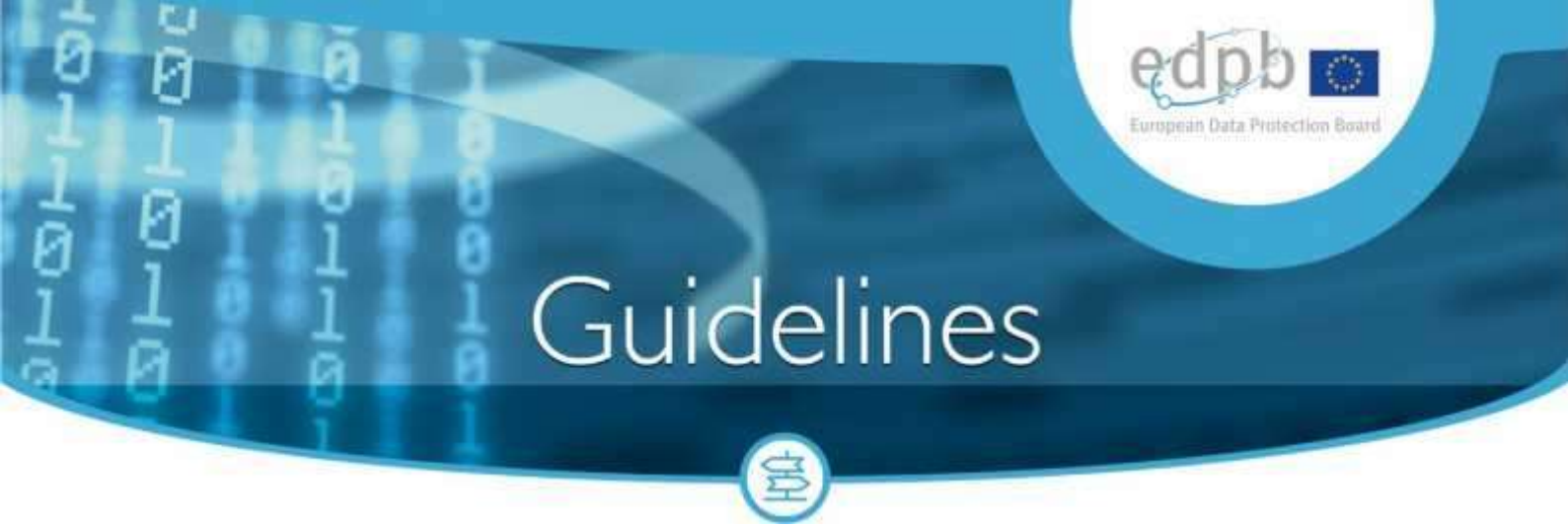


Leitlinien 07/2020 zu den Begriffen des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters in der GDPR

Version 2.0

Verabschiedet am 07. Juli 2021

Versionsgeschichte

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

KURZFASSUNG

Die Begriffe "für die Verarbeitung Verantwortlicher", "gemeinsam für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter" spielen bei der Anwendung der Datenschutz-Grundverordnung (DSGVO) 2016/679 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 korrekte Auslegung müssen im gesamten Europäischen Wirtschaftsraum (EWR) hinreichend klar und einheitlich sein.

Die Begriffe "für die Verarbeitung Verantwortlicher", "gemeinsam für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter" sind *funktionale* Begriffe, da sie darauf abzielen, die Verantwortlichkeiten entsprechend den tatsächlichen Rollen der Parteien zuzuweisen, und *autonome* Begriffe in dem Sinne, dass sie hauptsächlich gemäß dem EU-Datenschutzrecht ausgelegt werden sollten.

Controller

Im Prinzip gibt es keine Einschränkung hinsichtlich der Art der Einheit, die die Rolle des für die Verarbeitung Verantwortlichen übernehmen kann, aber in der Praxis ist es normalerweise die Organisation als solche und nicht eine Einzelperson innerhalb der Organisation (wie der CEO, ein Mitarbeiter oder ein Vorstandsmitglied), die als für die Verarbeitung Verantwortlicher handelt.

Ein für die Verarbeitung Verantwortlicher ist eine Stelle, die *über* bestimmte Schlüsselelemente der Verarbeitung *entscheidet*. Die Rolle des für die Verarbeitung Verantwortlichen kann gesetzlich festgelegt sein oder sich aus einer Analyse der tatsächlichen Elemente oder Umstände des Falles ergeben. Bestimmte Verarbeitungstätigkeiten können als natürlich mit der Rolle einer Stelle verbunden angesehen werden (ein Arbeitgeber gegenüber seinen Mitarbeitern, ein Verlag gegenüber seinen Abonnenten oder ein Verein gegenüber seinen Mitgliedern). In vielen Fällen können die Vertragsbedingungen helfen, den für die Verarbeitung Verantwortlichen zu identifizieren, obwohl sie nicht unter allen Umständen entscheidend sind.

Ein für die Verarbeitung Verantwortlicher bestimmt die Zwecke und Mittel der Verarbeitung, d. h. das *Warum* und *Wie* der Verarbeitung. Der für die Verarbeitung Verantwortliche muss sowohl über die Zwecke als auch über die Mittel entscheiden. Einige praktischere Aspekte der Umsetzung ("nicht wesentliche Mittel") können jedoch dem Auftragsverarbeiter überlassen werden. Es ist nicht erforderlich, dass der für die Verarbeitung Verantwortliche tatsächlich Zugang zu den Daten hat, die verarbeitet werden, um als für die Verarbeitung Verantwortlicher qualifiziert zu sein.

Gemeinsame Steuerungen

Die Qualifikation als gemeinsam für die Verarbeitung Verantwortliche kann sich ergeben, wenn mehr als ein Akteur an der Verarbeitung beteiligt ist. Die DSGVO führt spezifische Regeln für gemeinsam für die Verarbeitung Verantwortliche ein und legt einen Rahmen fest, der ihre Beziehung regelt. Das übergreifende Kriterium für das Vorliegen einer gemeinsamen Verantwortlichkeit ist die gemeinsame Beteiligung von zwei oder mehr Stellen an der Festlegung der Zwecke und Mittel einer Verarbeitung. Die gemeinsame Beteiligung kann in Form eines *gemeinsamen Beschlusses* von zwei oder mehr Stellen erfolgen oder sich aus *konvergierenden Beschlüssen* von zwei oder mehr Stellen ergeben, wobei die Beschlüsse einander ergänzen und für die Verarbeitung in einer Weise erforderlich sind, dass sie sich spürbar auf die Festlegung der Zwecke und Mittel der Verarbeitung auswirken. Ein wichtiges Kriterium ist, dass die Verarbeitung ohne die Mitwirkung beider Parteien nicht möglich wäre, in dem Sinne, dass die Verarbeitung durch jede Partei untrennbar, d. h. unauflösbar miteinander verbunden ist. Die gemeinsame Mitwirkung muss die Festlegung der Zwecke einerseits und die Festlegung der Mittel andererseits umfassen.

Prozessor

Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. Zwei Grundvoraussetzungen für die Qualifikation als Auftragsverarbeiter bestehen: dass es sich um eine im

Verhältnis zum Verantwortlichen getrennte Einheit handelt und dass sie personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Der Auftragsverarbeiter darf die Daten nicht anders als nach den Anweisungen des für die Verarbeitung Verantwortlichen verarbeiten. Die Anweisungen des für die Verarbeitung Verantwortlichen können immer noch einen gewissen Ermessensspielraum darüber lassen, wie er die Interessen des für die Verarbeitung Verantwortlichen, so dass der Auftragsverarbeiter die am besten geeigneten technischen und organisatorischen Mittel wählen kann. Ein Auftragsverarbeiter verstößt jedoch gegen die DSGVO, wenn er über die Anweisungen des für die Verarbeitung Verantwortlichen hinausgeht und beginnt, seine eigenen Zwecke und Mittel für die Verarbeitung zu bestimmen. Der Auftragsverarbeiter wird dann in Bezug auf diese Verarbeitung als Verantwortlicher betrachtet und kann Sanktionen für das Überschreiten der Anweisungen des Verantwortlichen unterliegen.

Beziehung zwischen Controller und Prozessor

Ein für die Verarbeitung Verantwortlicher darf nur Auftragsverarbeiter einsetzen, die ausreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen bieten, damit die Verarbeitung den Anforderungen der DSGVO entspricht. Zu berücksichtigende Elemente könnten das Fachwissen des Auftragsverarbeiters (z. B. technisches Fachwissen in Bezug auf Sicherheitsmaßnahmen und Datenschutzverletzungen), die Zuverlässigkeit des Auftragsverarbeiters, die Ressourcen des Auftragsverarbeiters und die Einhaltung eines genehmigten Verhaltenskodex oder Zertifizierungsmechanismus durch den Auftragsverarbeiter sein.

Jede Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter muss durch einen Vertrag oder einen anderen Rechtsakt geregelt werden, der schriftlich, auch in elektronischer Form, abgeschlossen werden muss und verbindlich ist. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter können wählen, ob sie einen eigenen Vertrag aushandeln, der alle obligatorischen Elemente enthält, oder ob sie sich ganz oder teilweise auf Standardvertragsklauseln stützen.

Die DSGVO listet die Elemente auf, die in der Verarbeitungsvereinbarung dargelegt werden müssen. Die Verarbeitungsvereinbarung sollte jedoch nicht einfach nur die Bestimmungen der DSGVO wiedergeben, sondern sie sollte spezifischere, konkrete Informationen darüber enthalten, wie die Anforderungen erfüllt werden und welches Sicherheitsniveau für die Verarbeitung personenbezogener Daten, die Gegenstand der Verarbeitungsvereinbarung ist, erforderlich ist.

Beziehung zwischen gemeinsamen Steuerungen

Gemeinsam für die Verarbeitung Verantwortliche müssen auf transparente Weise ihre jeweiligen Verantwortlichkeiten für die Einhaltung der Verpflichtungen aus der DSGVO festlegen und vereinbaren. Die Festlegung ihrer jeweiligen Verantwortlichkeiten muss insbesondere die Ausübung der Rechte der betroffenen Personen und die Informationspflichten berücksichtigen. Darüber hinaus sollte die Verteilung der Verantwortlichkeiten auch andere Pflichten des für die Verarbeitung Verantwortlichen abdecken, z. B. hinsichtlich der allgemeinen Datenschutzgrundsätze, der Rechtsgrundlage, der Sicherheitsmaßnahmen, der Pflicht zur Meldung von Datenschutzverletzungen, der Datenschutz-Folgenabschätzungen, des Einsatzes von Auftragsverarbeitern, der Übermittlung in Drittländer und der Kontakte mit betroffenen Personen und Aufsichtsbehörden.

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

Die rechtliche Form der Vereinbarung zwischen gemeinsam für die Verarbeitung Verantwortlichen ist in der DSGVO nicht festgelegt. Aus Gründen der Rechtssicherheit und um für Transparenz und Rechenschaftspflicht zu sorgen, empfiehlt der EDSB, dass eine solche Vereinbarung in Form eines verbindlichen Dokuments wie eines Vertrags oder eines anderen rechtsverbindlichen Akts nach dem Recht der EU oder eines Mitgliedstaats, dem die für die Verarbeitung Verantwortlichen unterliegen, getroffen wird.

Die Vereinbarung muss die jeweiligen Rollen und Beziehungen der gemeinsam für die Verarbeitung Verantwortlichen gegenüber den betroffenen Personen angemessen widerspiegeln, und der Kern der Vereinbarung muss der betroffenen Person zugänglich gemacht werden.

Unabhängig von den Bedingungen der Vereinbarung können die betroffenen Personen ihre Rechte gegenüber jedem der gemeinsam für die Verarbeitung Verantwortlichen geltend machen. Die Aufsichtsbehörden sind nicht an die Bedingungen der Vereinbarung gebunden, weder bei der Frage der Qualifikation der Parteien als gemeinsam für die Verarbeitung Verantwortliche noch bei der Frage der benannten Kontaktstelle.

INHALTSVERZEICHNIS

Der Europäische Datenschutzausschuss

gestützt auf Artikel 70 (1e) 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, (nachfolgend "DSGVO" oder "die Verordnung"),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 20181,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

Im Rahmen der Vorarbeiten zu diesen Leitlinien wurden Beiträge von Stakeholdern gesammelt, sowohl schriftlich als auch im Rahmen einer Stakeholder-Veranstaltung, um die dringendsten Herausforderungen zu identifizieren;

HAT DIE FOLGENDEN RICHTLINIEN VERABSCHIEDET

EINLEITUNG

1. Dieses Dokument soll eine Orientierungshilfe zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter" bieten, die sich auf die Vorschriften der DSGVO zu den Begriffsbestimmungen in Artikel 4 und die Bestimmungen zu den Pflichten in Kapitel IV stützt. Das Hauptziel ist es, die Bedeutung der Begriffe zu klären und die verschiedenen Rollen und die Verteilung der Verantwortlichkeiten zwischen diesen Akteuren zu verdeutlichen.

2. Das Konzept des für die Verarbeitung Verantwortlichen und sein Zusammenspiel 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. Die DSGVO führt ausdrücklich den Grundsatz der Rechenschaftspflicht ein, d. h. der für die Verarbeitung Verantwortliche muss für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten in Artikel 5 verantwortlich sein und dies auch nachweisen können. Darüber hinaus führt die DSGVO auch spezifischere Regeln für den Einsatz von Auftragsverarbeitern ein, und einige der Bestimmungen über die Verarbeitung personenbezogener Daten richten sich nicht nur an für die Verarbeitung Verantwortliche, sondern auch an Auftragsverarbeiter.

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

4. Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahme 1/2010 (WP169)[2] Leitlinien zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter" herausgegeben, um Klarstellungen und konkrete Beispiele in Bezug auf diese Begriffe zu liefern. Seit dem Inkrafttreten der DSGVO wurden viele Fragen dazu aufgeworfen, inwieweit die DSGVO Änderungen an den Konzepten des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters und ihrer jeweiligen Rollen mit sich bringt. Insbesondere wurden Fragen zum Inhalt und zu den Auswirkungen des Konzepts der gemeinsamen Kontrolle (z. B. gemäß Artikel 26 DSGVO) und zu den in Kapitel IV festgelegten spezifischen Verpflichtungen für Auftragsverarbeiter (z. B. gemäß Artikel 28 DSGVO) gestellt. Daher und da der EDSB anerkennt, dass die konkrete Anwendung der Konzepte weiterer Klärung bedarf, hält der EDSB es nun für erforderlich entwickeltere und spezifischere Leitlinien zu geben, um einen kohärenten und harmonisierten Ansatz in der gesamten EU und dem EWR zu gewährleisten. Die vorliegenden Leitlinien ersetzen die frühere Stellungnahme der Arbeitsgruppe 29 zu diesen Begriffen (WP169).

5. In Teil I werden in diesen Leitlinien die Definitionen der verschiedenen Konzepte des für die Verarbeitung Verantwortlichen, der gemeinsam für die Verarbeitung Verantwortlichen, des Auftragsverarbeiters und des Dritten/Empfängers erörtert. In Teil II werden weitere Hinweise zu den Konsequenzen gegeben, die mit den ~~verschiedenen Rollen des für die V~~erarbeitung Verantwortlichen, gemeinsam für die Verarbeitung Verantwortlichen und Auftragsverarbeiters verbunden sind.

TEIL I - KONZEPTE

1 ALLGEMEINE BEOBACHTUNGEN

6. Die DSGVO führt in Artikel 5 Absatz 2 ausdrücklich den Grundsatz der Rechenschaftspflicht ein, was bedeutet, dass:

   - der für die Verarbeitung Verantwortliche *für die Einhaltung der* in Artikel 5 Absatz 1 DSGVO dargelegten Grundsätze *verantwortlich ist*; und dass
   - der für die Verarbeitung Verantwortliche muss in der Lage sein, *die Einhaltung der* in Artikel 5 Absatz 1 DS-GVO genannten Grundsätze *nachzuweisen*.

   Dieses Prinzip wurde in einer Stellungnahme der Artikel 29-Arbeitsgruppe [3] beschrieben und soll hier nicht näher erörtert werden.

7. Mit der Aufnahme des Grundsatzes der Rechenschaftspflicht in die DSGVO und der Ernennung zu einem zentralen Grundsatz sollte betont werden, dass die für die Datenverarbeitung Verantwortlichen angemessene und wirksame Maßnahmen ergreifen müssen und in der Lage sein müssen, deren Einhaltung nachzuweisen. [4]

8. Der Grundsatz der Rechenschaftspflicht wurde in Artikel 24 weiter ausgearbeitet, der besagt, dass der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Maßnahmen ergreift, um sicherzustellen und **nachweisen zu können**, dass die Verarbeitung im Einklang mit der DSGVO erfolgt. Diese Maßnahmen sind zu überprüfen und erforderlichenfalls zu aktualisieren. Der Grundsatz der Rechenschaftspflicht kommt auch in Artikel 28 zum Ausdruck, in dem die Pflichten des für die Verarbeitung Verantwortlichen bei der Beauftragung eines Auftragsverarbeiters festgelegt sind.

9. Der Grundsatz der Rechenschaftspflicht richtet sich direkt an den für die Verarbeitung Verantwortlichen. Einige der spezifischeren Vorschriften sind jedoch sowohl an die für die Verarbeitung Verantwortlichen als auch an die Auftragsverarbeiter gerichtet, wie z. B. die Vorschriften über die Befugnisse der Aufsichtsbehörden in Artikel 58. Sowohl die für die Verarbeitung Verantwortlichen als auch die Auftragsverarbeiter können bei Nichteinhaltung der für sie relevanten Verpflichtungen der DSGVO mit einer Geldbuße belegt werden, und beide sind gegenüber den Aufsichtsbehörden direkt rechenschaftspflichtig, da sie verpflichtet sind, auf Verlangen geeignete Unterlagen zu führen und vorzulegen, im Falle einer Untersuchung zu kooperieren und behördlichen Anordnungen Folge zu leisten. Gleichzeitig sollte daran erinnert werden, dass Auftragsverarbeiter immer die Anweisungen des für die Verarbeitung Verantwortlichen befolgen und nur auf dessen Anweisung handeln müssen.

10. Der Grundsatz der Rechenschaftspflicht, zusammen mit den anderen, spezifischeren Regeln zur Einhaltung der DSGVO und der Verteilung der Verantwortung, macht es daher notwendig, die verschiedenen Rollen mehrerer an einer personenbezogenen Datenverarbeitung beteiligter Akteure zu definieren.

11. Eine allgemeine Beobachtung zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter" in der DSGVO ist, dass sie sich im Vergleich zur Richtlinie 95/46/EG nicht geändert haben und dass die Kriterien für die Zuweisung der verschiedenen Rollen insgesamt die gleichen bleiben.

12. Die Begriffe "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter" sind *funktionale* Begriffe: Sie zielen darauf ab, die Verantwortlichkeiten entsprechend den tatsächlichen Rollen der Parteien zuzuweisen. [5] Dies bedeutet, dass der rechtliche Status eines Akteurs als "für die Verarbeitung Verantwortlicher" oder "Auftragsverarbeiter" grundsätzlich durch seine tatsächlichen Aktivitäten in einer bestimmten Situation bestimmt werden muss, und nicht durch die formale Bezeichnung eines Akteurs als "für die Verarbeitung Verantwortlicher" oder "Auftragsverarbeiter" (z. B. in einem Vertrag). [6] Das bedeutet, dass die Zuweisung der Rollen in der Regel aus einer Analyse der faktischen Elemente oder Umstände des Falles resultieren sollte und als solche nicht verhandelbar ist.

13. Die Begriffe "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter" sind auch in dem Sinne *autonome* Begriffe, dass, obwohl externe Rechtsquellen dabei helfen können, festzustellen, wer ein für die Verarbeitung Verantwortlicher ist, dieser Begriff hauptsächlich nach dem EU-Datenschutzrecht ausgelegt werden sollte. Das Konzept des für die Verarbeitung Verantwortlichen sollte nicht durch andere - manchmal kollidierende oder sich überschneidende - Konzepte

in anderen Rechtsgebieten beeinträchtigt werden, wie z. B. den Urheber oder den Rechteinhaber in den Rechten des geistigen Eigentums oder im Wettbewerbsrecht.

14. Da das zugrunde liegende Ziel der Zuweisung der Rolle des für die Verarbeitung Verantwortlichen darin besteht, die Rechenschaftspflicht und einen wirksamen und umfassenden Schutz der personenbezogenen Daten zu gewährleisten, sollte der Begriff "für die Verarbeitung Verantwortlicher" weit genug ausgelegt werden, um einen möglichst wirksamen und vollständigen Schutz der betroffenen Personen7 zu fördern, damit die volle Wirksamkeit des EU-Datenschutzrechts gewährleistet ist, Lücken vermieden werden und eine mögliche Umgehung der Vorschriften verhindert wird, ohne dass die Rolle des Auftragsverarbeiters geschmälert wird.

2 DEFINITION DES CONTROLLERS

2.1 Definition von Controller

15. Ein für die Verarbeitung Verantwortlicher wird in Artikel 4(7) GDPR 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 personenbezogener Daten entscheidet**; werden die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten bestimmt, so können der für die Verarbeitung Verantwortliche oder die spezifischen Kriterien für seine Benennung **durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgesehen** werden".*

16. Die Definition des Begriffs "Controller" enthält fünf Hauptbausteine, die für die Zwecke dieses Leitfadens getrennt analysiert werden. Es sind dies die folgenden:

- "die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle"
- "bestimmt"
- "allein oder gemeinsam mit anderen"
- "die Zwecke und Mittel"
- "der Verarbeitung von personenbezogenen Daten".

2.1.1 "Natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle"

17. Der erste Baustein bezieht sich auf die Art der Einrichtung, die ein für die Verarbeitung Verantwortlicher sein kann. Nach der DSGVO kann ein für die Verarbeitung Verantwortlicher "*eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle*" sein. Das bedeutet, dass es im Prinzip keine Einschränkung hinsichtlich der Art der Einrichtung gibt, die die Rolle des für die Verarbeitung Verantwortlichen übernehmen kann. Es kann sich um eine Organisation handeln, aber auch um eine Einzelperson oder eine Gruppe von Einzelpersonen. [8] In der Praxis ist es jedoch in der Regel die Organisation als solche und nicht eine Einzelperson innerhalb der Organisation (z. B. der CEO, ein Mitarbeiter oder ein Vorstandsmitglied), die als Verantwortlicher im Sinne der DSGVO handelt. Soweit es um die Datenverarbeitung innerhalb einer Unternehmensgruppe geht, muss besonders auf die Frage geachtet werden, ob eine Niederlassung als Verantwortlicher oder als Auftragsverarbeiter handeln kann, 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 ernannt wird, um die Einhaltung der Datenschutzvorschriften zu gewährleisten, ist diese Person nicht der für die Verarbeitung Verantwortliche, sondern handelt im Namen der juristischen Person (Unternehmen oder öffentliche Einrichtung), die im Falle eines Verstoßes gegen die Vorschriften letztlich in ihrer Eigenschaft als für die Verarbeitung Verantwortlicher verantwortlich ist. Auch wenn eine bestimmte Abteilung oder Einheit einer

Organisation die operative Verantwortung für die Sicherstellung der Einhaltung bestimmter Verarbeitungstätigkeiten trägt, bedeutet dies nicht, dass diese Abteilung oder Einheit (und nicht die Organisation als Ganzes) zum für die Verarbeitung Verantwortlichen wird.

Beispiel:

Die Marketingabteilung von Unternehmen ABC startet eine Werbekampagne, um die Produkte von ABC zu bewerben. Die Marketingabteilung entscheidet über die Art der Kampagne, die zu verwendenden Mittel (E-Mail, soziale Medien ...), die anzusprechenden Kunden und die zu verwendenden Daten, um die Kampagne so erfolgreich wie möglich zu gestalten. Selbst wenn die Marketingabteilung mit erheblicher Unabhängigkeit handelte, wird Unternehmen ABC im Prinzip als der für die Verarbeitung Verantwortliche betrachtet, da die Werbekampagne vom Unternehmen gestartet wird und im Rahmen seiner Geschäftstätigkeit und für seine Zwecke stattfindet.

