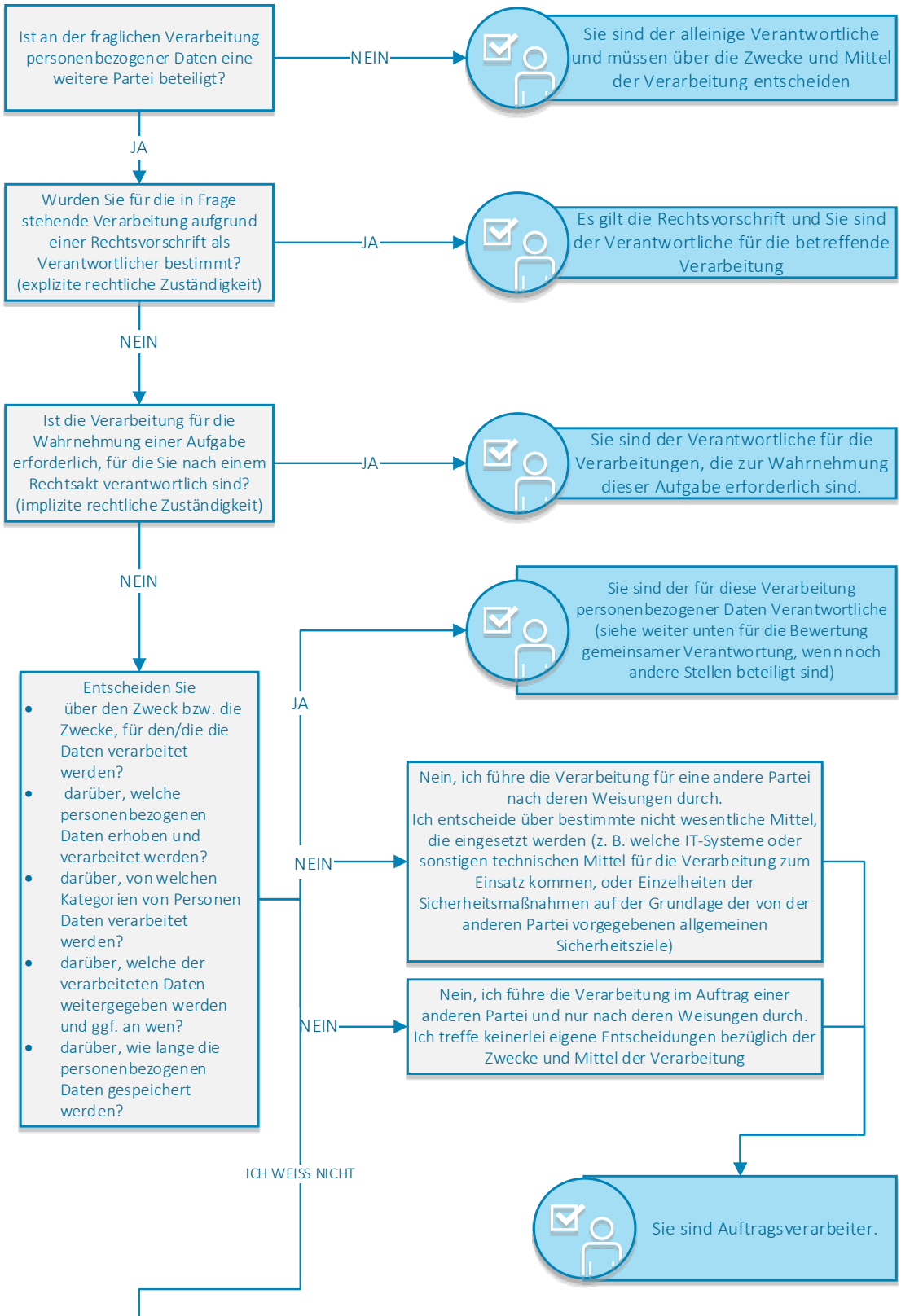
190. Gemeinsam Verantwortliche sollten in der Vereinbarung regeln, wie sie mit den zuständigen Datenschutzaufsichtsbehörden kommunizieren werden. Diese Kommunikation könnte eine mögliche