19. Grundsätzlich kann davon ausgegangen werden, dass jede Verarbeitung personenbezogener Daten durch Mitarbeiter, die im Rahmen der Aktivitäten einer Organisation stattfindet, unter der Kontrolle dieser Organisation erfolgt. [9] In Ausnahmefällen kann es jedoch vorkommen, dass ein Mitarbeiter beschließt, personenbezogene Daten für seine eigenen Zwecke zu verwenden und damit die ihm erteilte Befugnis unrechtmäßig überschreitet. (z. B. um seine eigene Firma zu gründen oder ähnliches). Es ist daher die Pflicht der Organisation als Controller, sicherzustellen, dass es angemessene technische und organisatorische Maßnahmen gibt, einschließlich z. B. Schulungen und Informationen für Mitarbeiter, um die Einhaltung der DSGVO zu gewährleisten. [10]

2.1.2 "Bestimmt"

20. Der zweite Baustein des Konzepts des für die Verarbeitung Verantwortlichen bezieht sich auf den *Einfluss* des für die Verarbeitung Verantwortlichen auf die Verarbeitung durch die *Ausübung von Entscheidungsbefugnissen*. Ein für die Verarbeitung Verantwortlicher ist eine Stelle, die über bestimmte Schlüsselelemente der Verarbeitung entscheidet. Diese Kontrollbefugnis kann gesetzlich definiert sein oder sich aus einer Analyse der faktischen Elemente oder Umstände des Falles ergeben. Man sollte sich die konkreten Verarbeitungsvorgänge ansehen und verstehen, wer sie bestimmt, indem man zunächst die folgenden Fragen betrachtet: "*Warum findet diese Verarbeitung statt*?" und "*Wer hat entschieden, dass die Verarbeitung zu einem bestimmten Zweck erfolgen soll?*".

Umstände, die zu einer Kontrolle führen

21. Da der Begriff des Controllers ein funktionales Konzept ist, basiert er eher auf einer **sachlichen als auf einer formalen Analyse**. Zur Erleichterung der Analyse können bestimmte Faustregeln und praktische Vermutungen herangezogen werden, um den Prozess zu lenken und zu vereinfachen. In den meisten Situationen kann das "bestimmende Organ" leicht und eindeutig durch Bezugnahme auf bestimmte rechtliche und/oder tatsächliche Umstände identifiziert werden, aus denen normalerweise auf einen "Einfluss" geschlossen werden kann, sofern nicht andere Elemente auf das Gegenteil hindeuten. Es können zwei Kategorien von Situationen unterschieden werden: (1) Kontrolle, die sich aus *gesetzlichen Bestimmungen* ergibt, und (2) Kontrolle, die sich aus *faktischer Einflussnahme* ergibt.

1) Steuerung aufgrund gesetzlicher Vorschriften

22. Es gibt Fälle, in denen die Kontrolle aus der ausdrücklichen rechtlichen Zuständigkeit abgeleitet werden kann, z. B. wenn der für die Verarbeitung Verantwortliche oder die spezifischen Kriterien für seine Benennung durch einzelstaatliches oder Unionsrecht festgelegt sind. In der Tat heißt es in Artikel 4 Absatz 7: "Werden die *Zwecke und Mittel einer solchen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten bestimmt, so können der für die Verarbeitung Verantwortliche oder die spezifischen Kriterien für seine Benennung durch das Recht der Union oder der Mitgliedstaaten vorgesehen werden.* " Während in Artikel 4 Absatz 7 nur im Singular von "dem für die Verarbeitung Verantwortlichen" die Rede ist, ist der EDSB der Ansicht, dass das Unionsrecht oder das Recht der Mitgliedstaaten auch mehr als einen für die Verarbeitung Verantwortlichen benennen kann,

möglicherweise sogar als gemeinsam für die Verarbeitung Verantwortlichen.

23. Wenn der für die Verarbeitung Verantwortliche durch das Gesetz ausdrücklich bestimmt wurde, ist dies ausschlaggebend für die Feststellung, wer als für die Verarbeitung Verantwortlicher handelt. Dies setzt voraus, dass der Gesetzgeber diejenige Stelle als für die Verarbeitung Verantwortlicher bestimmt hat, die tatsächlich in der Lage ist, Kontrolle auszuüben. In einigen Ländern sieht das nationale Recht vor, dass öffentliche Stellen im Rahmen ihrer Aufgaben für die Verarbeitung personenbezogener Daten verantwortlich sind.

24. Häufiger ist es jedoch so, dass das Gesetz, anstatt den für die Verarbeitung Verantwortlichen direkt zu benennen oder die Kriterien für seine Benennung festzulegen, eine Aufgabe festlegt oder jemandem die Pflicht auferlegt, bestimmte Daten zu sammeln und zu verarbeiten. In diesen Fällen wird der Zweck der Verarbeitung oft durch das Gesetz bestimmt. Der für die Verarbeitung Verantwortliche wird normalerweise derjenige sein, der durch das Gesetz für die Realisierung dieses Zwecks, dieser öffentlichen Aufgabe, bestimmt wurde. Dies wäre beispielsweise der Fall, wenn eine Einrichtung, die mit bestimmten öffentlichen Aufgaben (z. B. Sozialversicherung) betraut ist, die ohne die Erhebung zumindest einiger personenbezogener Daten nicht erfüllt werden können, eine Datenbank oder ein Register einrichtet, um diese öffentlichen Aufgaben zu erfüllen. In diesem Fall legt das Gesetz, wenn auch indirekt, fest, wer der für die Verarbeitung Verantwortliche ist. Ganz allgemein kann das Gesetz auch öffentlichen oder privaten Stellen die Verpflichtung auferlegen, bestimmte Daten aufzubewahren oder bereitzustellen. Diese Stellen würden dann normalerweise als für die Verarbeitung Verantwortliche in Bezug auf die Verarbeitung, die zur Erfüllung dieser Verpflichtung erforderlich ist, betrachtet werden.

Beispiel: Gesetzliche Bestimmungen

Das nationale Gesetz in Land A sieht eine Verpflichtung der kommunalen Behörden vor, Sozialleistungen wie monatliche Zahlungen an Bürger je nach deren finanzieller Situation zu leisten. Um diese Zahlungen durchführen zu können, muss die Gemeindebehörde Daten über die finanziellen Verhältnisse der Antragsteller sammeln und verarbeiten. Auch wenn das Gesetz nicht ausdrücklich festlegt, dass die Gemeindebehörden für diese Verarbeitung verantwortlich sind, ergibt sich dies implizit aus den gesetzlichen Bestimmungen.

2) Steuerung durch faktische Beeinflussung

25. In Ermangelung einer sich aus gesetzlichen Bestimmungen ergebenden Kontrolle muss die Qualifikation einer Partei als Verantwortlicher auf der Grundlage einer Bewertung der tatsächlichen Umstände der Verarbeitung festgestellt werden. Alle relevanten faktischen Umstände müssen berücksichtigt werden, um zu einer Schlussfolgerung zu gelangen, ob eine bestimmte Stelle einen bestimmenden Einfluss auf die Verarbeitung der betreffenden personenbezogenen Daten ausübt.

26. Die Notwendigkeit einer faktischen Beurteilung bedeutet auch, dass sich die Rolle eines für die Verarbeitung Verantwortlichen nicht aus der Natur einer Stelle ergibt, die Daten verarbeitet, sondern aus ihren konkreten Tätigkeiten in einem bestimmten Kontext. Mit anderen Worten, dieselbe Stelle kann gleichzeitig als für die Verarbeitung Verantwortlicher für bestimmte Verarbeitungsvorgänge und als Auftragsverarbeiter für andere handeln, und die Qualifikation als für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter muss im Hinblick auf jede spezifische Datenverarbeitungstätigkeit beurteilt werden.

27. In der Praxis können bestimmte Verarbeitungstätigkeiten als natürlich mit der Rolle oder den Tätigkeiten eines Unternehmens verbunden angesehen werden, die letztlich Verantwortlichkeiten aus Sicht des Datenschutzes nach sich ziehen. Dies kann auf allgemeinere gesetzliche Bestimmungen oder eine etablierte Rechtspraxis in verschiedenen Bereichen (Zivilrecht, Handelsrecht, Arbeitsrecht usw.) zurückzuführen sein. In diesem Fall helfen bestehende traditionelle Rollen und berufliches Fachwissen, die normalerweise eine bestimmte Verantwortung implizieren, bei der Identifizierung des für die Verarbeitung Verantwortlichen, z. B.: ein Arbeitgeber in Bezug auf die Verarbeitung personenbezogener Daten seiner Mitarbeiter, ein Verlag, der personenbezogene Daten über seine Abonnenten verarbeitet, oder ein Verein, der personenbezogene Daten über seine Mitglieder oder Beitragszahler verarbeitet. Wenn ein Unternehmen personenbezogene Daten im Rahmen der Interaktion mit seinen eigenen Mitarbeitern, Kunden oder Mitgliedern verarbeitet, ist es in der

Regel derjenige, der den Zweck und die Mittel im Zusammenhang mit der Verarbeitung bestimmt und daher als für die Verarbeitung Verantwortlicher im Sinne der DSGVO handelt.

Beispiel: Anwaltskanzleien

Die Firma ABC beauftragt eine Anwaltskanzlei, sie in einem Rechtsstreit zu vertreten. Um diese Aufgabe zu erfüllen, muss die Anwaltskanzlei personenbezogene Daten im Zusammenhang mit dem Fall verarbeiten. Der Grund für die Verarbeitung der personenbezogenen Daten ist das Mandat der Anwaltskanzlei, den Mandanten vor Gericht zu vertreten. Dieses Mandat ist jedoch nicht speziell auf die Verarbeitung personenbezogener Daten ausgerichtet. Die Anwaltskanzlei handelt mit einem erheblichen Maß an Unabhängigkeit, z. B. bei der Entscheidung, welche Informationen verwendet werden und wie sie verwendet werden, und es gibt keine Anweisungen des Kundenunternehmens hinsichtlich der Verarbeitung personenbezogener Daten. Die Verarbeitung, die die Anwaltskanzlei durchführt, um die Aufgabe als rechtlicher Vertreter des Unternehmens zu erfüllen, ist daher mit der funktionalen Rolle der Anwaltskanzlei verbunden, so dass sie für diese Verarbeitung als Verantwortlicher zu betrachten ist.

Beispiel: Telekommunikationsbetreiber:

Die Bereitstellung eines elektronischen Kommunikationsdienstes wie z. B. eines E-Mail-Dienstes beinhaltet die Verarbeitung personenbezogener Daten. Der Anbieter solcher Dienste wird in der Regel als Verantwortlicher in Bezug auf die Verarbeitung personenbezogener Daten betrachtet, die für den Betrieb des Dienstes als solchen erforderlich sind (z. B. Verkehrs- und Abrechnungsdaten). Wenn der einzige Zweck und die einzige Rolle des Anbieters darin besteht, die Übertragung von E-Mail-Nachrichten zu ermöglichen, wird der Anbieter nicht als Verantwortlicher in Bezug auf die in der Nachricht selbst enthaltenen personenbezogenen Daten angesehen. Als für die Verarbeitung Verantwortlicher in Bezug auf die in der Nachricht enthaltenen personenbezogenen Daten wird in der Regel die Person betrachtet, von der die Nachricht stammt, und nicht der Dienstanbieter, der den Übertragungsdienst anbietet.

28. In vielen Fällen kann eine Bewertung der Vertragsbedingungen zwischen den verschiedenen beteiligten Parteien die Feststellung erleichtern, welche Partei (oder Parteien) als für die Verarbeitung Verantwortlicher handelt. Selbst wenn ein Vertrag keine Angaben darüber enthält, wer der für die Verarbeitung Verantwortliche ist, kann er genügend Elemente enthalten, um daraus zu schließen, wer eine Entscheidungsfunktion in Bezug auf die Zwecke und Mittel der Verarbeitung ausübt. Es kann auch sein, dass der Vertrag eine ausdrückliche Erklärung über die Identität des für die Verarbeitung Verantwortlichen enthält. Wenn es keinen Grund gibt, daran zu zweifeln, dass dies die Realität genau widerspiegelt, spricht nichts dagegen, die Vertragsbedingungen zu befolgen. Allerdings sind die Vertragsbedingungen nicht unter allen Umständen entscheidend, da dies den Parteien lediglich erlauben würde, die Verantwortung nach eigenem Gutdünken zuzuweisen. Es ist weder möglich, Kontrolleur zu werden, noch sich den Kontrollpflichten zu entziehen, indem man den Vertrag in einer bestimmten Weise gestaltet, wenn die tatsächlichen Umstände etwas anderes besagen.

29. Wenn eine Partei tatsächlich entscheidet, warum und wie personenbezogene Daten verarbeitet werden, ist diese Partei ein für die Verarbeitung Verantwortlicher, auch wenn in einem Vertrag steht, dass sie ein Auftragsverarbeiter ist. Ebenso gilt ein Unternehmen aus datenschutzrechtlicher Sicht nicht deshalb als Auftragsverarbeiter, weil in einem Handelsvertrag der Begriff "Unterauftragnehmer" verwendet wird. [12]

30. Im Einklang mit dem faktischen Ansatz bedeutet das Wort "bestimmt", dass die Stelle, die tatsächlich einen entscheidenden Einfluss auf die Zwecke und Mittel der Verarbeitung ausübt, der Verantwortliche ist. Normalerweise wird in einem Auftragsverarbeitungsvertrag festgelegt, wer die bestimmende Partei (Verantwortlicher) und die beauftragte Partei (Auftragsverarbeiter) ist. Auch wenn der Auftragsverarbeiter einen Dienst anbietet, der vorab in einer bestimmten Art und Weise definiert wird, muss dem Verantwortlichen eine detaillierte Beschreibung des Dienstes vorgelegt werden und er muss die endgültige Entscheidung treffen, die Art und Weise der Verarbeitung aktiv zu genehmigen und gegebenenfalls Änderungen zu verlangen. Außerdem kann der Auftragsverarbeiter zu einem späteren Zeitpunkt die wesentlichen Elemente der Verarbeitung nicht ohne die Zustimmung des für die Verarbeitung Verantwortlichen ändern.

Beispiel: standardisierter Cloud-Speicherdienst

Ein großer Cloud-Speicheranbieter bietet seinen Kunden die Möglichkeit, große Mengen an persönlichen Daten zu speichern. Der Dienst ist vollständig standardisiert, wobei die Kunden wenig oder keine Möglichkeit haben, den Dienst anzupassen. Die Vertragsbedingungen werden einseitig vom Cloud-Anbieter festgelegt und ausgearbeitet und dem Kunden auf einer "take it or leave it"-Basis zur Verfügung gestellt. Unternehmen X beschließt, den Cloud-Anbieter zu nutzen, um personenbezogene Daten seiner Kunden zu speichern. Unternehmen X wird immer noch als für die Verarbeitung Verantwortlicher betrachtet, da es beschlossen hat, diesen speziellen Cloud-Service-Anbieter zu nutzen, um personenbezogene Daten für seine Zwecke zu verarbeiten. Sofern der Cloud-Dienstanbieter die personenbezogenen Daten nicht für seine eigenen Zwecke verarbeitet und die Daten ausschließlich im Auftrag seiner Kunden und gemäß den Anweisungen speichert, wird der Dienstanbieter als Auftragsverarbeiter betrachtet.

[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, WP128, S. 11.

2.1.3 "Alleine oder gemeinsam mit anderen"

31. Artikel 4 Absatz 7 erkennt an, dass die "Zwecke und Mittel" der Verarbeitung von mehr als einem Akteur bestimmt werden können. Er besagt, dass der für die Verarbeitung Verantwortliche der Akteur ist, der "allein oder gemeinsam mit anderen" die Zwecke und Mittel der Verarbeitung bestimmt. Das bedeutet, dass mehrere verschiedene Stellen als Verantwortliche für dieselbe Verarbeitung fungieren können, wobei jede von ihnen dann den geltenden Datenschutzbestimmungen unterliegt. Dementsprechend kann eine Organisation auch dann ein für die Verarbeitung Verantwortlicher sein, wenn sie nicht alle Entscheidungen über die Zwecke und Mittel trifft. Die Kriterien für die gemeinsame Verantwortlichkeit und das Ausmaß, in dem zwei oder mehr Akteure gemeinsam die Kontrolle ausüben, können unterschiedliche Formen annehmen, wie später noch erläutert wird. [13]

2.1.4 "Zwecke und Mittel"

32. Der vierte Baustein der Controller-Definition bezieht sich auf den Gegenstand des Einflusses des Controllers, nämlich die "Zwecke und Mittel" der Verarbeitung. Er stellt den materiellen Teil des Controller-Konzepts dar: was eine Partei bestimmen sollte, um als Controller zu gelten.

33. Wörterbücher definieren "Zweck" als "ein erwartetes Ergebnis, das beabsichtigt ist oder das Ihre geplanten Handlungen leitet" und "Mittel" als "wie ein Ergebnis erzielt wird oder ein Zweck erreicht wird".

34. Die DSGVO legt fest, dass Daten für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden dürfen. Die Bestimmung der "Zwecke" der Verarbeitung und der "Mittel" zur Erreichung dieser Zwecke ist daher besonders wichtig.

35. Die Festlegung der Zwecke und Mittel ist gleichbedeutend mit der Entscheidung über das "Warum" und das "Wie" der Verarbeitung:[14] Bei einer bestimmten Verarbeitung ist der für die Verarbeitung Verantwortliche der Akteur, der festgelegt hat, *warum* die Verarbeitung stattfindet (d. h. "zu welchem Zweck" oder "wozu") und *wie* dieses Ziel erreicht werden soll (d. h. welche Mittel zur Erreichung des Ziels eingesetzt werden sollen). Eine natürliche oder juristische Person, die einen solchen Einfluss auf die Verarbeitung personenbezogener Daten ausübt, wirkt damit an der Festlegung der Zwecke und Mittel dieser Verarbeitung gemäß der Definition in Artikel 4 Absatz 7 DSGVO mit. [15]

36. Der für die Verarbeitung Verantwortliche muss sowohl über den Zweck als auch über die Mittel der Verarbeitung entscheiden, wie unten beschrieben. Folglich kann sich der Verantwortliche nicht nur mit der Festlegung des Zwecks begnügen. Er muss auch Entscheidungen über die Mittel der Verarbeitung treffen. Umgekehrt kann die Partei, die als Auftragsverarbeiter handelt, niemals den Zweck der Verarbeitung bestimmen.

37. Wenn ein für die Verarbeitung Verantwortlicher einen Auftragsverarbeiter mit der Durchführung der Verarbeitung in seinem Namen beauftragt, bedeutet dies in der Praxis häufig, dass der Auftragsverarbeiter in der Lage sein muss, bestimmte eigene Entscheidungen darüber zu treffen, wie die Verarbeitung durchgeführt werden soll. Der EDPB erkennt an, dass ein gewisser Handlungsspielraum für den Auftragsverarbeiter bestehen kann, um auch einige Entscheidungen in Bezug auf die Verarbeitung treffen zu können. Unter diesem Gesichtspunkt ist es notwendig, eine Anleitung zu geben, welches **Maß an Einfluss** auf das "Warum" und das "Wie" die Einstufung eines Unternehmens als für die Verarbeitung Verantwortlicher nach sich ziehen sollte und in welchem Umfang ein Auftragsverarbeiter eigene Entscheidungen treffen kann.

38. Wenn eine Stelle Zwecke und Mittel eindeutig festlegt und eine andere Stelle mit Verarbeitungstätigkeiten betraut, die auf die Ausführung ihrer detaillierten Anweisungen hinauslaufen, ist die Situation eindeutig, und es besteht kein Zweifel daran, dass die zweite Stelle als Auftragsverarbeiter zu betrachten ist, während die erste Stelle der Verantwortliche ist.

Wesentliche vs. nicht-wesentliche Mittel

39. Die Frage ist, wo die Grenze zu ziehen ist zwischen Entscheidungen, die dem für die Verarbeitung Verantwortlichen vorbehalten sind, und Entscheidungen, die in das Ermessen des Auftragsverarbeiters gestellt werden können. Entscheidungen über den Zweck der Verarbeitung sind eindeutig immer dem für die Verarbeitung Verantwortlichen vorbehalten.

40. Bei der Bestimmung der Mittel kann zwischen wesentlichen und unwesentlichen Mitteln unterschieden werden. "Wesentliche Mittel" sind traditionell und naturgemäß dem Controller vorbehalten. Während nicht wesentliche Mittel auch durch den Prozessor bestimmt werden können, sind wesentliche Mittel durch den Controller zu bestimmen. "Wesentliche Mittel" sind Mittel, die in engem Zusammenhang mit dem Zweck und dem Umfang der Verarbeitung stehen, wie z. B. die Art der personenbezogenen Daten, die verarbeitet werden ("*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 von betroffenen Personen ("*Wessen personenbezogene Daten werden verarbeitet?*"). Zusammen mit dem Zweck der Verarbeitung sind die wesentlichen Mittel auch eng mit der Frage verbunden, ob die Verarbeitung rechtmäßig, erforderlich und verhältnismäßig ist. "Nicht wesentliche Mittel" betreffen eher praktische Aspekte der Umsetzung, wie z. B. die Entscheidung für eine bestimmte Art von Hard- oder Software oder die detaillierten Sicherheitsmaßnahmen, die dem Auftragsverarbeiter überlassen werden können.

Beispiel: Verwaltung der Gehaltsabrechnung

Arbeitgeber A beauftragt ein anderes Unternehmen mit der Verwaltung der Gehaltszahlungen an seine Mitarbeiter. Arbeitgeber A gibt klare Anweisungen, an wen, welche Beträge, bis zu welchem Datum, von welcher Bank, wie lange die Daten gespeichert werden sollen, welche Daten an die Steuerbehörde weitergegeben werden sollen usw. In diesem Fall erfolgt die Verarbeitung der Daten für den Zweck von Unternehmen A, die Gehälter an seine Mitarbeiter zu zahlen, und der Gehaltsabrechnungsverwalter darf die Daten nicht für irgendwelche eigenen Zwecke verwenden. Die Art und Weise, in der der Lohnbuchhalter die Verarbeitung durchführen soll, ist im Wesentlichen klar und eng definiert. Dennoch kann der Lohnbuchhalter über bestimmte Detailfragen im Zusammenhang mit der Verarbeitung entscheiden, z. B. welche Software er verwendet, wie er den Zugriff innerhalb seiner eigenen Organisation verteilt usw. Dies ändert nichts an seiner Rolle als Auftragsverarbeiter, solange der Administrator nicht gegen die von Unternehmen A erteilten Anweisungen verstößt oder darüber hinausgeht.

Beispiel: Bankzahlungen

Im Rahmen der Anweisungen von Arbeitgeber A übermittelt die Lohnbuchhaltung Informationen an Bank B, damit diese die tatsächliche Auszahlung an die Mitarbeiter von Arbeitgeber A vornehmen kann. Diese Tätigkeit beinhaltet die Verarbeitung personenbezogener Daten durch Bank B, die sie zum Zweck der Durchführung der 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 keinen Einfluss auf den Zweck und die Art und Weise der Datenverarbeitung durch Bank B nehmen. Bank B ist daher als Verantwortlicher für diese Verarbeitung zu sehen und die Übermittlung von personenbezogenen Daten aus der Lohnbuchhaltung ist als eine Weitergabe von Informationen zwischen zwei Verantwortlichen, von Arbeitgeber A an Bank B, zu betrachten.

Beispiel: Buchhalter

Arbeitgeber A beauftragt auch die Wirtschaftsprüfungsgesellschaft C mit der Prüfung seiner Buchhaltung und übermittelt daher Daten über Finanztransaktionen (einschließlich personenbezogener Daten) an C. Die Wirtschaftsprüfungsgesellschaft C verarbeitet diese Daten ohne detaillierte Anweisungen von A. Die Wirtschaftsprüfungsgesellschaft C entscheidet selbst in

nur zum Zweck der Prüfung von A verarbeitet werden und sie bestimmt, welche Daten sie benötigt, welche Personenkategorien erfasst werden müssen, wie lange die Daten aufzubewahren sind und welche technischen Mittel zu verwenden sind. Unter diesen Umständen ist die Wirtschaftsprüfungsgesellschaft C als eigener für die Verarbeitung Verantwortlicher zu betrachten, wenn sie ihre Prüfungsdienste für A erbringt. Diese Beurteilung kann jedoch je nach dem Grad der Weisungen von A unterschiedlich ausfallen. In einer Situation, in der das Gesetz keine spezifischen Verpflichtungen für die Wirtschaftsprüfungsgesellschaft vorsieht und das Kundenunternehmen sehr detaillierte Anweisungen für die Verarbeitung erteilt, würde die Wirtschaftsprüfungsgesellschaft tatsächlich als Auftragsverarbeiter handeln. Es könnte unterschieden werden zwischen einer Situation, in der die Verarbeitung - in Übereinstimmung mit den Gesetzen, die diesen Beruf regeln - als Teil der Kerntätigkeit der Wirtschaftsprüfungsgesellschaft erfolgt, und einer Situation, in der die Verarbeitung eine begrenztere, untergeordnete Aufgabe ist, die als Teil der Tätigkeit des Kundenunternehmens durchgeführt wird.

Beispiel: Hosting-Dienste

Arbeitgeber A beauftragt den Hosting-Dienst H mit der Speicherung verschlüsselter Daten auf den Servern von H. Der Hosting-Dienst H bestimmt weder, ob es sich bei den von ihm gehosteten Daten um personenbezogene Daten handelt, noch verarbeitet er die Daten auf eine andere Weise als durch Speicherung auf seinen Servern. Da die Speicherung ein Beispiel für eine Aktivität zur Verarbeitung personenbezogener Daten ist, verarbeitet der Hosting-Dienst H personenbezogene Daten im Auftrag von Arbeitgeber A und ist daher ein Auftragsverarbeiter. Arbeitgeber A muss H die erforderlichen Weisungen erteilen und einen Datenverarbeitungsvertrag nach Artikel 28 abschließen, der H zur Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen verpflichtet. H muss A dabei unterstützen, 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 für die Verarbeitung Verantwortliche dennoch bestimmte Elemente in der Auftragsverarbeitungsvereinbarung festlegen, wie - in Bezug auf die Sicherheitsanforderung - z. B. eine Anweisung, alle gemäß Artikel 32 der DSGVO erforderlichen Maßnahmen zu ergreifen. Die Vereinbarung muss auch festlegen, dass der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung von z. B. Artikel 32 unterstützt. In jedem Fall bleibt der für die Verarbeitung Verantwortliche für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen verantwortlich, um sicherzustellen und nachweisen zu können, 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. Aus diesem Grund muss der für die Verarbeitung Verantwortliche umfassend über die eingesetzten Mittel informiert werden, damit er diesbezüglich eine fundierte Entscheidung treffen kann. Damit der für die Verarbeitung Verantwortliche die Rechtmäßigkeit der Verarbeitung nachweisen kann, ist es ratsam, zumindest die erforderlichen technischen und organisatorischen Maßnahmen in dem Vertrag oder einem anderen rechtsverbindlichen Instrument zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter zu dokumentieren.

Beispiel: Call-Center

Unternehmen X beschließt, einen Teil seiner Kundendienstbeziehungen an ein Callcenter auszulagern. Das Callcenter erhält identifizierbare Daten über Kundenkäufe sowie Kontaktinformationen. Das Callcenter verwendet seine eigene Software und IT-Infrastruktur, um die personenbezogenen Daten über die Kunden von Unternehmen X zu verwalten. Unternehmen X schließt mit dem Anbieter des Callcenters einen Auftragsverarbeitungsvertrag gemäß Artikel 28 DSGVO ab, nachdem es sich vergewissert hat, dass die vom Callcenter vorgeschlagenen technischen und organisatorischen Sicherheitsmaßnahmen den betreffenden Risiken angemessen sind und dass das Callcenter die personenbezogenen Daten nur für die Zwecke von Unternehmen X und in Übereinstimmung mit dessen Anweisungen verarbeitet. Unternehmen X erteilt dem Callcenter keine weiteren Anweisungen bezüglich der zu verwendenden Software oder detaillierte Anweisungen bezüglich der zu implementierenden spezifischen Sicherheitsmaßnahmen. In diesem Beispiel bleibt Unternehmen X ein für die Verarbeitung Verantwortlicher, trotz der Tatsache, dass das Callcenter bestimmte nicht wesentliche Mittel der Verarbeitung bestimmt hat.

2.1.5 "Von der Verarbeitung personenbezogener Daten"

42. Die von dem für die Verarbeitung Verantwortlichen festgelegten Zwecke und Mittel müssen sich auf die "Verarbeitung personenbezogener Daten" beziehen. Artikel 4(2) GDPR definiert die Verarbeitung personenbezogener Daten als "*jeden Vorgang oder jede Vorgangsreihe, die mit personenbezogenen Daten oder mit einer Reihe personenbezogener Daten durchgeführt wird*". Infolgedessen kann der Begriff des für die Verarbeitung Verantwortlichen entweder mit einem einzelnen Verarbeitungsvorgang oder mit einer Reihe von Vorgängen verknüpft werden. In der Praxis kann dies bedeuten, dass sich die von einer bestimmten Stelle ausgeübte Kontrolle auf die Gesamtheit der fraglichen Verarbeitung erstrecken kann, aber auch auf eine bestimmte Phase der Verarbeitung beschränkt sein 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 einzeln bestimmt. Andererseits kann eine Abfolge oder eine Reihe von Verarbeitungsvorgängen, an denen mehrere Akteure beteiligt sind, auch für denselben Zweck bzw. dieselben Zwecke erfolgen; in diesem Fall ist es möglich, dass an der Verarbeitung ein oder mehrere gemeinsam für die Verarbeitung Verantwortliche beteiligt sind. Mit anderen Worten, es ist möglich, dass auf "Mikroebene" die verschiedenen Verarbeitungsvorgänge der Kette als unverbunden erscheinen, da jeder von ihnen einen anderen Zweck haben kann. Es ist jedoch zu prüfen, ob diese Verarbeitungsvorgänge auf der "Makroebene" nicht als eine "Menge von Vorgängen" betrachtet werden sollten, die einen gemeinsamen Zweck mit gemeinsam definierten Mitteln verfolgen.

44. Jeder, der beschließt, Daten zu verarbeiten, muss sich überlegen, ob dies personenbezogene Daten einschließt und, wenn ja, welche Verpflichtungen sich daraus nach der DSGVO ergeben. Ein Akteur wird auch dann als "für die Verarbeitung Verantwortlicher" betrachtet, wenn er nicht bewusst auf personenbezogene Daten als solche abzielt oder fälschlicherweise eingeschätzt hat, dass er keine personenbezogenen Daten verarbeitet.

45. Es ist nicht erforderlich, dass der Verantwortliche tatsächlich Zugang zu den Daten hat, die verarbeitet werden. [17] Jemand, der eine Verarbeitungstätigkeit auslagert und dabei einen bestimmenden Einfluss auf den Zweck und die (wesentlichen) Mittel der Verarbeitung hat (z. B. indem er Parameter eines Dienstes so einstellt, dass er Einfluss darauf hat, wessen personenbezogene Daten verarbeitet werden sollen), ist als für die Verarbeitung Verantwortlicher zu betrachten, auch wenn er nie tatsächlichen Zugang zu den Daten hat.

Beispiel: Marktforschung 1

Unternehmen ABC möchte verstehen, welche Arten von Verbrauchern sich am ehesten für seine Produkte interessieren und beauftragt einen Dienstleister, XYZ, mit der Beschaffung der entsprechenden Informationen.

Unternehmen ABC weist XYZ an, an welcher Art von Informationen es interessiert ist und stellt eine Liste von Fragen zur Verfügung, die den Teilnehmern der Marktforschung gestellt werden sollen.

Unternehmen ABC erhält von XYZ nur statistische Informationen (z. B. zur Identifizierung von Verbrauchertrends pro Region) und hat keinen Zugriff auf die personenbezogenen Daten selbst. Dennoch hat Unternehmen ABC entschieden, dass die Verarbeitung stattfinden soll, die Verarbeitung erfolgt für seinen Zweck und seine Tätigkeit und es hat XYZ detaillierte Anweisungen gegeben, welche Informationen zu sammeln sind. Unternehmen ABC ist daher in Bezug auf die Verarbeitung personenbezogener Daten, die stattfindet, um die von ihm angeforderten Informationen zu liefern, immer noch als für die Verarbeitung Verantwortlicher zu betrachten. XYZ darf die Daten nur zu dem von Unternehmen ABC angegebenen Zweck und nach dessen detaillierten Anweisungen verarbeiten und ist daher als Auftragsverarbeiter zu betrachten.

[16] Urteil *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, Rn. 74: "*Wie der Generalanwalt festgestellt hat, [...-] kann eine natürliche oder juristische Person nur in Bezug auf Vorgänge, die eine Verarbeitung personenbezogener Daten beinhalten, deren Zwecke und Mittel sie gemeinsam festlegt, gemeinsam mit anderen für die Verarbeitung Verantwortlicher im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 sein. Dagegen [...] kann diese natürliche oder juristische Person nicht als für die Verarbeitung Verantwortlicher im Sinne dieser Bestimmung im Zusammenhang mit Vorgängen angesehen werden, die in der gesamten Verarbeitungskette vorausgehen oder nachfolgen und für die diese Person weder die Zwecke noch die Mittel bestimmt".*

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

Beispiel: Marktforschung 2

Unternehmen ABC möchte verstehen, welche Arten von Verbrauchern am ehesten an seinen Produkten interessiert sind. Dienstleister XYZ ist ein Marktforschungsunternehmen, das Informationen über Verbraucherinteressen durch eine Vielzahl von Fragebögen gesammelt hat, die sich auf eine große Vielfalt von Produkten und Dienstleistungen beziehen. Dienstleister XYZ hat diese Daten unabhängig und nach seiner eigenen Methodik gesammelt und analysiert, ohne irgendwelche Anweisungen von Unternehmen ABC zu erhalten. Um die Anfrage von Unternehmen ABC zu beantworten, erstellt Dienstleister XYZ statistische Informationen, tut dies jedoch, ohne weitere Anweisungen darüber zu erhalten, welche personenbezogenen Daten verarbeitet werden sollen oder wie sie zu verarbeiten sind, um diese Statistiken zu erstellen. In diesem Beispiel handelt Dienstleister XYZ als alleiniger Verantwortlicher, der personenbezogene Daten zu Marktforschungszwecken verarbeitet und die Mittel dafür autonom bestimmt. Unternehmen ABC hat keine besondere Rolle oder Verantwortung nach dem Datenschutzrecht in Bezug auf diese Verarbeitungstätigkeiten, da Unternehmen ABC anonymisierte Statistiken erhält und nicht an der Bestimmung der Zwecke und Mittel der Verarbeitung beteiligt ist.

3 DEFINITION VON GEMEINSAMEN STEUERUNGEN

3.1 Definition von gemeinsamen Reglern

46. Die Qualifikation als gemeinsam für die Verarbeitung Verantwortlicher kann sich ergeben, wenn mehr als ein Akteur an der Verarbeitung beteiligt ist.

47. Während das Konzept nicht neu ist und bereits unter der Richtlinie 95/46/EG existierte, führt die Datenschutz-Grundverordnung in ihrem Artikel 26 spezifische Regeln für gemeinsam für die Verarbeitung Verantwortliche ein und legt einen Rahmen fest, der ihre Beziehung regelt. Darüber hinaus hat der Gerichtshof der Europäischen Union (EuGH) in jüngsten Urteilen Klarstellungen zu diesem Konzept und seinen Auswirkungen vorgenommen. [18]

48. Wie in Teil II, Abschnitt 2 näher ausgeführt, wird die Einstufung der gemeinsam für die Verarbeitung Verantwortlichen vor allem Auswirkungen auf die Verteilung der Pflichten zur Einhaltung der Datenschutzvorschriften und insbesondere auf die Rechte natürlicher Personen haben.

49. Vor diesem Hintergrund soll der folgende Abschnitt eine Anleitung zum Konzept der gemeinsam für die Verarbeitung Verantwortlichen in Übereinstimmung mit der DSGVO und der Rechtsprechung des EuGH bieten, um Unternehmen dabei zu helfen, festzustellen, wo sie möglicherweise als gemeinsam für die Verarbeitung Verantwortliche handeln und das Konzept in der Praxis anwenden.

3.2 Vorhandensein einer gemeinsamen Beherrschung

3.2.1 Allgemeine Überlegungen

50. Die Definition eines für die Verarbeitung Verantwortlichen in Artikel 4 (7) DSGVO bildet den Ausgangspunkt für die Bestimmung der gemeinsamen Kontrollbefugnis. Die Überlegungen in diesem Abschnitt stehen somit in direktem Zusammenhang mit und ergänzen die

[18] Siehe insbesondere, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie*, (C- 210/16), *Tietosuojavaltuutettu v Jehovan todistajat - uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG gegen Verbraucherzentrale NRW e.V. (*C-40/17). Zu beachten ist, dass diese Urteile des EuGH zwar zur Auslegung des Begriffs des gemeinsam für die Verarbeitung Verantwortlichen nach der Richtlinie 95/46/EG ergangen sind, aber im Kontext der DSGVO weiterhin gültig sind, da die Elemente, die diesen Begriff nach der DSGVO bestimmen, dieselben bleiben wie nach der Richtlinie.

Überlegungen im Abschnitt über den Begriff des für die Verarbeitung Verantwortlichen. Infolgedessen sollte die Beurteilung der gemeinsamen Kontrolle die oben entwickelte Beurteilung der "alleinigen" Kontrolle widerspiegeln.

51. Artikel 26 DSGVO, der die Definition in Artikel 4 (7) DSGVO widerspiegelt, sieht vor, dass *"[w]enn zwei oder mehr für die Verarbeitung Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung bestimmen, sind sie gemeinsam für die Verarbeitung Verantwortliche."* Im weitesten Sinne liegt eine gemeinsame Verantwortlichkeit in Bezug auf eine bestimmte Verarbeitungstätigkeit vor, wenn verschiedene Parteien *gemeinsam* den Zweck und die Mittel dieser Verarbeitungstätigkeit bestimmen. Um das Vorliegen einer gemeinsamen Verantwortlichkeit zu beurteilen, muss daher geprüft werden, ob die Bestimmung der Zwecke und Mittel, die einen für die Verarbeitung Verantwortlichen kennzeichnen, von mehr als einer Partei beschlossen werden. "Gemeinsam" ist so auszulegen, dass es "zusammen mit" oder "nicht allein" bedeutet, und zwar in verschiedenen Formen und Kombinationen, wie nachstehend erläutert.

52. Die Bewertung der gemeinsamen Kontrolle sollte auf der Grundlage einer faktischen und nicht einer formalen Analyse des tatsächlichen Einflusses auf die Zwecke und Mittel der Verarbeitung erfolgen. Alle bestehenden oder geplanten Vereinbarungen sollten anhand der faktischen Umstände der Beziehung zwischen den Parteien geprüft werden. Ein rein formales Kriterium würde aus mindestens zwei Gründen nicht ausreichen: In einigen Fällen würde die formale Ernennung eines gemeinsam für die Verarbeitung Verantwortlichen - z. B. gesetzlich oder vertraglich festgelegt - fehlen; in anderen Fällen könnte es sein, dass die formale Ernennung die Realität der Vereinbarungen nicht widerspiegelt, indem die Rolle des für die Verarbeitung Verantwortlichen formell einer Stelle übertragen wird, die tatsächlich nicht in der Lage ist, die Zwecke und Mittel der Verarbeitung zu "bestimmen".

53. Nicht jede Verarbeitung, an der mehrere Unternehmen beteiligt sind, führt zu einer gemeinsamen Kontrolle. Das übergreifende Kriterium für das Vorliegen einer gemeinsamen Kontrolle ist die **gemeinsame Beteiligung von zwei oder mehr Stellen an der Festlegung der Zwecke und Mittel** einer Verarbeitung. Genauer gesagt muss die gemeinsame Beteiligung die Bestimmung der Zwecke einerseits und die Bestimmung der Mittel andererseits umfassen. Wenn jedes dieser Elemente von allen betroffenen Stellen bestimmt wird, sollten sie als gemeinsam für die Verarbeitung Verantwortliche betrachtet werden.

3.2.2 Bewertung der gemeinsamen Teilnahme

54. Gemeinsame Beteiligung an der Festlegung der Zwecke und Mittel bedeutet, dass mehr als eine Stelle einen entscheidenden Einfluss darauf hat, ob und wie die Verarbeitung erfolgt. In der Praxis kann die gemeinsame Beteiligung mehrere verschiedene Formen annehmen. So kann die gemeinsame Beteiligung beispielsweise in Form einer **gemeinsamen Entscheidung** von zwei oder mehr Stellen erfolgen oder aus **konvergierenden Entscheidungen** von zwei oder mehr Stellen in Bezug auf die Zwecke und wesentlichen Mittel resultieren.

55. Gemeinsame Teilnahme durch eine *gemeinsame Entscheidung* bedeutet, dass eine gemeinsame Entscheidung getroffen wird und eine gemeinsame Absicht im Einklang mit dem gängigsten Verständnis des Begriffs "gemeinsam" gemäß Artikel 26 der DSGVO besteht.

Die Situation der gemeinsamen Beteiligung durch *konvergierende Entscheidungen* ergibt sich insbesondere aus der Rechtsprechung des EuGH zum Begriff des gemeinsam für die Verarbeitung Verantwortlichen. Entscheidungen können in Bezug auf Zwecke und Mittel als konvergierend angesehen werden**, wenn sie einander ergänzen und für die Verarbeitung in einer Weise erforderlich sind, dass sie sich spürbar auf die Festlegung der Zwecke und Mittel der Verarbeitung auswirken**. Es sollte hervorgehoben werden, dass der Begriff der konvergierenden Entscheidungen in Bezug auf die Zwecke und Mittel der Verarbeitung zu betrachten ist, nicht aber in Bezug auf andere Aspekte der Geschäftsbeziehung zwischen den Parteien. [19] Ein wichtiges Kriterium zur Identifizierung konvergierender Entscheidungen in diesem Zusammenhang **ist daher, ob die Verarbeitung ohne die Beteiligung beider Parteien an den Zwecken und Mitteln nicht möglich wäre, in dem Sinne, dass die Verarbeitung durch jede Partei**

[19] In der Tat beinhalten alle kommerziellen Vereinbarungen konvergierende Entscheidungen als Teil des Prozesses, durch den eine Vereinbarung erreicht wird.

untrennbar, d. h. unauflösbar miteinander verbunden. Die Situation gemeinsamer für die Verarbeitung Verantwortlicher, die auf der Grundlage konvergierender Entscheidungen handeln, sollte jedoch vom Fall eines Auftragsverarbeiters unterschieden werden, da letzterer - obwohl er an der Durchführung einer Verarbeitung beteiligt ist - die Daten nicht für seine eigenen Zwecke verarbeitet, sondern die Verarbeitung im Auftrag des für die Verarbeitung Verantwortlichen durchführt.

56. Die Tatsache, dass eine der Parteien keinen Zugang zu den verarbeiteten personenbezogenen Daten hat, reicht nicht aus, um eine gemeinsame Verantwortlichkeit auszuschließen. [20] In der Rechtssache *Jehovas Zeugen* vertrat der EuGH beispielsweise die Auffassung, dass eine Religionsgemeinschaft gemeinsam mit ihren Mitgliedern, die predigen, als für die Verarbeitung personenbezogener Daten durch letztere im Rahmen von Haus-zu-Haus-Predigten Verantwortliche anzusehen ist. [21] Der EuGH vertrat die Auffassung, dass es nicht erforderlich sei, dass die Gemeinschaft Zugang zu den fraglichen Daten hatte oder dass sie ihren Mitgliedern schriftliche Leitlinien oder Anweisungen in Bezug auf die Datenverarbeitung 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] Darüber hinaus hatte die Gemeinschaft auf allgemeiner Ebene Kenntnis davon, dass eine solche Verarbeitung durchgeführt wurde, um ihren Glauben zu verbreiten. [24]

57. Es ist auch wichtig zu betonen, wie der EuGH klargestellt hat, dass eine Stelle nur in Bezug auf diejenigen Vorgänge als gemeinsam für die Verarbeitung Verantwortlicher mit der/den anderen angesehen wird, für die sie gemeinsam mit anderen die Mittel und 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 vorausgehen oder nachfolgen, so ist diese Stelle als alleiniger für die Verarbeitung Verantwortlicher dieses vorausgehenden oder nachfolgenden Vorgangs anzusehen. [25]

58. Das Vorliegen einer gemeinsamen Verantwortung bedeutet nicht notwendigerweise, dass die verschiedenen an der Verarbeitung personenbezogener Daten beteiligten Betreiber gleichermaßen verantwortlich sind. Im Gegenteil, der EuGH hat klargestellt, dass diese Betreiber in verschiedenen Stadien dieser Verarbeitung und in unterschiedlichem Maße beteiligt sein können, so dass der Grad der Verantwortung jedes einzelnen von ihnen unter Berücksichtigung aller relevanten Umstände des Einzelfalls beurteilt werden muss.

3.2.2.1 Gemeinsam festgelegte(r) Zweck(e)

59. Gemeinsame Verantwortlichkeit liegt vor, wenn die an derselben Verarbeitung beteiligten Stellen 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 Einrichtungen nicht denselben Zweck mit der Verarbeitung verfolgen, kann im Lichte der Rechtsprechung des EuGH eine gemeinsame Verantwortlichkeit auch dann begründet werden, wenn die beteiligten Einrichtungen Zwecke verfolgen, die eng miteinander verbunden sind oder sich ergänzen. Dies kann z. B. der Fall sein, wenn aus derselben Verarbeitung ein gegenseitiger Nutzen entsteht, vorausgesetzt, dass jede der beteiligten Stellen an der Festlegung der Zwecke und Mittel der betreffenden Verarbeitung beteiligt ist. Der Begriff des gegenseitigen Nutzens ist jedoch nicht entscheidend und kann nur ein Indiz sein. In der Rechtssache *Fashion ID hat* der EuGH beispielsweise klargestellt, dass ein Website-Betreiber an der Festlegung der Zwecke

---

[20] Urteil in der Rechtssache *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, Rn. 38.
[21] Urteil in der Rechtssache *Zeugen Jehovas*, C-25/17, ECLI:EU:C:2018:551, Rn. 75.
[22] Ebd.
[23] Ebd., Absatz 71.
[24] Ebd.
[25] Urteil in der Rechtssache *Fashion ID*, C-40/17, ECLI:EU:2018:1039, Rn. 74: "*Dagegen kann eine natürliche oder juristische Person unbeschadet einer diesbezüglichen zivilrechtlichen Haftung nach nationalem Recht nicht als für die Verarbeitung Verantwortlicher im Sinne dieser Bestimmung im Rahmen von Vorgängen angesehen werden, die in der gesamten Verarbeitungskette vorausgehen oder nachgeordnet sind und für die diese Person weder die Zwecke noch die Mittel bestimmt*."

(und Mittel) der Verarbeitung durch die Einbettung eines Social Plug-Ins auf einer Website, um die Werbung für seine Waren zu optimieren, indem sie im sozialen Netzwerk besser sichtbar gemacht werden. Der EuGH vertrat die Auffassung, dass die fraglichen Verarbeitungen im wirtschaftlichen Interesse sowohl des Betreibers der Website als auch des Anbieters des Social Plug-Ins erfolgten. [26]

61. Ebenso dient, wie der EuGH in der Rechtssache *Wirtschaftsakademie* festgestellt hat, die Verarbeitung personenbezogener Daten durch Statistiken über die Besucher einer Fanpage dem Zweck, Facebook in die Lage zu versetzen, sein System der über sein Netzwerk übertragenen Werbung zu verbessern, und dem Administrator der Fanpage zu ermöglichen, Statistiken zur Verwaltung der Förderung seiner Tätigkeit zu erhalten. [27] Jede Einrichtung verfolgt in diesem Fall ihr eigenes Interesse, aber beide Parteien sind an der Festlegung der Zwecke (und Mittel) der Verarbeitung personenbezogener Daten in Bezug auf die Besucher der Fanpage beteiligt. [28]

62. In diesem Zusammenhang ist es wichtig zu betonen, dass das bloße Vorhandensein eines gegenseitigen Nutzens (z. B. kommerziell) aus einer Verarbeitungstätigkeit nicht zu einer gemeinsamen Kontrolle führt. Wenn die an der Verarbeitung beteiligte Stelle keine eigenen Zwecke in Bezug auf die Verarbeitungstätigkeit verfolgt, sondern lediglich für erbrachte Dienstleistungen bezahlt wird, handelt sie als Auftragsverarbeiter und nicht als gemeinsam für die Verarbeitung Verantwortlicher.