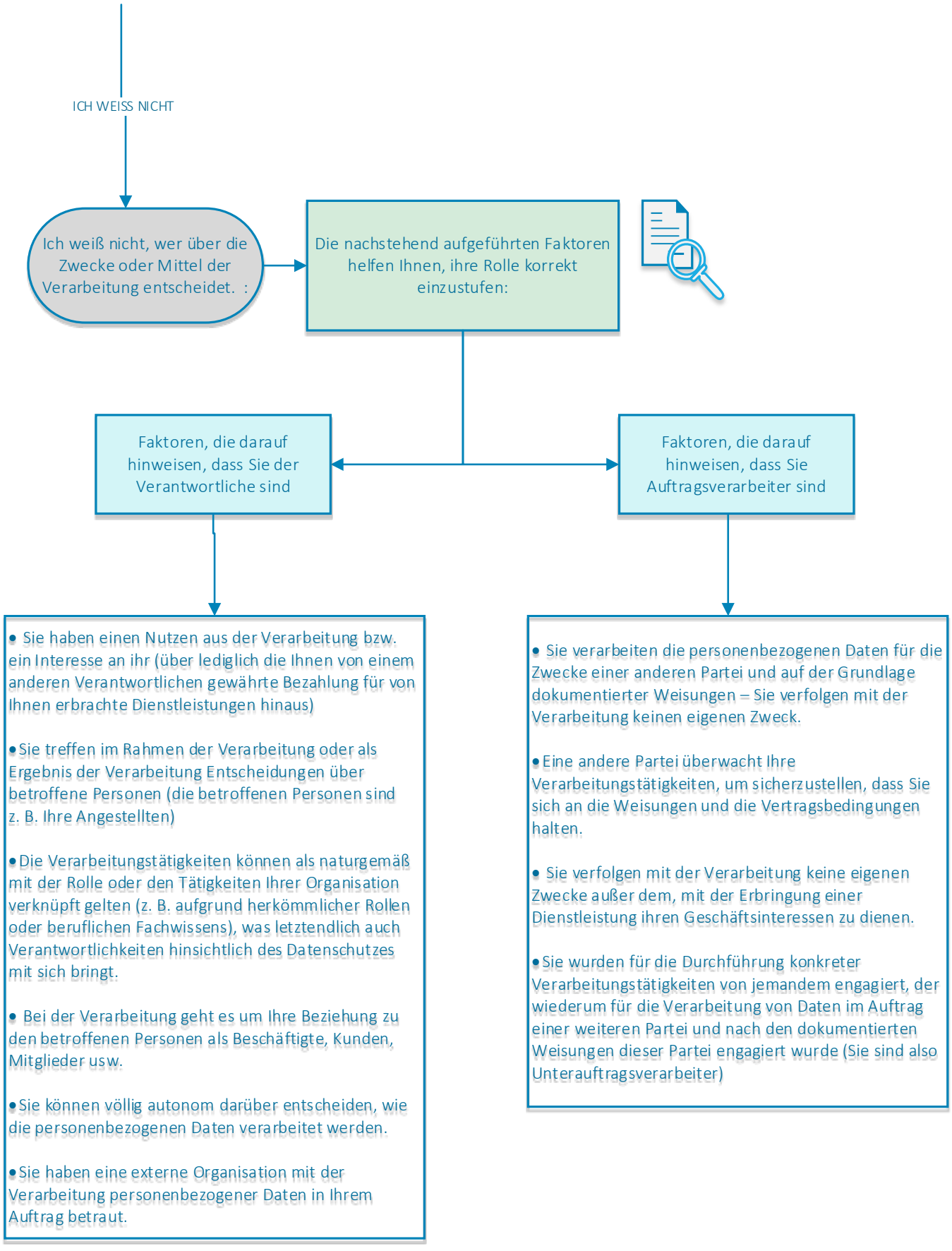
Konsultation gemäß Artikel 36 DSGVO, die Meldung einer Verletzung des Schutzes personenbezogener Daten oder die Benennung eines Datenschutzbeauftragten betreffen.