3.2.2.2 Gemeinsam festgelegt bedeutet

63. Gemeinsame Kontrolle erfordert auch, dass zwei oder mehr Unternehmen Einfluss auf die Mittel der Verarbeitung ausgeübt haben. Dies bedeutet nicht, dass jede beteiligte Einheit in allen Fällen alle Mittel bestimmen muss, damit eine gemeinsame Kontrolle vorliegt. Wie der EuGH klargestellt hat, können nämlich verschiedene Stellen in verschiedenen Phasen der Verarbeitung und in unterschiedlichem Maße beteiligt sein. Verschiedene gemeinsam für die Verarbeitung Verantwortliche können daher die Mittel der Verarbeitung in unterschiedlichem Maße festlegen, je nachdem, wer tatsächlich in der Lage ist, dies zu tun.

64. Es kann auch der Fall sein, dass eine der beteiligten Stellen die Mittel für die Verarbeitung bereitstellt und sie für die Verarbeitung personenbezogener Daten durch andere Stellen verfügbar macht. Die Stelle, die beschließt, diese Mittel zu nutzen, damit personenbezogene Daten für einen bestimmten Zweck verarbeitet werden können, ist auch an der Festlegung der Mittel für die Verarbeitung beteiligt.

65. Dieses Szenario kann insbesondere bei Plattformen, standardisierten Werkzeugen oder anderen Infrastrukturen auftreten, die es den Parteien ermöglichen, dieselben personenbezogenen Daten zu verarbeiten, und die von einer der Parteien in einer bestimmten Weise eingerichtet wurden, damit sie von anderen genutzt werden können, die ebenfalls 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 vorzunehmende Verarbeitung personenbezogener Daten entscheiden können.

66. Als Beispiel hierfür hat der EuGH in der Rechtssache *Wirtschaftsakademie* entschieden, dass der Administrator einer auf Facebook gehosteten Fanpage durch die Festlegung von Parametern auf der Grundlage seiner Zielgruppe und der Ziele der Verwaltung und Förderung seiner Aktivitäten als an der Bestimmung der Mittel für die Verarbeitung personenbezogener Daten in Bezug auf die Besucher seiner Fanpage beteiligt angesehen werden muss.

67. Darüber hinaus wird die Entscheidung einer Einrichtung, ein von einer anderen Einrichtung entwickeltes Tool oder System, das die Verarbeitung personenbezogener Daten ermöglicht, für ihre eigenen Zwecke zu nutzen, wahrscheinlich einer gemeinsamen Entscheidung über die Mittel ~~Art und Weise~~ dieser Verarbeitung durch diese Einrichtungen gleichkommen. Dies ergibt sich aus dem Fall Fashion ID, wo

---

[26] Urteil in der Rechtssache *Fashion ID,* C-40/17, ECLI:EU:2018:1039, Rn. 80.
[27] Urteil in der Rechtssache *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, Rn. 34.
[28] Urteil in der Rechtssache *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, Rn. 39.
[29] Der Anbieter des Systems kann ein gemeinsamer 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.

der EuGH zu dem Schluss kam, dass Fashion ID durch die Einbettung des von Facebook für Website-Betreiber zur Verfügung gestellten Facebook-Like-Buttons auf ihrer Website einen bestimmenden Einfluss auf die Vorgänge der Erhebung und Übermittlung der personenbezogenen Daten der Besucher ihrer Website an Facebook ausgeübt und damit gemeinsam mit Facebook die Mittel dieser Verarbeitung bestimmt hat. [30]

68. Es ist wichtig zu betonen, dass **die Nutzung eines gemeinsamen Datenverarbeitungssystems oder einer gemeinsamen Datenverarbeitungsinfrastruktur nicht in allen Fällen dazu führt, dass die beteiligten Parteien als gemeinsam für die** Verarbeitung **Verantwortliche eingestuft werden,** insbesondere dann nicht, wenn die von ihnen durchgeführte Verarbeitung trennbar ist und von einer Partei ohne Eingreifen der anderen durchgeführt werden könnte oder wenn der Anbieter ein Auftragsverarbeiter ohne eigenen Zweck ist (das Vorhandensein eines bloßen kommerziellen Vorteils für die beteiligten Parteien reicht nicht aus, um als Zweck der Verarbeitung eingestuft zu werden).

Beispiel: Reisebüro

Ein Reisebüro sendet persönliche Daten seiner Kunden an die Fluggesellschaft und eine Hotelkette, um Reservierungen für ein Reisepaket vorzunehmen. Die Fluggesellschaft und das Hotel bestätigen die Verfügbarkeit der gewünschten Plätze und Zimmer. Das Reisebüro stellt die Reiseunterlagen und Voucher für seine Kunden aus. Jeder der Akteure verarbeitet die Daten zur Durchführung seiner eigenen Aktivitäten und mit seinen eigenen Mitteln. In diesem Fall sind das Reisebüro, die Fluggesellschaft und das Hotel drei verschiedene für die Datenverarbeitung Verantwortliche, die die Daten für ihre eigenen und getrennten Zwecke verarbeiten, und es gibt keine gemeinsame Kontrollstelle.

Das Reisebüro, die Hotelkette und die Fluggesellschaft beschließen dann, sich gemeinsam an der Einrichtung einer internetbasierten gemeinsamen Plattform für den gemeinsamen Zweck der Bereitstellung von Pauschalreiseangeboten zu beteiligen. Sie einigen sich auf die wesentlichen zu verwendenden Mittel, wie z. B. welche Daten gespeichert werden, wie Reservierungen zugewiesen und bestätigt werden und wer Zugang zu den gespeicherten Informationen haben kann. Außerdem beschließen sie, die Daten ihrer Kunden gemeinsam zu nutzen, um gemeinsame Marketingaktionen durchzuführen. In diesem Fall legen das Reisebüro, die Fluggesellschaft und die Hotelkette gemeinsam fest, warum und wie personenbezogene Daten ihrer jeweiligen Kunden verarbeitet werden, und sind daher gemeinsam für die Verarbeitung Verantwortliche in Bezug auf die Verarbeitungsvorgänge im Zusammenhang mit der gemeinsamen internetbasierten Buchungsplattform und die gemeinsamen Marketingaktionen. Jeder von ihnen würde jedoch weiterhin die alleinige Kontrolle in Bezug auf andere Verarbeitungsvorgänge außerhalb der gemeinsamen internetbasierten Plattform behalten.

Beispiel: Forschungsprojekt von Instituten

Mehrere Forschungsinstitute beschließen, an einem bestimmten gemeinsamen Forschungsprojekt teilzunehmen und dazu die bestehende Plattform eines der am Projekt beteiligten Institute zu nutzen. Jedes Institut speist personenbezogene Daten, die es bereits besitzt, zum Zweck der gemeinsamen Forschung in die Plattform ein und nutzt die von anderen über die Plattform bereitgestellten Daten zur Durchführung der Forschung. In diesem Fall qualifizieren sich alle Institute als gemeinsame Verantwortliche für die Verarbeitung personenbezogener Daten, die durch die Speicherung und Weitergabe von Informationen aus dieser Plattform erfolgt, da sie gemeinsam über den Zweck der Verarbeitung und die zu verwendenden Mittel (die bestehende Plattform) entschieden haben. Jedes der Institute ist jedoch ein separater Verantwortlicher für jede andere Verarbeitung, die außerhalb der Plattform für ihre jeweiligen Zwecke durchgeführt werden kann.

Beispiel: Marketingbetrieb

Die Unternehmen A und B haben ein Co-Branding-Produkt C auf den Markt gebracht und möchten eine Veranstaltung organisieren, um dieses Produkt zu bewerben. Zu diesem Zweck beschließen sie, Daten von ihren jeweiligen Kunden- und Interessenten-

[30] Urteil in der Rechtssache Fashion ID, C-40/17, ECLI:EU:2018:1039, Randnrn. 77-79.

Datenbanken auszutauschen und entscheiden auf dieser Basis über die Liste der Eingeladenen zur Veranstaltung. Sie vereinbaren auch die Modalitäten für den Versand der Einladungen zu der Veranstaltung, die Erfassung von Rückmeldungen während der Veranstaltung und nachfolgende Marketingaktionen. Die Unternehmen A und B können als gemeinsam für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Organisation der Werbeveranstaltung Verantwortliche angesehen 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 Universität (der Sponsor) beschließen, gemeinsam eine klinische Studie mit demselben Ziel zu starten. Sie arbeiten gemeinsam an der Erstellung des Studienprotokolls (d. h. Zweck, Methodik/Design der Studie, zu erhebende Daten, Ausschluss-/Einschlusskriterien für Probanden, Wiederverwendung der Datenbank (sofern relevant) usw.). Sie können als gemeinsam für diese klinische Prüfung Verantwortliche angesehen werden, da sie gemeinsam denselben Zweck und die wesentlichen Mittel der Verarbeitung bestimmen und vereinbaren. Die Erhebung personenbezogener Daten aus der Patientenakte zu Forschungszwecken ist von der Speicherung und Nutzung derselben Daten zum Zweck der Patientenversorgung zu unterscheiden, für die der Gesundheitsdienstleister der für die Verarbeitung Verantwortliche bleibt.

Für den Fall, dass der Prüfer nicht an der Erstellung des Prüfplans beteiligt ist (er akzeptiert lediglich den vom Sponsor bereits ausgearbeiteten Prüfplan) und der Prüfplan nur vom Sponsor entworfen wird, sollte der Prüfer als Bearbeiter und der Sponsor als Verantwortlicher für diese klinische Prüfung betrachtet werden.

Beispiel: Headhunter

Unternehmen X hilft Unternehmen Y bei der Rekrutierung neuer Mitarbeiter - mit seinem berühmten Mehrwertdienst "global matchz". Unternehmen X sucht nach geeigneten Kandidaten sowohl unter den Lebensläufen, die direkt bei Unternehmen Y eingehen, als auch unter denen, die es bereits in seiner eigenen Datenbank hat. Diese Datenbank wird von Unternehmen X in Eigenregie erstellt und verwaltet. Dadurch wird sichergestellt, dass Unternehmen X das Matching zwischen Stellenangeboten und Stellensuchenden verbessert und somit seine Einnahmen erhöht. Auch wenn sie formal keine gemeinsame Entscheidung getroffen haben, beteiligen sich die Unternehmen X und Y gemeinsam an der Verarbeitung mit dem Ziel, geeignete Kandidaten auf der Grundlage konvergierender Entscheidungen zu finden: die Entscheidung, den Service "global matchz" für Unternehmen X zu erstellen und zu verwalten, und die Entscheidung von Unternehmen Y, die Datenbank mit den Lebensläufen anzureichern, die es direkt erhält. Diese Entscheidungen ergänzen sich gegenseitig, sind untrennbar miteinander verbunden und notwendig, damit der Prozess des Findens geeigneter Kandidaten stattfinden kann. Daher sollten sie in diesem besonderen Fall als gemeinsam für die Verarbeitung Verantwortliche 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 die anschließende Einstellungsverarbeitung für seine eigenen Zwecke (Organisation von Vorstellungsgesprächen, Abschluss des Vertrags und Verwaltung von Personaldaten).

Beispiel: Analyse von Gesundheitsdaten

Unternehmen ABC, der Entwickler einer App zur Blutdrucküberwachung, und Unternehmen XYZ, ein Anbieter von Apps für medizinisches Fachpersonal, möchten beide untersuchen, wie Blutdruckveränderungen zur Vorhersage bestimmter Krankheiten beitragen können. Die Unternehmen beschließen, ein gemeinsames Projekt auf die Beine zu stellen und wenden sich an das Krankenhaus DEF, um sich ebenfalls zu beteiligen.

Die personenbezogenen Daten, die in diesem Projekt verarbeitet werden, bestehen aus personenbezogenen Daten, die Unternehmen ABC, Krankenhaus DEF und Unternehmen XYZ als einzelne Verantwortliche getrennt voneinander verarbeiten. Die Entscheidung zu

Die Verarbeitung dieser Daten zur Beurteilung von Blutdruckveränderungen wird von den drei Akteuren gemeinsam vorgenommen. Unternehmen ABC, Krankenhaus DEF und Unternehmen XYZ haben gemeinsam die Zwecke der Verarbeitung festgelegt. Unternehmen XYZ ergreift die Initiative und schlägt die wesentlichen Mittel der Verarbeitung vor. Sowohl Unternehmen ABC als auch das Krankenhaus DEF akzeptieren diese wesentlichen Mittel, nachdem auch sie an der Entwicklung einiger Funktionen der App beteiligt waren, damit die Ergebnisse von ihnen ausreichend genutzt werden können. Die drei Organisationen einigen sich also auf einen gemeinsamen Zweck für die Verarbeitung, nämlich die Beurteilung, wie Blutdruckveränderungen zur Vorhersage bestimmter Krankheiten beitragen können. Sobald die Untersuchung abgeschlossen ist, können Unternehmen ABC, Krankenhaus DEF und Unternehmen XYZ von der Bewertung profitieren, indem sie die Ergebnisse für ihre eigenen Aktivitäten nutzen. Aus all diesen Gründen qualifizieren sie sich als gemeinsam für die Verarbeitung Verantwortliche für diese spezielle gemeinsame Verarbeitung.

Wäre die Firma XYZ von den anderen lediglich gebeten worden, diese Bewertung durchzuführen, ohne einen eigenen Zweck zu verfolgen, und hätte sie die Daten lediglich im Auftrag der anderen verarbeitet, wäre die Firma XYZ als Auftragsverarbeiter zu qualifizieren, selbst wenn sie mit der Bestimmung der nicht wesentlichen Mittel betraut worden wäre.

3.2.3 Situationen, in denen es keine gemeinsame Verantwortlichkeit gibt

69. Die Tatsache, dass mehrere Akteure an der gleichen Verarbeitung beteiligt sind, bedeutet nicht, dass sie notwendigerweise als gemeinsam für die Verarbeitung Verantwortliche handeln. Nicht alle Arten von Partnerschaften, Kooperationen oder Zusammenarbeit implizieren die Einstufung als gemeinsam für die Verarbeitung Verantwortliche, da eine solche Einstufung eine Einzelfallanalyse der jeweiligen Verarbeitung und der genauen Rolle jeder Einheit in Bezug auf jede Verarbeitung erfordert. Die folgenden Fälle sind nicht erschöpfende Beispiele für Situationen, in denen keine gemeinsame für die Verarbeitung Verantwortlichkeit vorliegt.

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 eine Übermittlung von Daten zwischen getrennten für die Verarbeitung Verantwortlichen betrachtet werden.

Beispiel: Übermittlung von Mitarbeiterdaten an Steuerbehörden

Ein Unternehmen sammelt und verarbeitet personenbezogene Daten seiner Mitarbeiter zum Zweck der Verwaltung von Gehältern, Krankenversicherungen usw. Ein Gesetz verpflichtet das Unternehmen, alle Daten über Gehälter an die Steuerbehörden zu übermitteln, um die Steuerkontrolle zu verstärken.

Auch wenn in diesem Fall sowohl das Unternehmen als auch die Steuerbehörde dieselben Daten über die Gehälter verarbeiten, führt das Fehlen gemeinsam festgelegter Zwecke und Mittel in Bezug auf diese Datenverarbeitung dazu, dass die beiden Einheiten als zwei getrennte Datenverantwortliche eingestuft werden.

71. Die gemeinsame Kontrolle kann auch in einer Situation ausgeschlossen werden, in der mehrere Einheiten eine gemeinsame Datenbank oder eine gemeinsame Infrastruktur nutzen, wenn jede Einheit unabhängig ihre eigenen Zwecke bestimmt.

Beispiel: Marketingaktivitäten in einer Gruppe von Unternehmen, die eine gemeinsame Datenbank verwenden:

Eine Gruppe von Unternehmen verwendet dieselbe Datenbank für die Verwaltung von Kunden und Interessenten. Eine solche Datenbank wird auf den Servern der Muttergesellschaft gehostet, die daher hinsichtlich der Speicherung der Daten ein Auftragsverarbeiter der Unternehmen ist. Jedes Unternehmen der Gruppe gibt die Daten seiner eigenen Kunden und Interessenten ein und verarbeitet diese Daten nur für seine eigenen Zwecke. Auch entscheidet jedes Unternehmen unabhängig über den Zugang, die Aufbewahrungsfristen, die Korrektur oder Löschung der Daten seiner Kunden und Interessenten. Sie können nicht auf die Daten des jeweils anderen zugreifen oder diese nutzen. Die bloße Tatsache, dass diese Unternehmen eine gemeinsame Konzerndatenbank nutzen, führt als solche nicht zu einer gemeinsamen Beherrschung. Unter diesen Umständen ist also jedes Unternehmen ein separater Verantwortlicher.

Beispiel: Unabhängige Steuerungen bei Verwendung einer gemeinsamen Infrastruktur

Unternehmen XYZ hostet eine Datenbank und stellt sie anderen Unternehmen zur Verfügung, um personenbezogene Daten über deren Mitarbeiter zu verarbeiten und zu hosten. Unternehmen XYZ ist ein Auftragsverarbeiter in Bezug auf die Verarbeitung und Speicherung der Mitarbeiter anderer Unternehmen, da diese Vorgänge im Namen und nach den Anweisungen dieser anderen Unternehmen durchgeführt werden. Darüber hinaus verarbeiten die anderen Unternehmen die Daten ohne jegliche Beteiligung von Unternehmen XYZ und für Zwecke, die in keiner Weise von Unternehmen XYZ geteilt werden.

72. Es kann auch Situationen geben, in denen verschiedene Akteure nacheinander dieselben personenbezogenen Daten in einer Kette von Vorgängen verarbeiten, wobei jeder dieser Akteure in seinem Teil der Kette einen unabhängigen Zweck und unabhängige Mittel hat. In Ermangelung einer gemeinsamen Beteiligung an der Festlegung der Zwecke und Mittel ein und desselben Verarbeitungsvorgangs oder einer Reihe von Vorgängen ist eine gemeinsame Verantwortlichkeit auszuschließen, und die verschiedenen Akteure sind als aufeinanderfolgende unabhängige für die Verarbeitung Verantwortliche zu betrachten.

Beispiel: Statistische Analyse für eine Aufgabe von öffentlichem Interesse

Eine öffentliche Behörde (Behörde A) hat die gesetzliche Aufgabe, relevante Analysen und Statistiken darüber zu erstellen, wie sich die Beschäftigungsquote des Landes entwickelt. Dazu sind viele andere öffentliche Stellen gesetzlich verpflichtet, bestimmte Daten an Behörde A weiterzugeben. Behörde A beschließt, ein bestimmtes System zur Verarbeitung der Daten, einschließlich der Erfassung, zu verwenden. Das bedeutet auch, dass die anderen Stellen verpflichtet sind, das System für ihre Datenbekanntgabe zu verwenden. In diesem Fall ist Behörde A, unbeschadet einer gesetzlichen Rollenverteilung, der einzige für die Verarbeitung Verantwortliche zum Zweck der Analyse und Statistik der im System verarbeiteten Beschäftigungsquote, da Behörde A den Zweck der Verarbeitung bestimmt und entschieden hat, wie die Verarbeitung organisiert wird. Natürlich sind die anderen öffentlichen Stellen als Verantwortliche für ihre eigenen Verarbeitungstätigkeiten für die Richtigkeit der Daten verantwortlich, die sie zuvor verarbeitet haben und die sie dann an Behörde A weitergeben.

4 DEFINITION DES AUFTRAGSVERARBEITERS

73. Ein Auftragsverarbeiter ist in Artikel 4 (8) definiert als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. Ähnlich wie die Definition des für die Verarbeitung Verantwortlichen sieht auch die Definition des Auftragsverarbeiters 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 im Prinzip keine Einschränkung gibt, welche Art von Akteur die Rolle des Auftragsverarbeiters übernehmen kann. Es kann sich um eine Organisation handeln, aber auch um eine Einzelperson.

74. Die DSGVO legt Verpflichtungen fest, die direkt und speziell für Auftragsverarbeiter gelten, wie in Teil II Abschnitt 1 dieser Leitlinien näher erläutert. Ein Auftragsverarbeiter kann haftbar gemacht oder mit einer Geldstrafe belegt werden, wenn er diesen Verpflichtungen nicht nachkommt oder wenn er außerhalb der rechtmäßigen Anweisungen des für die Verarbeitung Verantwortlichen oder entgegen diesen handelt.

75. An der Verarbeitung von personenbezogenen Daten können mehrere Auftragsverarbeiter beteiligt sein. Beispielsweise kann ein für die Verarbeitung Verantwortlicher selbst entscheiden, mehrere Auftragsverarbeiter direkt zu beauftragen, indem er verschiedene Auftragsverarbeiter in verschiedenen Phasen der Verarbeitung einbezieht (mehrere Auftragsverarbeiter). Ein für die Verarbeitung Verantwortlicher kann auch beschließen, einen Auftragsverarbeiter zu beauftragen, der seinerseits - mit Genehmigung des für die Verarbeitung Verantwortlichen - einen oder mehrere andere Auftragsverarbeiter ("Unterauftragsverarbeiter") einbezieht. Die dem Auftragsverarbeiter anvertraute Verarbeitungstätigkeit kann auf eine ganz bestimmte Aufgabe oder einen bestimmten Kontext beschränkt sein oder allgemeiner und umfassender sein.

76. Zwei Grundvoraussetzungen für die Qualifizierung als Prozessor sind:

a) *eine separate Einheit* in Bezug auf den Controller ist und

b) Verarbeitung personenbezogener Daten im *Auftrag des für die Verarbeitung Verantwortlichen*.

77. *Eine getrennte Einheit* bedeutet, dass der Verantwortliche beschließt, alle oder einen Teil der Verarbeitungstätigkeiten an eine externe Organisation zu delegieren. Innerhalb einer Unternehmensgruppe kann ein Unternehmen ein Auftragsverarbeiter für ein anderes Unternehmen sein, das als Verantwortlicher agiert, da beide Unternehmen getrennte Einheiten sind. Andererseits kann eine Abteilung innerhalb eines Unternehmens nicht als Auftragsverarbeiter für eine andere Abteilung innerhalb desselben Unternehmens auftreten.

78. Wenn der für die Verarbeitung Verantwortliche beschließt, Daten selbst zu verarbeiten, indem er seine eigenen Ressourcen innerhalb seiner Organisation einsetzt, z. B. durch seine eigenen Mitarbeiter, ist dies keine Auftragsverarbeitungssituation. Mitarbeiter und andere Personen, die unter der direkten Autorität des für die Verarbeitung Verantwortlichen handeln, wie z. B. vorübergehend angestellte Mitarbeiter, sind nicht als Auftragsverarbeiter zu betrachten, da sie personenbezogene Daten als Teil der Einheit des für die Verarbeitung Verantwortlichen verarbeiten werden. Gemäß Artikel 29 sind auch sie an die Weisungen des für die Verarbeitung Verantwortlichen gebunden.

79. Die *Verarbeitung personenbezogener Daten im Auftrag des für die Verarbeitung Verantwortlichen* setzt zunächst voraus, dass die getrennte Stelle personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. In Artikel 4 Absatz 2 wird die Verarbeitung als ein Konzept definiert, das eine breite Palette von Vorgängen umfasst, die von der Erhebung, Speicherung und Abfrage bis hin zur Nutzung, Verbreitung oder sonstigen Bereitstellung und Vernichtung reichen. Das Konzept der "Verarbeitung" wird weiter oben unter 2.1.5 beschrieben.