- Es sei daran erinnert, dass die Datenschutzaufsichtsbehörden nicht an die Bestimmungen der Vereinbarung gebunden sind, weder in Bezug auf die Frage der Einstufung der Parteien als gemeinsam Verantwortliche noch hinsichtlich der angegebenen Anlaufstelle. Daher können die Behörden sich an jeden der gemeinsam Verantwortlichen wenden, um ihre Befugnisse gemäß Artikel 58 in Bezug auf die gemeinsame Verarbeitung auszuüben.

Anhang I – Ablaufdiagramm für die Anwendung der Begriffe „Verantwortlicher“, „Auftragsverarbeiter“ und „gemeinsam Verantwortliche“ in der Praxis

Anmerkung: Um die Rolle der einzelnen beteiligten Stellen korrekt beurteilen zu können, müssen zunächst die betreffende konkrete Verarbeitung personenbezogener Daten und ihr genauer Zweck ermittelt werden. Sind mehrere Stellen daran beteiligt, muss zunächst ermittelt werden, ob die Zwecke und Mittel gemeinsam festgelegt werden, also eine gemeinsame Verantwortlichkeit besteht.




ICH WEISS NICHT
Ich weiß nicht, wer über die Zwecke oder Mittel der Verarbeitung entscheidet. :
Die nachstehend aufgeführten Faktoren helfen Ihnen, ihre Rolle korrekt einzustufen:
Faktoren, die darauf hinweisen, dass Sie der Verantwortliche sind
Faktoren, die darauf hinweisen, dass Sie Auftragsverarbeiter sind
• Sie haben einen Nutzen aus der Verarbeitung bzw. ein Interesse an ihr (über lediglich die Ihnen von einem anderen Verantwortlichen gewährte Bezahlung für von Ihnen erbrachte Dienstleistungen hinaus)
• Sie treffen im Rahmen der Verarbeitung oder als Ergebnis der Verarbeitung Entscheidungen über betroffene Personen (die betroffenen Personen sind z. B. Ihre Angestellten)
• Die Verarbeitungstätigkeiten können als naturgemäß mit der Rolle oder den Tätigkeiten Ihrer Organisation verknüpft gelten (z. B. aufgrund herkömmlicher Rollen oder beruflichen Fachwissens), was letztendlich auch Verantwortlichkeiten hinsichtlich des Datenschutzes mit sich bringt.
• Bei der Verarbeitung geht es um Ihre Beziehung zu den betroffenen Personen als Beschäftigte, Kunden, Mitglieder usw.
• Sie können völlig autonom darüber entscheiden, wie die personenbezogenen Daten verarbeitet werden.
• Sie haben eine externe Organisation mit der Verarbeitung personenbezogener Daten in Ihrem Auftrag betraut.
• Sie verarbeiten die personenbezogenen Daten für die Zwecke einer anderen Partei und auf der Grundlage dokumentierter Weisungen – Sie verfolgen mit der Verarbeitung keinen eigenen Zweck.
• Eine andere Partei überwacht Ihre Verarbeitungstätigkeiten, um sicherzustellen, dass Sie sich an die Weisungen und die Vertragsbedingungen halten.
• Sie verfolgen mit der Verarbeitung keine eigenen Zwecke außer dem, mit der Erbringung einer Dienstleistung ihren Geschäftsinteressen zu dienen.
• Sie wurden für die Durchführung konkreter Verarbeitungstätigkeiten von jemandem engagiert, der wiederum für die Verarbeitung von Daten im Auftrag einer weiteren Partei und nach den dokumentierten Weisungen dieser Partei engagiert wurde (Sie sind also Unterauftragsverarbeiter)

Gemeinsame Verantwortlichkeit – Sie sind der Verantwortliche, und an der Verarbeitung personenbezogener Daten sind noch andere Parteien beteiligt