80. Zweitens muss die Verarbeitung im Auftrag eines für die Verarbeitung Verantwortlichen erfolgen, aber nicht unter dessen direkter Autorität oder Kontrolle. Handeln "im Auftrag" bedeutet, dem Interesse eines anderen zu dienen und erinnert an den Rechtsbegriff der "Delegation". Im Falle des Datenschutzrechts ist ein Auftragsverarbeiter aufgerufen, die vom Verantwortlichen erteilten Weisungen zumindest im Hinblick auf den Zweck der Verarbeitung und die wesentlichen Elemente der Mittel umzusetzen. Die Rechtmäßigkeit der Verarbeitung gemäß Artikel 6 und gegebenenfalls Artikel 9 der Verordnung wird aus der Tätigkeit des für die Verarbeitung Verantwortlichen abgeleitet, und der Auftragsverarbeiter darf die Daten nicht anders als nach den Anweisungen des für die Verarbeitung Verantwortlichen verarbeiten. Dennoch können die Weisungen des für die Verarbeitung Verantwortlichen, wie oben beschrieben, immer noch einen gewissen Ermessensspielraum darüber lassen, wie den Interessen des für die Verarbeitung Verantwortlichen am besten gedient werden kann, so dass der Auftragsverarbeiter die am besten geeigneten technischen und organisatorischen Mittel wählen kann. [32]

81. Handeln "im Auftrag" bedeutet auch, dass der Auftragsverarbeiter keine Verarbeitung für seine eigenen Zwecke durchführen darf. Wie in Artikel 28 Absatz 10 vorgesehen, verstößt ein Auftragsverarbeiter gegen die DSGVO, wenn er über die Anweisungen des für die Verarbeitung Verantwortlichen hinausgeht und beginnt, seine eigenen Zwecke und Mittel der Verarbeitung zu bestimmen. Der Auftragsverarbeiter wird in Bezug auf diese Verarbeitung als für die Verarbeitung Verantwortlicher betrachtet und kann Sanktionen für das Überschreiten der Anweisungen des für die Verarbeitung Verantwortlichen unterworfen werden.

Beispiel: Dienstleister wird als Datenverarbeiter bezeichnet, handelt aber als Controller

Der Dienstleister MarketinZ erbringt für verschiedene Unternehmen Dienstleistungen im Bereich der kommerziellen Werbung und des Direktmarketings. Das Unternehmen GoodProductZ schließt mit MarketinZ einen Vertrag ab, wonach letzteres Unternehmen kommerzielle Werbung für GoodProductZ-Kunden bereitstellt und als Datenverarbeiter bezeichnet wird. MarketinZ beschließt jedoch, die Kundendatenbank von GoodProductZ auch für andere Zwecke als die Werbung für GoodProductZ zu nutzen, z. B. für die Entwicklung ihrer eigenen Geschäftstätigkeit. Die Entscheidung, einen zusätzlichen Zweck zu dem hinzuzufügen, für den die personenbezogenen Daten übermittelt wurden, macht MarketinZ zu einem Datenverantwortlichen für diese Reihe von Verarbeitungsvorgängen und ihre Verarbeitung für diesen Zweck würde einen Verstoß gegen die DSGVO darstellen.

82. Der EDSB erinnert daran, dass nicht jeder Diensteanbieter, der personenbezogene Daten im Rahmen der Erbringung einer Dienstleistung verarbeitet, ein "Auftragsverarbeiter" im Sinne der DSGVO ist. Die Rolle eines Auftragsverarbeiters ergibt sich nicht aus der Art einer Einrichtung, die Daten verarbeitet, sondern aus ihren konkreten Tätigkeiten in einem bestimmten Kontext. Mit anderen Worten, dieselbe Stelle kann bei bestimmten Verarbeitungen gleichzeitig als Verantwortlicher handeln

[32] Siehe Teil I, Unterabschnitt 2.1.4, der die Unterscheidung zwischen wesentlichen und nicht-wesentlichen Mitteln beschreibt.

Vorgänge und als Auftragsverarbeiter für andere, und die Qualifikation als Verantwortlicher oder Auftragsverarbeiter muss in Bezug auf bestimmte Datensätze oder Vorgänge beurteilt werden. Die Art des Dienstes bestimmt, ob die Verarbeitungstätigkeit eine Verarbeitung personenbezogener Daten im Auftrag des für die Verarbeitung Verantwortlichen im Sinne der DSGVO darstellt. In der Praxis kann der Diensteanbieter in Fällen, in denen der erbrachte Dienst nicht speziell auf die Verarbeitung personenbezogener Daten ausgerichtet ist oder eine solche Verarbeitung kein Schlüsselelement des Dienstes darstellt, in der Lage sein, die Zwecke und Mittel dieser Verarbeitung, die für die Erbringung des Dienstes erforderlich ist, selbst zu bestimmen. In diesem Fall ist der Diensteanbieter als eigenständiger für die Verarbeitung Verantwortlicher und nicht als Auftragsverarbeiter zu betrachten. [33] [Es] ist jedoch weiterhin eine Einzelfallanalyse erforderlich, um festzustellen, wie groß der Einfluss ist, den jede Stelle bei der Festlegung der Zwecke und Mittel der Verarbeitung tatsächlich hat.

Beispiel: Taxidienst

Ein Taxi-Service bietet eine Online-Plattform an, über die Unternehmen ein Taxi für den Transport von Mitarbeitern oder Gästen zum und vom Flughafen buchen können. Bei der Buchung eines Taxis gibt Unternehmen ABC den Namen des Mitarbeiters an, der vom 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 Unternehmen ABC, aber die Verarbeitung als solche ist nicht das Ziel der Dienstleistung. Der Taxidienst hat die Online-Buchungsplattform als Teil der Entwicklung seiner eigenen Geschäftstätigkeit zur Erbringung von Beförderungsleistungen ohne Anweisungen von Unternehmen ABC entwickelt. Der Taxidienst bestimmt auch selbständig, welche Datenkategorien er erhebt und wie lange er sie aufbewahrt. Der Taxidienst handelt daher als für die Verarbeitung Verantwortlicher in eigenem Recht, ungeachtet der Tatsache, dass die Verarbeitung nach einer Anfrage für eine Dienstleistung von Unternehmen ABC erfolgt.

83. Der EDSB stellt fest, dass ein Dienstleister auch dann als Auftragsverarbeiter tätig sein kann, wenn die Verarbeitung personenbezogener Daten nicht der Haupt- oder Primärgegenstand des Dienstes ist, sofern der Kunde des Dienstes in der Praxis weiterhin die Zwecke und Mittel der Verarbeitung bestimmt. Bei der Erwägung, ob die Verarbeitung personenbezogener Daten einem bestimmten Dienstleister anvertraut werden soll oder nicht, sollten die für die Verarbeitung Verantwortlichen sorgfältig prüfen, ob der betreffende Dienstleister ihnen ein ausreichendes Maß an Kontrolle ermöglicht, wobei Art, Umfang, Kontext und Zwecke der Verarbeitung sowie die potenziellen Risiken für die betroffenen Personen zu berücksichtigen sind.

Beispiel: Call-Center

Unternehmen X lagert seinen Kundensupport an Unternehmen Y aus, das ein Callcenter bereitstellt, um den Kunden von Unternehmen X bei ihren Fragen zu helfen. Die Kundenbetreuung bedeutet, dass Unternehmen Y Zugriff auf die Kundendatenbanken von Unternehmen X haben muss. Unternehmen Y kann nur auf Daten zugreifen, um den von Unternehmen X vermittelten Support zu leisten, und darf Daten nicht für andere als die von Unternehmen X angegebenen Zwecke verarbeiten. Unternehmen Y ist als Verarbeiter personenbezogener Daten zu sehen, und zwischen Unternehmen X und Y muss ein Verarbeitungsvertrag geschlossen werden.

Beispiel: Allgemeiner IT-Support

Unternehmen Z beauftragt einen IT-Dienstleister mit dem allgemeinen Support seiner IT-Systeme, die eine große Menge an personenbezogenen Daten enthalten. Der Zugriff auf personenbezogene Daten ist nicht der Hauptgegenstand der Supportleistung, aber es ist unvermeidlich, dass der IT-

[33] Siehe auch Erwägungsgrund 81 der DSGVO, der sich auf die "Beauftragung eines Auftragsverarbeiters mit Verarbeitungstätigkeiten" bezieht und darauf hinweist, dass die Verarbeitungstätigkeit als solche ein wichtiger Bestandteil der Entscheidung des für die Verarbeitung Verantwortlichen ist, einen Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten in seinem Namen zu beauftragen.

Erbringung der Dienstleistung. Unternehmen Z kommt daher zu dem Schluss, dass der IT-Dienstleister - der ein eigenständiges Unternehmen ist und zwangsläufig personenbezogene Daten verarbeiten muss, auch wenn dies nicht der Hauptzweck der Dienstleistung ist - als Auftragsverarbeiter zu betrachten ist. Daher wird mit dem IT-Dienstleister ein Auftragsverarbeitungsvertrag geschlossen.

Beispiel: IT-Berater, der einen Softwarefehler behebt

Unternehmen ABC stellt einen IT-Spezialisten eines anderen Unternehmens ein, um einen Fehler in einer Software zu beheben, die von dem Unternehmen verwendet wird. Der IT-Berater wird nicht eingestellt, um personenbezogene Daten zu verarbeiten, und Unternehmen ABC stellt fest, dass jeder Zugriff auf personenbezogene Daten rein zufällig und daher in der Praxis sehr begrenzt sein wird. ABC kommt daher zu dem Schluss, dass der IT-Spezialist kein Auftragsverarbeiter (und auch kein für die Verarbeitung Verantwortlicher in eigenem Recht) ist und dass Unternehmen ABC geeignete Maßnahmen gemäß Artikel 32 der DSGVO ergreifen wird, um zu verhindern, dass der IT-Berater personenbezogene Daten auf unzulässige Weise verarbeitet.

84. Wie bereits erwähnt, hindert nichts den Auftragsverarbeiter daran, einen vorläufig definierten Dienst anzubieten, aber der für die Verarbeitung Verantwortliche muss die endgültige Entscheidung treffen, die Art und Weise der Verarbeitung aktiv zu genehmigen, zumindest was die wesentlichen Mittel der Verarbeitung betrifft. Wie bereits erwähnt, hat der Auftragsverarbeiter einen Handlungsspielraum in Bezug auf nicht wesentliche Mittel, siehe oben unter Unterabschnitt 2.1.4.

Beispiel: Cloud-Dienstleister

Eine Gemeinde hat beschlossen, einen Cloud-Dienstanbieter für die Handhabung von Informationen in ihren Schul- und Bildungsdiensten zu nutzen. Der Cloud-Dienst bietet Messaging-Dienste, Videokonferenzen, Speicherung von Dokumenten, Kalenderverwaltung, Textverarbeitung usw. und wird die Verarbeitung personenbezogener Daten von Schulkindern und Lehrern mit sich bringen. Der Cloud-Service-Anbieter hat einen standardisierten Dienst angeboten, der weltweit angeboten wird. Die Gemeinde muss jedoch sicherstellen, dass die bestehende Vereinbarung mit Artikel 28 Absatz 3 der DSGVO übereinstimmt und dass die personenbezogenen Daten, für die sie verantwortlich ist, nur für die Zwecke der Gemeinde verarbeitet werden. Sie muss auch sicherstellen, dass ihre spezifischen Anweisungen zu Aufbewahrungsfristen, Löschung von Daten usw. vom Cloud-Service-Anbieter eingehalten werden, unabhängig davon, was allgemein im standardisierten Dienst angeboten wird.

5 DEFINITION DES DRITTEN/EMPFÄNGERS

85. Die Verordnung definiert nicht nur die Begriffe "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", sondern auch die Begriffe "Empfänger" und "Dritter". Im Gegensatz zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter" legt die Verordnung keine spezifischen Pflichten oder Verantwortlichkeiten für Empfänger und Dritte fest. Diese können als relative Begriffe in dem Sinne bezeichnet werden, dass sie eine Beziehung zu einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter aus einer bestimmten Perspektive beschreiben, z. B. ein für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter gibt Daten an einen Empfänger weiter. Ein Empfänger personenbezogener Daten und ein Dritter können durchaus gleichzeitig aus anderen Perspektiven als für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter angesehen werden. Beispielsweise sind Stellen, die aus einer Perspektive als Empfänger oder Dritte zu betrachten sind, für die Verarbeitung, deren Zweck und Mittel sie bestimmen, Verantwortliche.

Dritte Partei

86. In Artikel 4 Absatz 10 wird ein "*Dritter*" definiert als eine natürliche oder juristische Person, Behörde, Einrichtung oder Stelle mit Ausnahme von

- die betroffene Person,
- die Steuerung,
- den Prozessor und

- Personen, die unter der direkten Autorität des Verantwortlichen oder des Auftragsverarbeiters befugt sind, personenbezogene Daten zu verarbeiten.

87. Die Definition entspricht im Wesentlichen der bisherigen Definition des Begriffs "*Dritter*" in der Richtlinie 95/46/EG.

88. Während die Begriffe "*personenbezogene Daten*", "*betroffene Person*", "*für die Verarbeitung Verantwortlicher*" und "*Auftragsverarbeiter*" in der Verordnung definiert sind, ist der Begriff "*Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung 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 Rechtsperson des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters gehören (ein Angestellter oder eine Rolle, die in hohem Maße mit der von Angestellten vergleichbar ist, z. B. Zeitarbeitskräfte, die über ein Zeitarbeitsunternehmen zur Verfügung gestellt werden), aber nur insoweit, als sie zur Verarbeitung personenbezogener Daten befugt sind. Ein Mitarbeiter etc., der sich Zugang zu Daten verschafft, zu denen er nicht befugt ist, und zwar zu anderen Zwecken als denen des Arbeitgebers, fällt nicht in diese Kategorie. Vielmehr ist dieser Mitarbeiter als Dritter gegenüber der Verarbeitung durch den Arbeitgeber zu betrachten. Sofern der Arbeitnehmer personenbezogene Daten für seine eigenen Zwecke, die sich von denen seines Arbeitgebers unterscheiden, verarbeitet, wird er als Verantwortlicher betrachtet und übernimmt alle sich daraus ergebenden Konsequenzen und Haftungen in Bezug auf die Verarbeitung personenbezogener Daten. [34]

89. Ein Dritter bezieht sich somit auf jemanden, der in der konkreten Situation weder eine betroffene Person noch ein Verantwortlicher, ein Auftragsverarbeiter oder ein Mitarbeiter ist. Der für die Verarbeitung Verantwortliche kann z. B. einen Auftragsverarbeiter beauftragen und diesen anweisen, personenbezogene Daten an einen Dritten zu übertragen. Dieser Dritte wird dann für die Verarbeitung, die er für seine eigenen Zwecke durchführt, als eigenständiger Verantwortlicher betrachtet. Es ist zu beachten, dass innerhalb einer Unternehmensgruppe ein anderes Unternehmen als der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter ein Dritter ist, auch wenn es zur selben Gruppe gehört wie das Unternehmen, das als für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter handelt.

Beispiel: Reinigungsdienste

Unternehmen A schließt einen Vertrag mit einem Reinigungsdienstleister zur Reinigung seiner Büros ab. Die Reinigungskräfte sollen nicht auf personenbezogene Daten zugreifen oder diese anderweitig verarbeiten. Auch wenn sie gelegentlich auf solche Daten stoßen, wenn sie sich im Büro bewegen, können sie ihre Aufgabe ausführen, 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 nicht die Absicht, die Reinigungsfirma oder ihre Mitarbeiter mit der Verarbeitung personenbezogener Daten im Namen von Unternehmen A zu beauftragen. Die Reinigungsfirma und ihre Mitarbeiter sind daher als Dritte zu betrachten, und der für die Verarbeitung Verantwortliche muss dafür sorgen, dass es angemessene Sicherheitsmaßnahmen gibt, um zu verhindern, dass sie Zugang zu Daten haben, und eine Vertraulichkeitsverpflichtung festlegen, falls sie versehentlich auf personenbezogene Daten stoßen

Beispiel: Unternehmensgruppen - Muttergesellschaft und Tochtergesellschaften

Die Unternehmen X und Y sind Teil des Konzerns Z. Die Unternehmen X und Y verarbeiten beide Daten über ihre jeweiligen Mitarbeiter zu Zwecken der Mitarbeiterverwaltung. Zu einem bestimmten Zeitpunkt beschließt die Muttergesellschaft ZZ, Mitarbeiterdaten von allen Tochtergesellschaften anzufordern, um konzernweite Statistiken zu erstellen. Bei der Übermittlung der Daten von den Unternehmen X und Y an ZZ ist letzteres als Dritter zu betrachten, ungeachtet der Tatsache, dass alle Unternehmen Teil desselben Konzerns sind. Unternehmen ZZ wird für seine Verarbeitung der Daten zu statistischen Zwecken als Verantwortlicher angesehen.

[34] Der Arbeitgeber (als ursprünglich für die Verarbeitung Verantwortlicher) könnte dennoch eine gewisse Verantwortung behalten, falls die neue Verarbeitung aufgrund eines Mangels an angemessenen Sicherheitsmaßnahmen erfolgt.

Empfänger

90. Artikel 4 Absatz 9 definiert einen "*Empfänger*" als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der die personenbezogenen Daten offengelegt werden, unabhängig davon, ob es sich um einen Dritten handelt oder nicht. Öffentliche Stellen sind jedoch nicht als Empfänger anzusehen, wenn sie personenbezogene Daten im Rahmen einer bestimmten Untersuchung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erhalten (z. B. Steuer- und Zollbehörden, Finanzermittlungsstellen usw.)[35]

91. Die Definition entspricht im Wesentlichen der bisherigen Definition von "*Empfänger*" in der Richtlinie 95/46/EG.

92. Die Definition umfasst jeden, der personenbezogene Daten erhält, unabhängig davon, ob er ein Dritter ist oder nicht. Wenn beispielsweise ein für die Verarbeitung Verantwortlicher personenbezogene Daten an eine andere Stelle sendet, entweder an einen Auftragsverarbeiter oder an einen Dritten, ist diese Stelle ein Empfänger. Ein Dritter, der Empfänger ist, gilt als für die Verarbeitung Verantwortlicher für jede Verarbeitung, die er für seine eigenen Zwecke durchführt, nachdem er die Daten erhalten hat.

Beispiel: Weitergabe von Daten zwischen Unternehmen

Das Reisebüro ExploreMore arrangiert Reisen auf Anfrage seiner individuellen Kunden. Im Rahmen dieser Dienstleistung übermittelt es die personenbezogenen Daten der Kunden an Fluggesellschaften, Hotels und Ausflugsveranstalter, damit diese ihre jeweiligen Leistungen erbringen können. ExploreMore, die Hotels, Fluggesellschaften und Ausflugsanbieter sind jeweils als für die Verarbeitung Verantwortliche zu betrachten, die sie im Rahmen ihrer jeweiligen Dienstleistungen durchführen. Es gibt keine Controller-Prozessor-Beziehung. Die Fluggesellschaften, Hotels und Ausflugsanbieter sind jedoch als Empfänger zu betrachten, wenn sie die personenbezogenen Daten von ExploreMore erhalten.

TEIL II - FOLGEN DER ZUWEISUNG UNTERSCHIEDLICHER ROLLEN

1 BEZIEHUNG ZWISCHEN CONTROLLER UND PROZESSOR

93. Eine deutliche Neuerung in der DSGVO sind die Bestimmungen, die den Auftragsverarbeitern direkte Pflichten auferlegen. So muss ein Auftragsverarbeiter beispielsweise sicherstellen, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind (Artikel 28 Absatz 3); ein Auftragsverarbeiter muss ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten führen (Artikel 30 Absatz 2) und geeignete technische und organisatorische Maßnahmen ergreifen (Artikel 32). Ein Auftragsverarbeiter muss außerdem unter bestimmten Bedingungen einen Datenschutzbeauftragten benennen (Artikel 37) und hat die Pflicht, den für die Verarbeitung Verantwortlichen unverzüglich zu benachrichtigen, nachdem er von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt hat (Artikel 33 Absatz 2). Darüber hinaus gelten die Vorschriften über die Übermittlung von Daten in Drittländer (Kapitel V) sowohl für Auftragsverarbeiter als auch für für die für die Verarbeitung Verantwortlichen. In diesem Zusammenhang ist der EDSB der Ansicht, dass Artikel 28 Absatz 3 DSGVO zwar einen bestimmten Inhalt für den erforderlichen Vertrag zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter vorschreibt, den Auftragsverarbeitern jedoch direkte Verpflichtungen auferlegt, einschließlich der Pflicht, den für die Verarbeitung Verantwortlichen bei der Einhaltung der Vorschriften zu unterstützen. [36]

1.1 Auswahl des Prozessors

94. Der für die Verarbeitung Verantwortliche hat die **Pflicht, "nur Auftragsverarbeiter einzusetzen, die hinreichende Garantien** für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen bieten", so dass die Verarbeitung den Anforderungen der

[35] Siehe auch Erwägungsgrund 31 der DS-GVO

[36] Beispielsweise sollte der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen bei Bedarf und auf Anfrage bei der Einhaltung der Pflichten im Zusammenhang mit Datenschutz-Folgenabschätzungen unterstützen (Erwägungsgrund 95 DSGVO). Dies muss sich im Vertrag zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter gemäß Artikel 28 Absatz 3 Buchstabe f DSGVO widerspiegeln.

GDPR - auch für die Sicherheit der Verarbeitung - und gewährleistet den Schutz der Rechte der betroffenen Person. [37] Der für die Verarbeitung Verantwortliche ist daher dafür verantwortlich, die Angemessenheit der vom Auftragsverarbeiter gebotenen Garantien zu bewerten und sollte in der Lage sein, nachzuweisen, dass er alle in der DSGVO vorgesehenen Elemente ernsthaft berücksichtigt hat.

95. Die vom Auftragsverarbeiter "geleisteten" Garantien sind diejenigen, die der Auftragsverarbeiter **zur Zufriedenheit des für die Verarbeitung Verantwortlichen nachweisen** kann, da dies die einzigen sind, die der für die Verarbeitung Verantwortliche bei der Beurteilung der Einhaltung seiner Verpflichtungen tatsächlich berücksichtigen kann. Häufig erfordert dies den Austausch relevanter Unterlagen (z. B. Datenschutzpolitik, Nutzungsbedingungen, Aufzeichnungen über Verarbeitungstätigkeiten, Grundsätze der Aktenverwaltung, Grundsätze der Informationssicherheit, Berichte über externe Datenschutzaudits, anerkannte internationale Zertifizierungen wie die ISO 27000-Reihe).

96. Die Beurteilung des für die Verarbeitung Verantwortlichen, ob die Garantien ausreichend sind, ist eine Form der Risikobewertung, die stark von der Art der dem Auftragsverarbeiter anvertrauten Verarbeitung abhängt und von Fall zu Fall unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen vorgenommen werden muss. Infolgedessen kann der EDPB keine erschöpfende Liste der Dokumente oder Maßnahmen vorlegen, die der Auftragsverarbeiter in einem bestimmten Szenario vorlegen oder nachweisen muss, da dies weitgehend von den spezifischen Umständen der Verarbeitung abhängt.

97. Die folgenden Elemente38 sollten von dem für die Verarbeitung Verantwortlichen berücksichtigt werden, um die Angemessenheit der Garantien zu beurteilen: das **Fachwissen** des Auftragsverarbeiters (z. B. technisches Fachwissen in Bezug auf Sicherheitsmaßnahmen und Datenverletzungen); die **Zuverlässigkeit** des Auftragsverarbeiters; die **Ressourcen** des Auftragsverarbeiters. Auch der Ruf des Auftragsverarbeiters auf dem Markt kann ein relevanter Faktor sein, den die für die Verarbeitung Verantwortlichen berücksichtigen müssen.

98. Darüber hinaus kann die Einhaltung eines genehmigten Verhaltenskodex oder Zertifizierungsmechanismus als ein Element verwendet werden, mit dem ausreichende Garantien nachgewiesen werden können. [39] [Den] Auftragsverarbeitern wird daher empfohlen, den für die Verarbeitung Verantwortlichen über diesen Umstand sowie über jede Änderung einer solchen Einhaltung zu informieren.

99. Die in Artikel 28 Absatz 1 DSGVO enthaltene Verpflichtung, nur Auftragsverarbeiter einzusetzen, "die ausreichende Garantien bieten", ist eine fortlaufende Verpflichtung. Sie endet nicht in dem Moment, in dem der Verantwortliche und der Auftragsverarbeiter einen Vertrag oder einen anderen Rechtsakt abschließen. Vielmehr sollte der für die Verarbeitung Verantwortliche in angemessenen Abständen die Garantien des Auftragsverarbeiters überprüfen, gegebenenfalls auch durch Audits und Inspektionen. [40]

1.2 Form des Vertrags oder sonstigen Rechtsakts

100. Jede Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter muss durch einen Vertrag oder einen anderen Rechtsakt nach EU- oder mitgliedstaatlichem Recht zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter geregelt sein, wie in Artikel 28 Absatz 3 DSGVO gefordert.

101. Ein solcher Rechtsakt muss **schriftlich erfolgen, auch in elektronischer Form**. [41] Daher können nicht-schriftliche Vereinbarungen (unabhängig davon, wie gründlich oder wirksam sie sind) nicht als ausreichend angesehen werden, um die in Artikel 28 DSGVO festgelegten Anforderungen zu erfüllen. Um Schwierigkeiten beim Nachweis zu vermeiden, dass der Vertrag oder ein anderer Rechtsakt tatsächlich in Kraft ist, empfiehlt der EDPB sicherzustellen, dass die erforderlichen Unterschriften im Einklang mit dem geltenden Recht (z. B. dem Vertragsrecht) in den Rechtsakt aufgenommen werden.

[37] Artikel 28(1) und Erwägungsgrund 81 DSGVO.
[38] Erwägungsgrund 81 GDPR.
[39] Artikel 28(5) und Erwägungsgrund 81 DSGVO.
[40] Siehe auch Artikel 28(3)h GDPR.
[41] Artikel 28(9) GDPR.

102. Darüber hinaus muss der Vertrag oder der andere Rechtsakt nach Unionsrecht oder dem Recht der Mitgliedstaaten **für den Auftragsverarbeiter gegenüber dem** für die Verarbeitung Verantwortlichen **verbindlich** sein, d. h. er muss für den Auftragsverarbeiter Verpflichtungen begründen, die nach dem Recht der Union oder der Mitgliedstaaten verbindlich sind. Außerdem muss sie die Pflichten des für die Verarbeitung Verantwortlichen darlegen. In den meisten Fällen wird es sich um einen Vertrag handeln, aber die Verordnung verweist auch auf "andere Rechtsakte", wie z. B. ein nationales Gesetz (primär oder sekundär) oder ein anderes Rechtsinstrument. Wenn der Rechtsakt nicht alle erforderlichen Mindestinhalte enthält, muss er durch einen Vertrag oder einen anderen Rechtsakt ergänzt werden, der die fehlenden Elemente enthält.

103. Da die Verordnung eine eindeutige Verpflichtung zum Abschluss eines schriftlichen Vertrags vorsieht, wenn kein anderer einschlägiger Rechtsakt in Kraft ist, stellt das Fehlen eines solchen einen Verstoß gegen die DSGVO dar. [42] Sowohl der für die Verarbeitung Verantwortliche als auch der Auftragsverarbeiter sind dafür verantwortlich, dass es einen Vertrag oder einen anderen Rechtsakt gibt, der die Verarbeitung regelt. [43] Vorbehaltlich der Bestimmungen von Artikel 83 der DSGVO kann die zuständige Aufsichtsbehörde unter Berücksichtigung der Umstände des Einzelfalls ein Bußgeld sowohl gegen den Verantwortlichen als auch gegen den Auftragsverarbeiter verhängen. Verträge, die vor dem Datum des Inkrafttretens der DSGVO geschlossen wurden, sollten im Lichte von Artikel 28(3) aktualisiert worden sein. Das Fehlen einer solchen Aktualisierung, um einen zuvor bestehenden Vertrag mit den Anforderungen der DSGVO in Einklang zu bringen, stellt einen Verstoß gegen Artikel 28(3) dar.

Ein schriftlicher Vertrag gemäß Artikel 28(3) DSGVO kann in einen umfassenderen Vertrag eingebettet sein, z. B. in eine Dienstgütevereinbarung. Um den Nachweis der Einhaltung der DSGVO zu erleichtern, empfiehlt der EDPB, dass die Vertragsbestandteile, die Artikel 28 DSGVO Wirkung verleihen sollen, an einer Stelle (z. B. in einem Anhang) klar als solche gekennzeichnet werden.

104. Um der Pflicht zum Abschluss eines Vertrags nachzukommen, **können der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter wählen, ob sie einen eigenen Vertrag aushandeln**, der alle obligatorischen Elemente enthält**, oder ob sie sich ganz oder teilweise auf Standardvertragsklauseln in Bezug auf die Verpflichtungen gemäß Artikel 28 stützen**.[44]

[42] Das Vorhandensein (oder Nichtvorhandensein) einer schriftlichen Vereinbarung ist jedoch nicht ausschlaggebend für das Bestehen eines Auftragsverarbeiter-Verhältnis. Wenn es Grund zu der Annahme gibt, dass der Vertrag in Bezug auf die tatsächliche Kontrolle nicht der Realität entspricht, kann die Vereinbarung auf der Grundlage einer Tatsachenanalyse der Umstände, die die Beziehung zwischen den Parteien und die durchgeführte Verarbeitung personenbezogener Daten umgeben, aufgehoben werden. Umgekehrt kann eine Beziehung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter auch dann als gegeben angesehen werden, wenn kein schriftlicher Verarbeitungsvertrag vorliegt. Dies würde jedoch einen Verstoß gegen Artikel 28(3) DSGVO bedeuten. Darüber hinaus kann das Fehlen einer klaren Definition der Beziehung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter unter bestimmten Umständen das Problem des Fehlens einer Rechtsgrundlage aufwerfen, auf die sich jede Verarbeitung stützen sollte, z. B. in Bezug auf die Übermittlung von Daten zwischen dem für die Verarbeitung Verantwortlichen und dem angeblichen Auftragsverarbeiter.

[43] Artikel 28(3) ist nicht nur auf für die Verarbeitung Verantwortliche anwendbar. In der Situation, in der nur der Auftragsverarbeiter dem territorialen Anwendungsbereich der DSGVO unterliegt, gilt die Verpflichtung nur für den Auftragsverarbeiter unmittelbar, siehe auch EDPB-Leitlinien 3/2018 zum territorialen Anwendungsbereich der DSGVO, S. 12.

[44] Artikel 28(6) DSGVO. Der EDSB erinnert daran, dass Standardvertragsklauseln für die Zwecke der Einhaltung von Artikel 28 DSGVO nicht dasselbe sind wie die in Artikel 46 Absatz 2 genannten Standardvertragsklauseln. Während erstere weiter festlegen und klarstellen, wie die Bestimmungen von Artikel 28 Absätze 3 und 4 erfüllt werden, bieten letztere angemessene Garantien für den Fall der Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation bei Fehlen eines Angemessenheitsbeschlusses gemäß Artikel 45 Absatz 3.

105. Eine Reihe von Standardvertragsklauseln (SCC) kann alternativ von der Kommission45 oder von einer Aufsichtsbehörde im Einklang mit dem Kohärenzverfahren angenommen werden. [46] Diese Klauseln könnten Teil einer Zertifizierung sein, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 oder 43 erteilt wird.[47]

106. Der EDSB möchte klarstellen, dass es keine Verpflichtung für für die Verarbeitung Verantwortliche und Auftragsverarbeiter gibt, einen Vertrag auf der Grundlage von SCCs abzuschließen, noch ist dies notwendigerweise der Aushandlung eines individuellen Vertrags vorzuziehen. Beide Optionen sind für die Zwecke der Einhaltung des Datenschutzrechts je nach den spezifischen Umständen praktikabel, solange sie die Anforderungen von Artikel 28 Absatz 3 erfüllen.

107. Wenn die Parteien die Vorteile von Standardvertragsklauseln nutzen möchten, müssen die Datenschutzklauseln ihrer Vereinbarung mit denen der SCCs übereinstimmen. Die SCCs lassen oft einige Leerstellen, die ausgefüllt werden müssen, oder Optionen, die von den Parteien ausgewählt werden können. Wie bereits erwähnt, sind die SCC in der Regel in eine umfassendere Vereinbarung eingebettet, in der der Vertragsgegenstand, die finanziellen Bedingungen und andere vereinbarte Klauseln beschrieben werden: Die Parteien können zusätzliche Klauseln (z. B. über das anwendbare Recht und den Gerichtsstand) hinzufügen, solange diese weder direkt noch indirekt den SCC widersprechen48 und den durch die DSGVO und die Datenschutzgesetze der EU oder der Mitgliedstaaten gewährleisteten Schutz nicht untergraben.

108. Verträge zwischen Verantwortlichen und Auftragsverarbeitern können manchmal einseitig von einer der Parteien aufgesetzt werden. Welche Partei(en) den Vertrag entwirft/entwerfen, kann von mehreren Faktoren abhängen, u. a. von der Stellung der Parteien auf dem Markt und ihrer Vertragsmacht, ihrem technischen Fachwissen sowie dem Zugang zu Rechtsdienstleistungen. Beispielsweise neigen einige Dienstanbieter dazu, Standardbedingungen aufzustellen, die Datenverarbeitungsverträge enthalten.

109. Eine Vereinbarung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter muss die Anforderungen von Artikel 28 DSGVO erfüllen, um sicherzustellen, dass der Auftragsverarbeiter personenbezogene Daten in Übereinstimmung mit der DSGVO verarbeitet. Jede derartige Vereinbarung sollte die spezifischen Verantwortlichkeiten von für die Verarbeitung Verantwortlichen und Auftragsverarbeitern berücksichtigen. Obwohl Artikel 28 eine Liste von Punkten enthält, die in jedem Vertrag, der die Beziehung zwischen Verantwortlichen und Auftragsverarbeitern regelt, angesprochen werden müssen, lässt er Raum für Verhandlungen zwischen den Parteien solcher Verträge. In manchen Situationen kann ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter in einer schwächeren Verhandlungsposition sein, um den Datenschutzvertrag anzupassen. Der Rückgriff auf die gemäß Artikel 28 (Absätze 7 und 8) angenommenen Standardvertragsklauseln kann dazu beitragen, die Verhandlungspositionen auszugleichen und sicherzustellen, dass die Verträge die DSGVO einhalten.

---

[45] Artikel 28(7) GDPR. Artikel 28(7) DS-GVO. Artikel 28(7) DS-GVO. Artikel 28(7) DSGVO. Siehe die gemeinsame Stellungnahme des EDSB und des EDSB1/2021 zu Standardvertragsklauseln zwischen für die Verarbeitung 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(8) GDPR. 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 Art. 28 DSGVO, kann hier eingesehen werden: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for- decisions_de.

[47] Artikel 28(6) GDPR.

[48] Der EDSB erinnert daran, dass das gleiche Maß an Flexibilität erlaubt ist, wenn sich die Parteien für die Verwendung von SCCs als geeignete Schutzmaßnahmen für Übermittlungen in Drittländer gemäß Artikel 46 Absatz 2 Buchstabe c oder Artikel 46 Absatz 2 Buchstabe d DSGVO entscheiden. Erwägungsgrund 109 DSGVO stellt klar: "*Die Möglichkeit für den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter, von der Kommission oder einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln zu verwenden, sollte den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter weder daran hindern, die Standarddatenschutzklauseln in einen umfassenderen Vertrag aufzunehmen, z. B. in einen Vertrag zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, noch andere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese nicht direkt oder indirekt im Widerspruch zu den Standardvertragsklauseln stehen [...] oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beeinträchtigen. Die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter sollten ermutigt werden, über vertragliche Verpflichtungen, die die Standardschutzklauseln ergänzen, zusätzliche Garantien vorzusehen*".

110. Die Tatsache, dass der Vertrag und seine detaillierten Geschäftsbedingungen vom Diensteanbieter und nicht vom für die Verarbeitung Verantwortlichen erstellt werden, ist an sich nicht problematisch und stellt an sich keine ausreichende Grundlage für die Schlussfolgerung dar, dass der Diensteanbieter als für die Verarbeitung Verantwortlicher betrachtet werden sollte. Auch das Ungleichgewicht in der Vertragsmacht eines kleinen für die Verarbeitung Verantwortlichen gegenüber großen Dienstanbietern sollte nicht als Rechtfertigung dafür angesehen werden, dass der für die Verarbeitung Verantwortliche Klauseln und Vertragsbedingungen akzeptiert, die nicht im Einklang mit dem Datenschutzrecht stehen, noch kann es den für die Verarbeitung Verantwortlichen von seinen Datenschutzpflichten entbinden. Der für die Verarbeitung Verantwortliche muss die Bedingungen bewerten, und insofern er sie freiwillig akzeptiert und den Dienst in Anspruch nimmt, hat er auch die volle Verantwortung für die Einhaltung der DSGVO übernommen. Jede von einem Auftragsverarbeiter vorgeschlagene Änderung von Datenverarbeitungsvereinbarungen, die in den Allgemeinen Geschäftsbedingungen enthalten sind, sollte dem für die Verarbeitung Verantwortlichen direkt mitgeteilt und von diesem genehmigt werden, wobei der Spielraum zu berücksichtigen ist, den der Auftragsverarbeiter in Bezug auf nicht wesentliche Elemente des Mittels genießt (siehe Paragraphen 40-41 oben). Die bloße Veröffentlichung dieser Änderungen auf der Website des Auftragsverarbeiters steht nicht im Einklang mit Artikel 28.

1.3 Inhalt des Vertrags oder anderer Rechtsakte

111. Bevor auf die einzelnen detaillierten Anforderungen der DSGVO an den Inhalt des Vertrags oder eines anderen Rechtsakts eingegangen wird, sind einige allgemeine Anmerkungen erforderlich.

112. Während die in Artikel 28 der Verordnung festgelegten Elemente deren Kerninhalt darstellen, sollte der Vertrag für den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter eine Möglichkeit sein, weiter zu klären, wie diese Kernelemente mit detaillierten Anweisungen umgesetzt werden sollen. Daher **sollte der Verarbeitungsvertrag nicht einfach nur die Bestimmungen der DSGVO wiedergeben**: Er sollte vielmehr spezifischere, konkrete Informationen darüber enthalten, wie die Anforderungen erfüllt werden und welches Sicherheitsniveau für die Verarbeitung personenbezogener Daten, die Gegenstand des Verarbeitungsvertrags ist, erforderlich ist. Weit davon entfernt, eine Pro-forma-Übung zu sein, sind die Verhandlung und die Festlegung des Vertrags eine Chance, Details bezüglich der Verarbeitung zu spezifizieren. [49] In der Tat erfordert der "Schutz der Rechte und Freiheiten der betroffenen Personen sowie die Verantwortung und Haftung der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter [...] eine klare Zuweisung der Verantwortlichkeiten" gemäß der DSGVO. [50]

113. Gleichzeitig sollte der Vertrag **"*die spezifischen Aufgaben und Verantwortlichkeiten des Auftragsverarbeiters im Zusammenhang mit der durchzuführenden Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person*" berücksichtigen**. [51] Generell sollte der Vertrag zwischen den Parteien im Hinblick auf die spezifische Datenverarbeitungstätigkeit abgefasst werden. So besteht beispielsweise keine Notwendigkeit, 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 in der Verordnung festgelegten Anforderungen erfüllen, doch sollten die Maßnahmen und Verfahren auf die jeweilige Situation zugeschnitten sein. In jedem Fall müssen alle Elemente von Artikel 28 Absatz 3 durch den Vertrag abgedeckt sein. Gleichzeitig sollte der Vertrag einige Elemente enthalten, die dem Auftragsverarbeiter helfen können, die Risiken für die Rechte und Freiheiten der betroffenen Personen, die sich aus der Verarbeitung ergeben, zu verstehen: Da die Tätigkeit im Auftrag des für die Verarbeitung Verantwortlichen durchgeführt wird, hat der für die Verarbeitung Verantwortliche oft ein tieferes Verständnis für die Risiken, die die Verarbeitung mit sich bringt, da er die Umstände kennt, in die die Verarbeitung eingebettet ist.

114. Was den **erforderlichen Inhalt** des Vertrags oder sonstigen Rechtsakts betrifft, so legt der EDPB Artikel 28 Absatz 3 so aus, dass er dargelegt werden muss:

[49] Siehe auch EDPB-Stellungnahme 14/2019 zu dem von der DK SA vorgelegten Entwurf von Standardvertragsklauseln (Artikel 28(8) DSGVO), S. 5.
[50] Erwägungsgrund 79 GDPR.
[51] Erwägungsgrund 81 GDPR.

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

- die **Dauer**[52] der Verarbeitung: Der genaue Zeitraum oder die Kriterien, nach denen er bestimmt wird, sollten angegeben werden; beispielsweise könnte auf die Dauer der Verarbeitungsvereinbarung Bezug genommen werden;

- die **Art** der Verarbeitung: die Art der im Rahmen der Verarbeitung durchgeführten Vorgänge (z. B. "Filmen", "Aufzeichnen", "Archivieren von Bildern", ...) **und der Zweck** der Verarbeitung (z. B. Aufdecken von unrechtmäßigem Betreten). Diese Beschreibung sollte je nach spezifischer 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**: Diese sollte so detailliert wie möglich angegeben werden (zum Beispiel: Videobilder von Personen beim Betreten und Verlassen der Einrichtung). Es wäre nicht ausreichend, lediglich anzugeben, dass es sich um "personenbezogene Daten gemäß Artikel 4 Absatz 1 DSGVO" oder "besondere Kategorien personenbezogener Daten gemäß Artikel 9" handelt. Bei besonderen Datenkategorien sollte im Vertrag oder Rechtsakt zumindest angegeben werden, welche Arten von Daten betroffen sind, z. B. "Informationen über Gesundheitsdaten" oder "Informationen darüber, ob die betroffene Person Mitglied einer Gewerkschaft ist";

- die **Kategorien der betroffenen Personen**: auch dies sollte ganz konkret angegeben werden (z. B. "Besucher", "Mitarbeiter", Lieferdienste usw.);

- die **Pflichten und Rechte des für die Verarbeitung Verantwortlichen**: Auf die Rechte des für die Verarbeitung Verantwortlichen wird in den folgenden Abschnitten näher eingegangen (z. B. in Bezug auf das Recht des für die Verarbeitung Verantwortlichen, Inspektionen und Audits durchzuführen). Zu den Pflichten des für die Verarbeitung Verantwortlichen gehören beispielsweise die Verpflichtung des für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter die im Vertrag genannten Daten zur Verfügung zu stellen, alle Anweisungen, die sich auf die Verarbeitung von Daten durch den Auftragsverarbeiter beziehen, zu erteilen und zu dokumentieren, vor und während der Verarbeitung die Einhaltung der in der DSGVO festgelegten Pflichten des Auftragsverarbeiters sicherzustellen, die Verarbeitung zu überwachen, auch durch die Durchführung von Audits und Inspektionen beim Auftragsverarbeiter.

115. Während die DSGVO Elemente auflistet, die immer in die Vereinbarung aufgenommen werden müssen, müssen je nach Kontext und den Risiken der Verarbeitung sowie je nach zusätzlichen anwendbaren Anforderungen möglicherweise weitere relevante Informationen aufgenommen werden.

1.3.1 Der Auftragsverarbeiter darf Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten (Art. 28(3)(a) GDPR)

116. Die Notwendigkeit, diese Verpflichtung zu spezifizieren, ergibt sich aus der Tatsache, dass der Auftragsverarbeiter Daten im Auftrag des Verantwortlichen verarbeitet. Der für die Verarbeitung Verantwortliche muss seinen Auftragsverarbeitern Anweisungen in Bezug auf jede Verarbeitungstätigkeit geben. Solche Anweisungen können den zulässigen und unzulässigen Umgang mit personenbezogenen Daten, detailliertere Verfahren, Möglichkeiten der Datensicherung usw. umfassen. Der Auftragsverarbeiter darf nicht über das hinausgehen, was der für die Verarbeitung Verantwortliche angewiesen hat. Es ist jedoch möglich, dass der Auftragsverarbeiter Elemente vorschlägt, die, wenn sie von dem für die Verarbeitung Verantwortlichen akzeptiert werden, Teil der erteilten Anweisungen werden.

[52] Die Dauer der Verarbeitung entspricht nicht notwendigerweise der Dauer der Vereinbarung (es können gesetzliche Verpflichtungen bestehen, die Daten länger oder kürzer aufzubewahren).

117. Wenn ein Auftragsverarbeiter Daten außerhalb oder über die Weisungen des für die Verarbeitung Verantwortlichen hinaus verarbeitet und dies auf eine Entscheidung hinausläuft, mit der die Zwecke und Mittel der Verarbeitung festgelegt werden, verstößt der Auftragsverarbeiter gegen seine Pflichten und wird in Bezug auf diese Verarbeitung sogar als für die Verarbeitung Verantwortlicher im Sinne von Artikel 28 Absatz 10 betrachtet (siehe Unterabschnitt 1.5 unten53).

118. Die vom für die Verarbeitung Verantwortlichen erteilten Anweisungen müssen **dokumentiert** werden. Für diese Zwecke wird empfohlen, ein Verfahren und eine Vorlage für die Erteilung weiterer Anweisungen in einen Anhang zum Vertrag oder einem anderen Rechtsakt aufzunehmen. Alternativ können die Anweisungen in jeder schriftlichen Form (z. B. per E-Mail) sowie in jeder anderen dokumentierten Form erteilt werden, solange es möglich ist, Aufzeichnungen über diese Anweisungen zu führen. Um Schwierigkeiten beim Nachweis zu vermeiden, dass die Anweisungen des für die Verarbeitung Verantwortlichen ordnungsgemäß dokumentiert wurden, empfiehlt der EDSB in jedem Fall, solche Anweisungen zusammen mit dem Vertrag oder einem anderen Rechtsakt aufzubewahren.

119. Die Pflicht des Auftragsverarbeiters, jede Verarbeitungstätigkeit zu unterlassen, die nicht auf den Anweisungen des für die Verarbeitung Verantwortlichen beruht, gilt auch für die **Übermittlung** personenbezogener Daten an ein Drittland oder eine internationale Organisation. Im Vertrag sollten die Anforderungen für Übermittlungen an Drittländer oder internationale Organisationen festgelegt werden, wobei die Bestimmungen von Kapitel V der DSGVO zu berücksichtigen sind.

120. Der EDSB empfiehlt, dass der für die Verarbeitung Verantwortliche diesem speziellen Punkt gebührende Aufmerksamkeit schenkt, insbesondere wenn der Auftragsverarbeiter einige Verarbeitungstätigkeiten an andere Auftragsverarbeiter delegieren wird und wenn der Auftragsverarbeiter Abteilungen oder Einheiten in Drittländern hat. Wenn die Anweisungen des für die Verarbeitung Verantwortlichen keine Übertragungen oder Offenlegungen in Drittländer zulassen, darf der Auftragsverarbeiter die Verarbeitung nicht an einen Unterauftragsverarbeiter in einem Drittland übertragen, 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 für die Verarbeitung Verantwortlichen verarbeiten**, wenn der Auftragsverarbeiter auf der Grundlage von EU-Recht oder dem Recht der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, verpflichtet ist, personenbezogene Daten zu verarbeiten und/oder zu übermitteln**. Diese Bestimmung macht deutlich, wie wichtig es ist, Datenverarbeitungsverträge sorgfältig auszuhandeln und abzufassen, da z. B. beide Parteien möglicherweise Rechtsrat einholen müssen, um festzustellen, ob eine solche rechtliche Verpflichtung besteht. Dies muss rechtzeitig geschehen, da der Auftragsverarbeiter verpflichtet ist, den für die Verarbeitung Verantwortlichen vor Beginn der Verarbeitung über eine solche Anforderung zu informieren. Nur wenn dasselbe (EU- oder mitgliedstaatliche) Recht dem Auftragsverarbeiter verbietet, den für die Verarbeitung Verantwortlichen aus "wichtigen Gründen des öffentlichen Interesses" zu informieren, besteht keine solche Informationspflicht. In jedem Fall darf eine Übermittlung oder Offenlegung nur dann erfolgen, wenn sie nach dem Unionsrecht, auch gemäß Artikel 48 der DSGVO, zulässig ist.

1.3.2 Der Auftragsverarbeiter muss sicherstellen, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28(3)(b) GDPR)

122. Im Vertrag muss festgelegt werden, dass der Auftragsverarbeiter sicherstellen muss, dass jeder, dem er die Verarbeitung der personenbezogenen Daten erlaubt, zur Vertraulichkeit verpflichtet ist. Dies kann entweder über eine spezifische vertragliche Vereinbarung oder aufgrund bereits bestehender gesetzlicher Verpflichtungen geschehen.

123. Der weite Begriff der "zur Verarbeitung der personenbezogenen Daten befugten Personen" umfasst auch Angestellte und Zeitarbeiter. Generell sollte der Auftragsverarbeiter die personenbezogenen Daten nur den Mitarbeitern zur Verfügung stellen, die sie tatsächlich zur Erfüllung der Aufgaben benötigen, für die der Auftragsverarbeiter vom Verantwortlichen eingestellt wurde.

[53] Siehe Teil II, Unterabschnitt 1.5 ("Der Auftragsverarbeiter bestimmt die Zwecke und Mittel der Verarbeitung").

124. Die Zusage oder Verpflichtung zur Vertraulichkeit muss "angemessen" sein, d. h. sie muss der befugten Person die unbefugte Weitergabe vertraulicher Informationen wirksam untersagen, und sie muss so weit gefasst sein, dass sie alle im Auftrag des für die Verarbeitung Verantwortlichen verarbeiteten personenbezogenen Daten sowie die Bedingungen, unter denen die personenbezogenen Daten verarbeitet werden, umfasst.

1.3.3 Der Auftragsverarbeiter muss alle Maßnahmen ergreifen, die gemäß Artikel 32 erforderlich sind (Art. 28(3)(c) GDPR)

125. Artikel 32 verpflichtet den Verantwortlichen und den Auftragsverarbeiter, geeignete technische und organisatorische Sicherheitsmaßnahmen zu ergreifen. Während diese Verpflichtung bereits direkt dem Auftragsverarbeiter auferlegt wird, dessen Verarbeitungsvorgänge in den Anwendungsbereich der DSGVO fallen, muss sich die Pflicht, alle gemäß Artikel 32 erforderlichen Maßnahmen zu ergreifen, noch in dem Vertrag über die von dem für die Verarbeitung Verantwortlichen übertragenen Verarbeitungstätigkeiten widerspiegeln.

126. Wie bereits erwähnt, sollte der Verarbeitungsvertrag nicht nur die Bestimmungen der DSGVO wiedergeben. Der Vertrag muss Informationen über die zu ergreifenden Sicherheitsmaßnahmen enthalten oder auf diese verweisen**, eine Verpflichtung des Auftragsverarbeiters, vor Änderungen die Zustimmung des für die Verarbeitung Verantwortlichen einzuholen**, und eine regelmäßige Überprüfung der Sicherheitsmaßnahmen, um ihre Angemessenheit im Hinblick auf Risiken, die sich im Laufe der Zeit entwickeln können, zu gewährleisten. Der Detaillierungsgrad der Informationen über die in den Vertrag aufzunehmenden Sicherheitsmaßnahmen muss so beschaffen sein, dass der für die Verarbeitung Verantwortliche die Angemessenheit der Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO beurteilen kann. Darüber hinaus ist die Beschreibung auch erforderlich, damit der für die Verarbeitung 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 für die Verarbeitung Verantwortlichen zu unterstützen und alle Informationen zur Verfügung zu stellen, die für den Nachweis der Einhaltung erforderlich sind, ergibt sich aus Art. 28.3 (f) und (h) DS-GVO ableiten.

127. Der Grad der Anweisungen, die der für die Verarbeitung Verantwortliche dem Auftragsverarbeiter hinsichtlich der zu ergreifenden Maßnahmen erteilt, hängt von den jeweiligen Umständen ab. In einigen Fällen kann die Steuerung eine klare und detaillierte Beschreibung der zu implementierenden Sicherheitsmaßnahmen liefern. In anderen Fällen kann der für die Verarbeitung Verantwortliche die zu erreichenden Mindestsicherheitsziele beschreiben und gleichzeitig den Auftragsverarbeiter auffordern, die Durchführung spezifischer Sicherheitsmaßnahmen vorzuschlagen. In jedem Fall muss der für die Verarbeitung Verantwortliche dem Auftragsverarbeiter eine Beschreibung der Verarbeitungstätigkeiten und der Sicherheitsziele (auf der Grundlage der Risikobewertung des für die Verarbeitung Verantwortlichen) vorlegen und die vom Auftragsverarbeiter vorgeschlagenen Maßnahmen genehmigen. Dies könnte in einen Anhang zum Vertrag aufgenommen werden. Der für die Verarbeitung Verantwortliche übt seine Entscheidungsbefugnis über die wesentlichen Merkmale der Sicherheitsmaßnahmen aus, sei es durch ausdrückliche Auflistung der Maßnahmen oder durch Genehmigung der vom Auftragsverarbeiter vorgeschlagenen Maßnahmen.

1.3.4 Der Auftragsverarbeiter muss die in Artikel 28 Absatz 2 und 4 genannten Bedingungen für die Beauftragung eines anderen Auftragsverarbeiters einhalten (Art. 28 Absatz 3 Buchstabe d DSGVO).

128. In der Vereinbarung muss festgelegt werden, dass der Auftragsverarbeiter keinen anderen Auftragsverarbeiter ohne die vorherige schriftliche Genehmigung des für die Verarbeitung Verantwortlichen beauftragen darf und ob diese Genehmigung spezifisch oder allgemein sein wird. Im Falle einer allgemeinen Genehmigung muss der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen über jeden Wechsel von Unterauftragsverarbeitern im Rahmen einer schriftlichen Genehmigung informieren und dem für die Verarbeitung Verantwortlichen die Möglichkeit zum Widerspruch geben. Es wird empfohlen, das Verfahren hierfür im Vertrag zu regeln. Es ist zu beachten, dass die Pflicht des Auftragsverarbeiters, den für die Verarbeitung Verantwortlichen über jeden Wechsel von Unterauftragsverarbeitern zu informieren, impliziert, dass der Auftragsverarbeiter aktiv

solche Änderungen gegenüber dem für die Verarbeitung Verantwortlichen anzeigt oder kennzeichnet. [54] Wenn eine besondere Genehmigung erforderlich ist, sollte der Vertrag auch das Verfahren zur Erlangung dieser Genehmigung festlegen.

129. Wenn der Auftragsverarbeiter einen anderen Auftragsverarbeiter beauftragt, muss zwischen ihnen ein Vertrag geschlossen werden, der ihnen dieselben Datenschutzverpflichtungen auferlegt wie dem ursprünglichen Auftragsverarbeiter, oder diese Verpflichtungen müssen durch einen anderen Rechtsakt nach dem Unionsrecht oder dem Recht eines Mitgliedstaats auferlegt werden (siehe auch unten Nummer 160). Dazu gehört auch die Verpflichtung nach Artikel 28 Absatz 3 Buchstabe h, Prüfungen durch den für die Verarbeitung Verantwortlichen oder einen anderen von ihm beauftragten Prüfer zuzulassen und daran mitzuwirken. [55] Der Auftragsverarbeiter haftet gegenüber dem für die Verarbeitung Verantwortlichen für die Einhaltung der Datenschutzverpflichtungen durch die anderen Auftragsverarbeiter (für weitere Einzelheiten zum empfohlenen Inhalt der Vereinbarung siehe Unterabschnitt 1.6 unten56).

1.3.5 Der Auftragsverarbeiter muss den für die Verarbeitung Verantwortlichen bei der Erfüllung seiner Verpflichtung zur Beantwortung von Anfragen zur Ausübung der Rechte der betroffenen Person unterstützen (Artikel 28 Absatz 3 Buchstabe e DSGVO).

130. Während es Sache des für die Verarbeitung Verantwortlichen ist, dafür zu sorgen, dass die Anfragen der betroffenen Personen bearbeitet werden, muss im Vertrag festgelegt werden, dass der Auftragsverarbeiter verpflichtet ist, "durch geeignete technische und organisatorische Maßnahmen Unterstützung zu leisten, soweit dies möglich ist". Die Art dieser Unterstützung kann "unter Berücksichtigung der Art der Verarbeitung" und in Abhängigkeit von der Art der dem Auftragsverarbeiter übertragenen Tätigkeit sehr unterschiedlich sein. Die Einzelheiten bezüglich der vom Auftragsverarbeiter zu leistenden Unterstützung sollten in den Vertrag oder in einen Anhang zu diesem aufgenommen werden.

131. Während die Unterstützung einfach darin bestehen kann, jede eingegangene Anfrage unverzüglich weiterzuleiten und/oder den für die Verarbeitung Verantwortlichen in die Lage zu versetzen, die betreffenden personenbezogenen Daten direkt zu extrahieren und zu verwalten, werden dem Auftragsverarbeiter unter Umständen spezifischere, technische Aufgaben übertragen, insbesondere wenn er in der Lage ist, die personenbezogenen Daten zu extrahieren und zu verwalten.

132. Es ist von entscheidender Bedeutung zu bedenken, dass, obwohl die praktische Verwaltung einzelner Anfragen an den Auftragsverarbeiter ausgelagert werden kann, der für die Verarbeitung Verantwortliche die Verantwortung für die Befolgung solcher Anfragen trägt. Daher sollte die Beurteilung, ob Anträge von betroffenen Personen zulässig sind und/oder die Anforderungen der DSGVO erfüllt sind, von dem für die Verarbeitung Verantwortlichen vorgenommen werden, entweder auf Einzelfallbasis oder durch klare Anweisungen, die dem Auftragsverarbeiter im Vertrag vor Beginn der Verarbeitung gegeben werden. Auch die in Kapitel III festgelegten Fristen können von dem für die Verarbeitung Verantwortlichen nicht mit der Begründung verlängert werden, dass die erforderlichen Informationen vom Auftragsverarbeiter bereitgestellt werden müssen.

1.3.6 Der Auftragsverarbeiter muss den für die Verarbeitung Verantwortlichen bei der Erfüllung der Pflichten nach den Artikeln 32 bis 36 unterstützen (Art. 28 Abs. 3 Buchstabe f) DSGVO).

133. **Es ist** notwendig, dass der Vertrag diese Unterstützungspflichten nicht einfach nur wiedergibt: **Der Vertrag sollte Einzelheiten darüber enthalten, wie der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen bei der Erfüllung der aufgeführten Pflichten unterstützen soll**. Beispielsweise können in den Anhängen der Vereinbarung Verfahren und Musterformulare hinzugefügt werden, die es dem Auftragsverarbeiter ermöglichen, dem für die Verarbeitung Verantwortlichen alle erforderlichen Informationen zur Verfügung zu stellen.

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*" stark variieren. Der Verantwortliche muss

---

[54] In dieser Hinsicht reicht es dagegen z. B. nicht aus, wenn der Prozessor dem Controller lediglich einen verallgemeinerten Zugang zu einer Liste der Unterprozessoren verschafft, die von Zeit zu Zeit aktualisiert werden könnte, ohne auf jeden neuen vorgesehenen Unterprozessor hinzuweisen. Mit anderen Worten: Der Prozessor muss die Steuerung aktiv über jede Änderung der Liste (d. h. insbesondere über jeden neuen vorgesehenen Sub-Prozessor) informieren.

[55] Siehe auch EDPB-Stellungnahme 14/2019 zu dem von der DK SA vorgelegten Entwurf von Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO), 9. Juli 2019, Randnummer 44.

[56] Siehe Teil II, Unterabschnitt 1.6 ("Unterauftragsverarbeiter").

den Auftragsverarbeiter angemessen über das mit der Verarbeitung verbundene Risiko und über alle anderen Umstände zu informieren, die dem Auftragsverarbeiter helfen können, seiner Pflicht nachzukommen.

135. Zu den spezifischen Pflichten: Der Auftragsverarbeiter hat zunächst die Pflicht, den für die Verarbeitung Verantwortlichen bei der Erfüllung der Pflicht zu unterstützen, angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu treffen. [57] Obwohl sich dies bis zu einem gewissen Grad mit der Anforderung überschneiden kann, dass der Auftragsverarbeiter selbst angemessene Sicherheitsmaßnahmen ergreift, wenn die Verarbeitungsvorgänge des Auftragsverarbeiters in den Anwendungsbereich der DSGVO fallen, bleiben es zwei unterschiedliche Verpflichtungen, da sich die eine auf die eigenen Maßnahmen des Auftragsverarbeiters und die andere auf die des Verantwortlichen bezieht.

136. Zweitens muss der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen bei der Erfüllung der Verpflichtung zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und an die betroffenen Personen unterstützen. Der Auftragsverarbeiter muss den für die Verarbeitung Verantwortlichen benachrichtigen, wenn er eine Verletzung des Schutzes personenbezogener Daten entdeckt, die die Einrichtungen/IT-Systeme des Auftragsverarbeiters oder eines Unterauftragsverarbeiters betrifft, und dem für die Verarbeitung Verantwortlichen bei der Beschaffung der Informationen helfen, die in der Meldung an die Aufsichtsbehörde angegeben werden müssen. [58] Die DSGVO verlangt, dass der für die Verarbeitung Verantwortliche eine Verletzung ohne unangemessene Verzögerung meldet, um den Schaden für den Einzelnen zu minimieren und die Möglichkeit zu maximieren, die Verletzung in angemessener Weise zu beheben. Daher sollte die Benachrichtigung des Auftragsverarbeiters an den für die Datenverarbeitung Verantwortlichen ebenfalls ohne unangemessene Verzögerung erfolgen. [59] Je nach den Besonderheiten der dem Auftragsverarbeiter anvertrauten Verarbeitung kann es für die Parteien angemessen sein, im Vertrag einen bestimmten Zeitrahmen (z. B. Anzahl der Stunden) festzulegen, innerhalb dessen der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen benachrichtigen sollte, sowie die Kontaktstelle für solche Benachrichtigungen, die Modalität und den vom für die Verarbeitung Verantwortlichen erwarteten Mindestinhalt. [60] Die vertragliche Vereinbarung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter kann auch eine Ermächtigung und eine Verpflichtung für den Auftragsverarbeiter enthalten, eine Datenschutzverletzung gemäß Artikel 33 und 34 direkt zu melden, aber die rechtliche Verantwortung für die Meldung verbleibt bei dem für die Verarbeitung Verantwortlichen. [61] Wenn der Auftragsverarbeiter eine Datenschutzverletzung direkt bei der Aufsichtsbehörde meldet und die betroffenen Personen gemäß Artikel 33 und 34 informiert, muss der Auftragsverarbeiter auch den für die Verarbeitung Verantwortlichen informieren und dem für die Verarbeitung Verantwortlichen Kopien der Meldung und Informationen für die betroffenen Personen zur Verfügung stellen.

137. Darüber hinaus muss der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen bei Bedarf bei der Durchführung von Datenschutz-Folgenabschätzungen und bei der Konsultation der Aufsichtsbehörde unterstützen, wenn das Ergebnis zeigt, 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 für die Verarbeitung Verantwortlichen auferlegt werden. Obwohl beispielsweise die Datenschutz-Folgenabschätzung in der Praxis von einem Auftragsverarbeiter durchgeführt werden kann, bleibt der für die Verarbeitung Verantwortliche für die Pflicht zur Durchführung der Abschätzung verantwortlich62 und der Auftragsverarbeiter ist nur verpflichtet, den für die Verarbeitung Verantwortlichen zu unterstützen, "wenn dies erforderlich ist und auf Anfrage".[63] Folglich ist der für die Verarbeitung Verantwortliche derjenige, der die Initiative zur Durchführung der Datenschutz-Folgenabschätzung ergreifen muss, nicht der Auftragsverarbeiter.

---

[57] Artikel 32 GDPR.

[58] Artikel 33(3) GDPR.

[59] Weitere Informationen finden Sie in den Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6. Februar 2018, S. 13-14.

[60] Siehe auch EDPB-Stellungnahme 14/2019 zu dem von der DK SA vorgelegten Entwurf von Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO), 9. Juli 2019, Randnummer 40.

[61] Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6. Februar 2018, S. 14.

[62] Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DPIA) und zur Bestimmung, ob die Verarbeitung "wahrscheinlich zu einem hohen Risiko führt" im Sinne der Verordnung 2016/679, WP 248 rev.01, S. 14

[63] Erwägungsgrund 95 GDPR.

1.3.7 Bei Beendigung der Verarbeitungstätigkeiten muss der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten löschen oder an den Verantwortlichen zurückgeben und vorhandene Kopien löschen (Art. 28(3)(g) GDPR).

139. Die Vertragsbedingungen sollen sicherstellen, dass die personenbezogenen Daten nach dem Ende der "Erbringung von Dienstleistungen im Zusammenhang mit der Verarbeitung" einem angemessenen Schutz unterliegen: Es obliegt daher dem für die Verarbeitung Verantwortlichen zu entscheiden, was der Auftragsverarbeiter mit den personenbezogenen Daten tun soll.

140. Der für die Verarbeitung Verantwortliche kann zu Beginn entscheiden, ob personenbezogene Daten gelöscht oder zurückgegeben werden sollen, indem er dies im Vertrag festlegt, und zwar durch eine schriftliche Mitteilung, die rechtzeitig an den Auftragsverarbeiter zu senden ist. Der Vertrag oder ein anderer Rechtsakt sollte die Möglichkeit für den für die Verarbeitung Verantwortlichen widerspiegeln, die getroffene Entscheidung vor dem Ende der Erbringung der mit der Verarbeitung verbundenen Dienstleistungen zu ändern. Der Vertrag sollte das Verfahren für die Erteilung solcher Anweisungen festlegen.

141. Wenn der für die Verarbeitung Verantwortliche beschließt, dass die personenbezogenen Daten gelöscht werden, sollte der Auftragsverarbeiter sicherstellen, dass die Löschung auf sichere Weise erfolgt, auch um Artikel 32 DSGVO zu erfüllen. Der Auftragsverarbeiter sollte dem für die Verarbeitung Verantwortlichen bestätigen, dass die Löschung innerhalb eines vereinbarten Zeitrahmens und in einer vereinbarten Weise erfolgt ist.

142. Der Auftragsverarbeiter muss alle vorhandenen Kopien der Daten löschen, es sei denn, das Recht der EU oder eines Mitgliedstaats schreibt eine weitere Speicherung vor. Wenn der Auftragsverarbeiter oder der für die Verarbeitung Verantwortliche Kenntnis von einer solchen gesetzlichen Verpflichtung hat, sollte er die andere Partei so schnell wie möglich informieren.

1.3.8 Der Auftragsverarbeiter muss dem für die Verarbeitung Verantwortlichen alle Informationen zur Verfügung stellen, die erforderlich sind, um die Einhaltung der in Artikel 28 festgelegten Verpflichtungen nachzuweisen, und Audits, einschließlich Inspektionen, die von dem für die Verarbeitung Verantwortlichen oder einem anderen von dem für die Verarbeitung Verantwortlichen beauftragten Prüfer durchgeführt werden, zulassen und dazu beitragen (Art. 28 Abs. 3 Buchstabe h DSGVO).

143. Der Vertrag muss Einzelheiten darüber enthalten, wie oft und wie der Informationsfluss zwischen dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen erfolgen soll, damit der für die Verarbeitung 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 relevanten Teile der Aufzeichnungen des Auftragsverarbeiters über die Verarbeitungstätigkeiten an den für die Verarbeitung Verantwortlichen weitergegeben werden. Der Auftragsverarbeiter sollte alle Informationen darüber zur Verfügung stellen, wie die Verarbeitungstätigkeit im Auftrag des für die Verarbeitung Verantwortlichen durchgeführt wird. Diese Informationen sollten Angaben zur Funktionsweise der verwendeten Systeme, zu den Sicherheitsmaßnahmen, zur Erfüllung der Anforderungen an die Datenaufbewahrung, zum Speicherort der Daten, zu Datenübertragungen, zu den Personen, die Zugang zu den Daten haben, und zu den Empfängern der Daten, zu den verwendeten Unterauftragsverarbeitern usw. umfassen.

144. Im Vertrag sind auch weitere Einzelheiten über die Fähigkeit zur Durchführung von und die Pflicht zur Mitwirkung bei Inspektionen und Audits durch den für die Verarbeitung Verantwortlichen oder einen anderen von ihm beauftragten Prüfer festzulegen.

Die DSGVO legt fest, dass die Inspektionen und Audits von dem für die Verarbeitung Verantwortlichen oder von einem von dem Verantwortlichen beauftragten Dritten durchgeführt werden. Das Ziel eines solchen Audits ist es, sicherzustellen, dass der für die Verarbeitung Verantwortliche über alle Informationen bezüglich der in seinem Auftrag durchgeführten Verarbeitungstätigkeit und der vom Auftragsverarbeiter gegebenen Garantien verfügt. Der Auftragsverarbeiter kann die Wahl eines bestimmten Prüfers vorschlagen, aber die endgültige Entscheidung muss gemäß Artikel 28 Absatz 3 Buchstabe h der DSGVO dem für die Verarbeitung Verantwortlichen überlassen werden. [64] Zusätzlich, auch wenn der

[64] Siehe Gemeinsame Stellungnahme 1/2021 des EDSB und des EDSB zu Standardvertragsklauseln zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern, Absatz 43.

Inspektion durch einen vom Auftragsverarbeiter vorgeschlagenen Prüfer durchgeführt wird, behält der Verantwortliche das Recht, den Umfang, die Methodik und die Ergebnisse der Inspektion anzufechten. [65]

Die Parteien sollten nach Treu und Glauben zusammenarbeiten und beurteilen, ob und wann Audits in den Räumlichkeiten des Auftragsverarbeiters erforderlich sind und welche Art von Audit oder Inspektion (aus der Ferne / vor Ort / auf andere Weise, um die erforderlichen Informationen zu sammeln) im konkreten Fall erforderlich und angemessen wäre, auch unter Berücksichtigung von Sicherheitsbedenken; die endgültige Entscheidung darüber trifft der für die Verarbeitung Verantwortliche. Im Anschluss an die Ergebnisse der Inspektion sollte der für die Verarbeitung Verantwortliche in der Lage sein, den Auftragsverarbeiter aufzufordern, Folgemaßnahmen zu ergreifen, z. B. um festgestellte Mängel und Lücken zu beheben. [66] Ebenso sollten spezifische Verfahren für die Inspektion von Unterauftragsverarbeitern durch den Auftragsverarbeiter und den für die Verarbeitung Verantwortlichen festgelegt werden (siehe Unterabschnitt 1.6 unten67).

145. Die Frage der Aufteilung der Kosten zwischen einem für die Verarbeitung Verantwortlichen und einem Auftragsverarbeiter in Bezug auf Audits wird von der DSGVO nicht abgedeckt und unterliegt wirtschaftlichen Erwägungen. Artikel 28 Absatz 3 Buchstabe h verlangt jedoch, dass der Vertrag eine Verpflichtung des Auftragsverarbeiters enthält, dem für die Verarbeitung Verantwortlichen alle erforderlichen Informationen zur Verfügung zu stellen, sowie die Verpflichtung, Audits, einschließlich Inspektionen, die von dem für die Verarbeitung Verantwortlichen oder einem anderen von dem für die Verarbeitung Verantwortlichen beauftragten Prüfer durchgeführt werden, zuzulassen und zu unterstützen. Dies bedeutet in der Praxis, dass die Parteien keine Klauseln in den Vertrag aufnehmen sollten, die die Zahlung von Kosten oder Gebühren vorsehen, die eindeutig unverhältnismäßig oder überhöht wären und somit eine abschreckende Wirkung auf eine der Parteien hätten. Solche Klauseln würden in der Tat dazu führen, dass die in Artikel 28 Absatz 3 Buchstabe h genannten Rechte und Pflichten in der Praxis nie ausgeübt werden und rein theoretisch werden, während sie ein integraler Bestandteil der in Artikel 28 DSGVO vorgesehenen Datenschutzgarantien sind.

1.4 Anweisungen, die gegen das Datenschutzrecht verstoßen

146. Gemäß Artikel 28 Absatz 3 muss der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen unverzüglich informieren, wenn eine Anweisung seiner Meinung nach gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

147. In der Tat hat der Auftragsverarbeiter die Pflicht, die Anweisungen des für die Verarbeitung Verantwortlichen zu befolgen, aber er hat auch eine allgemeine Verpflichtung, das Gesetz einzuhalten. Eine Anweisung, die gegen das Datenschutzrecht verstößt, scheint einen Konflikt zwischen den beiden vorgenannten Pflichten zu verursachen.

148. Sobald der für die Verarbeitung Verantwortliche darüber informiert wird, dass eine seiner Anweisungen möglicherweise gegen das Datenschutzrecht verstößt, muss er die Situation bewerten und feststellen, ob die Anweisung tatsächlich gegen das Datenschutzrecht verstößt.

149. Der EDSB empfiehlt den Parteien, im Vertrag die Folgen der Benachrichtigung über eine rechtswidrige Anweisung durch den Auftragsverarbeiter und für den Fall der Untätigkeit des für die Verarbeitung Verantwortlichen in diesem Zusammenhang auszuhandeln und zu vereinbaren. Ein Beispiel wäre die Aufnahme einer Klausel über die Beendigung des Vertrags, wenn der für die Verarbeitung Verantwortliche auf einer rechtswidrigen Anweisung beharrt. Ein anderes Beispiel wäre eine Klausel über die Möglichkeit des Auftragsverarbeiters, die Durchführung der betroffenen Weisung auszusetzen, bis der für die Verarbeitung Verantwortliche seine Weisung bestätigt, ändert oder zurückzieht68.

[65] Siehe Stellungnahme 14/2019 zu dem von der DK SA vorgelegten Entwurf von Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO), Randnummer 43.
[66] Siehe Stellungnahme 14/2019 zu dem von der DK SA vorgelegten Entwurf von Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO), Randnummer 43.
[67] Siehe Teil II, Unterabschnitt 1.6 ("Unterauftragsverarbeiter").
[68] Siehe Gemeinsame Stellungnahme 1/2021 des EDSB und des EDSB zu Standardvertragsklauseln zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern, Absatz 39.

1.5 Der Verarbeiter bestimmt die Zwecke und Mittel der Verarbeitung

150. Verstößt der Auftragsverarbeiter bei der Festlegung der Zwecke und Mittel der Verarbeitung gegen die Verordnung, so ist er in Bezug auf diese Verarbeitung als für die Verarbeitung Verantwortlicher zu betrachten (Artikel 28 Absatz 10 DSGVO).

1.6 Unterprozessoren

151. Datenverarbeitungstätigkeiten werden oft von einer großen Anzahl von Akteuren durchgeführt, und die Ketten der Unterauftragsvergabe werden immer komplexer. Die DSGVO führt spezifische Verpflichtungen ein, die ausgelöst werden, wenn ein (Unter-)Auftragsverarbeiter beabsichtigt, einen anderen Akteur zu beauftragen und damit ein weiteres Glied in die Kette einzufügen, indem er diesem Tätigkeiten überträgt, die die Verarbeitung personenbezogener Daten erfordern. Die Analyse, ob der Dienstleister als Unterauftragsverarbeiter agiert, sollte im Einklang mit dem oben beschriebenen Konzept des Auftragsverarbeiters durchgeführt werden (siehe oben Ziffer 83).

152. Obwohl die Kette recht lang sein kann, behält der für die Verarbeitung Verantwortliche seine zentrale Rolle bei der Bestimmung des Zwecks und der Mittel der Verarbeitung. Artikel 28 Absatz 2 DSGVO legt fest, dass der Auftragsverarbeiter keinen anderen Auftragsverarbeiter ohne vorherige spezielle oder allgemeine schriftliche Genehmigung des für die Verarbeitung Verantwortlichen (auch in elektronischer Form) einschalten darf. Im Falle einer allgemeinen schriftlichen Genehmigung muss der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen über alle beabsichtigten Änderungen in Bezug auf die Hinzufügung oder den Austausch anderer Auftragsverarbeiter informieren und dem für die Verarbeitung Verantwortlichen die Möglichkeit geben, gegen solche Änderungen Einspruch zu erheben. In beiden Fällen muss der Auftragsverarbeiter die schriftliche Genehmigung des für die Verarbeitung Verantwortlichen einholen, bevor er den Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten betraut. Für die Beurteilung und die Entscheidung über die Genehmigung der Unterauftragsvergabe muss der Auftragsverarbeiter dem für die Verarbeitung Verantwortlichen eine Liste der vorgesehenen Unterauftragsverarbeiter vorlegen (einschließlich für jeden einzelnen: deren Standorte, was sie tun werden und einen Nachweis darüber, welche Sicherheitsvorkehrungen sie getroffen haben). [69]

153. Die vorherige schriftliche Genehmigung kann spezifisch sein, d. h. sich auf einen bestimmten Unterauftragsverarbeiter für eine bestimmte Verarbeitungstätigkeit und zu einem bestimmten Zeitpunkt beziehen, oder allgemein sein. Dies sollte in dem Vertrag oder einem anderen Rechtsakt, der die Verarbeitung regelt, festgelegt werden.

154. In Fällen, in denen der für die Verarbeitung Verantwortliche beschließt, bestimmte Unterauftragsverarbeiter zum Zeitpunkt der Unterzeichnung des Vertrags zuzulassen, sollte eine Liste der zugelassenen Unterauftragsverarbeiter in den Vertrag oder einen Anhang dazu aufgenommen werden. Die Liste sollte dann gemäß der vom für die Verarbeitung Verantwortlichen erteilten allgemeinen oder besonderen Genehmigung auf dem neuesten Stand gehalten werden.

155. Entscheidet sich der für die Verarbeitung Verantwortliche dafür, eine **Sondergenehmigung** zu erteilen, sollte er schriftlich angeben, auf welchen Unterauftragsverarbeiter und auf welche Verarbeitungstätigkeit sie sich bezieht. Jede spätere Änderung muss vom für die Verarbeitung Verantwortlichen weiter genehmigt werden, bevor sie in Kraft tritt. Wird der Antrag des Auftragsverarbeiters auf Erteilung einer Sondergenehmigung nicht innerhalb des festgelegten Zeitrahmens beantwortet, sollte er als abgelehnt gelten. Der für die Verarbeitung Verantwortliche sollte seine Entscheidung über die Erteilung oder Verweigerung der Genehmigung unter Berücksichtigung seiner Verpflichtung treffen, nur Auftragsverarbeiter einzusetzen, die "ausreichende Garantien" bieten (siehe Unterabschnitt 1.1 oben70).

156. Alternativ kann der für die Verarbeitung Verantwortliche seine **allgemeine Genehmigung** für den Einsatz von Unterauftragsverarbeitern erteilen (im Vertrag, einschließlich einer Liste mit solchen Unterauftragsverarbeitern in einem Anhang dazu), die durch Kriterien ergänzt werden sollte, die dem Auftragsverarbeiter als Richtschnur für seine Auswahl dienen (z. B. Garantien in Bezug auf technische und organisatorische

[69] Diese Informationen werden benötigt, damit der für die Verarbeitung Verantwortliche den Grundsatz der Rechenschaftspflicht gemäß Artikel 24 sowie die Bestimmungen von Artikel 28 Absatz 1, Artikel 32 und Kapitel V der DSGVO einhalten kann.

[70] Siehe Teil II - Unterabschnitt 1.1 ("Wahl des Bearbeiters").

Maßnahmen, Fachwissen, Zuverlässigkeit und Ressourcen). [71] In diesem Szenario muss der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen rechtzeitig über eine beabsichtigte Hinzufügung oder einen beabsichtigten Austausch von Unterauftragsverarbeitern informieren, um dem für die Verarbeitung Verantwortlichen die Möglichkeit zu geben, Einspruch zu erheben.

157. Der Hauptunterschied zwischen dem Szenario der besonderen Genehmigung und dem der allgemeinen Genehmigung liegt daher in der Bedeutung, die dem Schweigen des für die Verarbeitung Verantwortlichen gegeben wird: In der Situation der allgemeinen Genehmigung kann das Versäumnis des für die Verarbeitung Verantwortlichen, innerhalb des festgelegten Zeitrahmens Einspruch zu erheben, als Genehmigung interpretiert werden.

158. In beiden Fällen sollte der Vertrag Einzelheiten zum Zeitrahmen für die Genehmigung oder den Widerspruch des für die Verarbeitung Verantwortlichen und zur Art und Weise der Kommunikation zwischen den Parteien zu diesem Thema (z. B. Vorlagen) enthalten. Ein solcher Zeitrahmen muss im Hinblick auf die Art der Verarbeitung, die Komplexität der dem Auftragsverarbeiter (und den Unterauftragsverarbeitern) übertragenen Tätigkeiten und die Beziehung zwischen den Parteien angemessen sein. Darüber hinaus sollte der Vertrag Einzelheiten zu den praktischen Schritten nach dem Widerspruch des für die Verarbeitung Verantwortlichen enthalten (z. B. durch Festlegung eines Zeitrahmens, innerhalb dessen der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter entscheiden sollten, ob die Verarbeitung beendet werden soll).

159. Unabhängig von den Kriterien, die der für die Verarbeitung Verantwortliche für die Auswahl der Anbieter vorschlägt, bleibt der Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen in vollem Umfang für die Erfüllung der Pflichten der Unterauftragsverarbeiter verantwortlich (Artikel 28 Absatz 4 DSGVO). Daher sollte der Auftragsverarbeiter sicherstellen, dass er Unterauftragsverarbeiter vorschlägt, die ausreichende Garantien bieten.

160. Außerdem muss ein Auftragsverarbeiter, wenn er einen (zugelassenen) Unterauftragsverarbeiter einsetzen will, mit diesem einen Vertrag schließen, der ihm dieselben Verpflichtungen auferlegt, die der für die Verarbeitung Verantwortliche dem Erstverarbeiter auferlegt hat, oder die Verpflichtungen müssen durch einen anderen Rechtsakt nach EU-Recht oder dem Recht eines Mitgliedstaats auferlegt werden. Die gesamte Kette der Verarbeitungstätigkeiten muss durch schriftliche Vereinbarungen geregelt werden. Die Auferlegung "gleicher" Verpflichtungen sollte eher funktional als formal ausgelegt werden: Der Vertrag muss nicht genau die gleichen Worte enthalten wie der Vertrag zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter, aber er sollte sicherstellen, dass die Verpflichtungen in der Substanz die gleichen sind. Dies bedeutet auch, dass, wenn der Auftragsverarbeiter den Unterauftragsverarbeiter mit einem bestimmten Teil der Verarbeitung betraut, 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. Als Beispiel für die Unterstützung bei Verpflichtungen im Zusammenhang mit Datenschutzverletzungen könnte die Meldung einer Datenschutzverletzung durch einen Unterauftragsverarbeiter direkt an den für die Verarbeitung Verantwortlichen erfolgen, wenn alle drei zustimmen. Im Falle einer solchen direkten Benachrichtigung sollte der Auftragsverarbeiter jedoch informiert werden und eine Kopie der Benachrichtigung erhalten.

2 FOLGEN DER GEMEINSAMEN VERANTWORTLICHKEIT

2.1 Transparente Festlegung der jeweiligen Verantwortlichkeiten der gemeinsam für die Verarbeitung Verantwortlichen für die Einhaltung der Verpflichtungen aus der DSGVO

161. Artikel 26 Absatz 1 der DSGVO sieht vor, dass gemeinsam für die Verarbeitung Verantwortliche in transparenter Weise ihre jeweiligen Verantwortlichkeiten für die Einhaltung der Verpflichtungen aus der Verordnung festlegen und vereinbaren.

162. Die gemeinsam für die Verarbeitung Verantwortlichen müssen daher festlegen, "wer was tut", indem sie untereinander entscheiden, wer welche Aufgaben auszuführen hat, um sicherzustellen, dass die Verarbeitung mit den geltenden Verpflichtungen gemäß der DSGVO in Bezug auf die betreffende gemeinsame Verarbeitung übereinstimmt. Mit anderen Worten, es ist eine Verteilung der Verantwortlichkeiten für die Einhaltung vorzunehmen, wie sie sich aus der Verwendung des Begriffs "*jeweils*" in

[71] Diese Pflicht des für die Verarbeitung Verantwortlichen ergibt sich aus dem Grundsatz der Rechenschaftspflicht in Artikel 24 und aus der Verpflichtung zur Einhaltung der Bestimmungen von Artikel 28 Absatz 1, 32 und Kapitel V der DSGVO.

Artikel 26 Absatz 1. Dies schließt nicht aus, dass in den Rechtsvorschriften der EU oder der Mitgliedstaaten bereits bestimmte Verantwortlichkeiten der einzelnen gemeinsam für die Verarbeitung Verantwortlichen festgelegt sind. Ist dies der Fall, sollte die Vereinbarung über den gemeinsam für die Verarbeitung Verantwortlichen auch etwaige zusätzliche Verantwortlichkeiten regeln, die für die Einhaltung der DSGVO erforderlich sind und in den gesetzlichen Bestimmungen nicht geregelt sind. [72]

163. Ziel dieser Vorschriften ist es, sicherzustellen, dass bei der Beteiligung mehrerer Akteure, insbesondere in komplexen Datenverarbeitungsumgebungen, die Verantwortung für die Einhaltung der Datenschutzvorschriften eindeutig zugewiesen wird, um zu vermeiden, dass der Schutz personenbezogener Daten verringert wird oder dass ein negativer Kompetenzkonflikt zu Schlupflöchern führt, durch die einige Verpflichtungen von einer der an der Verarbeitung beteiligten Parteien nicht eingehalten werden. Es sollte hier klargestellt werden, dass alle Zuständigkeiten entsprechend den tatsächlichen Gegebenheiten zugewiesen werden müssen, um eine wirksame Vereinbarung zu erreichen. Der EDSB stellt fest, dass es Situationen gibt, in denen der Einfluss eines gemeinsam Verantwortlichen und dessen faktischer Einfluss das Zustandekommen einer Vereinbarung erschweren. Diese Umstände negieren jedoch nicht die gemeinsame Verantwortlichkeit und können nicht dazu dienen, eine der Parteien von ihren Verpflichtungen gemäß der DSGVO zu befreien.

164. Genauer gesagt legt Artikel 26 Absatz 1 fest, dass die Festlegung ihrer jeweiligen Verantwortlichkeiten (d. h. Aufgaben) für die Einhaltung der Verpflichtungen nach der DSGVO von den gemeinsam für die Verarbeitung Verantwortlichen "*insbesondere*" in Bezug auf die Ausübung der Rechte der betroffenen Person und die in den Artikeln 13 und 14 genannten Informationspflichten vorzunehmen ist, sofern und soweit die jeweiligen Verantwortlichkeiten der für die Verarbeitung Verantwortlichen nicht durch das Unionsrecht oder das Recht der Mitgliedstaaten, dem die für die Verarbeitung Verantwortlichen unterliegen, festgelegt sind.

165. Aus dieser Bestimmung geht klar hervor, dass gemeinsam für die Verarbeitung Verantwortliche festlegen müssen, wer jeweils für die Beantwortung von Anfragen zuständig ist, wenn betroffene Personen ihre durch die DSGVO gewährten Rechte ausüben, und für die Bereitstellung von Informationen an sie gemäß Artikel 13 und 14 der DSGVO. Dies bezieht sich nur darauf, im Innenverhältnis festzulegen, welche der Parteien verpflichtet ist, auf welche Anfragen der betroffenen Personen zu antworten. . Unabhängig von einer solchen Vereinbarung kann sich die betroffene Person gemäß Artikel 26 (3) DSGVO an jeden der gemeinsam für die Verarbeitung Verantwortlichen wenden. Die Verwendung des Begriffs "*insbesondere*" deutet jedoch darauf hin, dass die Verpflichtungen, die der Verteilung der Verantwortlichkeiten für die Einhaltung durch jede beteiligte Partei unterliegen, wie in dieser Bestimmung erwähnt, nicht erschöpfend sind. Daraus folgt, dass die Verteilung der Verantwortlichkeiten für die Einhaltung der Vorschriften unter den gemeinsam für die Verarbeitung Verantwortlichen nicht auf die in Artikel 26 Absatz 1 genannten Themen beschränkt ist, sondern sich auch auf andere Verpflichtungen des für die Verarbeitung Verantwortlichen gemäß der DSGVO erstreckt. Tatsächlich müssen gemeinsam für die Verarbeitung Verantwortliche sicherstellen, dass die gesamte gemeinsame Verarbeitung vollständig mit der DSGVO übereinstimmt.

166. Unter diesem Gesichtspunkt umfassen die Maßnahmen zur Einhaltung der Vorschriften und die damit verbundenen Verpflichtungen, die die gemeinsam für die Verarbeitung Verantwortlichen bei der Festlegung ihrer jeweiligen Zuständigkeiten berücksichtigen sollten, zusätzlich zu den in Artikel 26 Absatz 1 ausdrücklich genannten Maßnahmen u. a. und ohne Einschränkung:

- Umsetzung der allgemeinen Datenschutzgrundsätze (Artikel 5)
- Rechtsgrundlage der Verarbeitung73 (Artikel 6)
- Sicherheitsmaßnahmen (Artikel 32)

[72] "In jedem Fall sollte die Vereinbarung der gemeinsam für die Verarbeitung Verantwortlichen umfassend alle Verantwortlichkeiten der gemeinsam für die Verarbeitung Verantwortlichen regeln, einschließlich derjenigen, die möglicherweise bereits im einschlägigen EU-Recht oder im Recht der Mitgliedstaaten festgelegt sind, und unbeschadet der Verpflichtung der gemeinsam für die Verarbeitung Verantwortlichen, den Kern der Vereinbarung der gemeinsam für die Verarbeitung Verantwortlichen gemäß Artikel 26 Absatz 2 DSGVO zugänglich zu machen."

[73] Obwohl die DSGVO es nicht ausschließt, dass gemeinsam für die Verarbeitung Verantwortliche unterschiedliche Rechtsgrundlagen für verschiedene von ihnen durchgeführte Verarbeitungsvorgänge verwenden, wird empfohlen, wann immer möglich, dieselbe Rechtsgrundlage für einen bestimmten Zweck zu verwenden.

- Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde und an die betroffene Person74 (Artikel 33 und 34)
- Datenschutz-Folgenabschätzungen (Artikel 35 und 36)[75]
- Der Einsatz eines Verarbeiters (Artikel 28)
- Übermittlung von Daten an Drittländer (Kapitel V)
- Organisation des Kontakts mit betroffenen Personen und Aufsichtsbehörden

167. Andere Themen, die in Abhängigkeit von der jeweiligen Verarbeitung und der Absicht der Parteien in Betracht gezogen werden könnten, sind beispielsweise die Beschränkungen der Nutzung personenbezogener Daten für einen anderen Zweck durch einen der gemeinsam für die Verarbeitung Verantwortlichen. In dieser Hinsicht haben beide für die Verarbeitung Verantwortlichen immer die Pflicht, sicherzustellen, dass beide eine Rechtsgrundlage für die Verarbeitung haben. Manchmal werden im Rahmen der gemeinsamen Verantwortung personenbezogene Daten von einem Verantwortlichen an einen anderen weitergegeben. Im Rahmen der Rechenschaftspflicht hat jeder für die Verarbeitung Verantwortliche die Pflicht, sicherzustellen, dass die Daten nicht in einer Weise weiterverarbeitet werden, die mit den Zwecken, für die sie ursprünglich von dem für die Weitergabe der Daten Verantwortlichen erhoben wurden, unvereinbar ist. [76]

168. Gemeinsam für die Verarbeitung Verantwortliche können einen gewissen Grad an Flexibilität bei der Verteilung und Zuweisung von Pflichten unter ihnen haben, solange sie die vollständige Einhaltung der DSGVO in Bezug auf die jeweilige Verarbeitung sicherstellen. Bei der Aufteilung sollten Faktoren berücksichtigt werden, wie z. B. wer kompetent und in der Lage ist, die Rechte der betroffenen Person effektiv zu gewährleisten und die relevanten Verpflichtungen gemäß der DSGVO zu erfüllen. Der EDPB empfiehlt, die relevanten Faktoren und die interne Analyse zu dokumentieren, die durchgeführt wurde, um die verschiedenen Pflichten zuzuordnen. Diese Analyse ist Teil der Dokumentation im Rahmen des Grundsatzes der Rechenschaftspflicht.

169. Die Pflichten müssen nicht gleichmäßig auf die gemeinsam für die Verarbeitung Verantwortlichen verteilt sein. Diesbezüglich hat der EuGH kürzlich festgestellt, dass "*das Vorhandensein einer gemeinsamen Verantwortung nicht notwendigerweise eine gleiche Verantwortung der verschiedenen an der Verarbeitung personenbezogener Daten beteiligten Akteure impliziert*". [77] Es kann jedoch Fälle geben, in denen nicht alle Pflichten verteilt werden können und alle gemeinsam für die Verarbeitung Verantwortlichen die gleichen Anforderungen aus der DSGVO erfüllen müssen, wobei die Art und der Kontext der gemeinsamen Verarbeitung zu berücksichtigen sind. So müssen beispielsweise gemeinsam für die Verarbeitung Verantwortliche, die gemeinsam genutzte Datenverarbeitungsinstrumente oder -systeme nutzen, beide die Einhaltung insbesondere des Grundsatzes der Zweckbindung sicherstellen und geeignete Maßnahmen ergreifen, um die Sicherheit der mit den gemeinsam genutzten Instrumenten verarbeiteten personenbezogenen Daten zu gewährleisten.

---

[74] Siehe auch die EDPB-Leitlinien zur Meldung von Datenschutzverletzungen gemäß der Verordnung (EU) 2016/679, WP250.rev.01, die vorsehen, dass die gemeinsame für die Verarbeitung Verantwortlichkeit "die *Festlegung, welche Partei die Verantwortung für die Einhaltung der Verpflichtungen gemäß Artikel 33 und 34 übernimmt",* beinhaltet*. WP29 empfiehlt, dass die vertraglichen Vereinbarungen zwischen gemeinsam für die Verarbeitung Verantwortlichen Bestimmungen enthalten, die festlegen, welcher für die Verarbeitung Verantwortliche die Führung bei der Einhaltung der Pflichten zur Meldung von Datenschutzverletzungen gemäß der DSGVO übernimmt bzw. dafür verantwortlich ist*" (S. 13).

[75] Siehe auch EDPB-Leitlinien zu DPIAs, WP248.rev01, die Folgendes vorsehen: "*Wenn an der Verarbeitung gemeinsame Verantwortliche beteiligt sind, müssen sie ihre jeweiligen Pflichten genau festlegen. Ihr DPIA sollte darlegen, welche Partei für die verschiedenen Maßnahmen zur Behandlung von Risiken und zum Schutz der Rechte und Freiheiten der betroffenen Personen verantwortlich ist. Jeder für die Datenverarbeitung Verantwortliche sollte seine Bedürfnisse zum Ausdruck bringen und nützliche Informationen weitergeben, ohne entweder Geheimnisse zu gefährden (z. B.: Schutz von Geschäftsgeheimnissen, geistigem Eigentum, vertraulichen Geschäftsinformationen) oder Schwachstellen offenzulegen*" (S.7).

[76] Jede Weitergabe durch einen für die Verarbeitung Verantwortlichen erfordert eine rechtmäßige Grundlage und eine Bewertung der Vereinbarkeit, unabhängig davon, ob der Empfänger ein eigenständig für die Verarbeitung Verantwortlicher oder ein gemeinsam für die Verarbeitung Verantwortlicher ist. Mit anderen Worten: Das Bestehen einer Beziehung zwischen gemeinsam für die Verarbeitung Verantwortlichen bedeutet nicht automatisch, dass der gemeinsam für die Verarbeitung Verantwortliche, der die Daten erhält, diese auch rechtmäßig für zusätzliche Zwecke verarbeiten kann, die über den Bereich der gemeinsamen Kontrolle hinausgehen.

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

170. Ein weiteres Beispiel ist die Anforderung an jeden gemeinsam für die Verarbeitung Verantwortlichen, ein Verzeichnis der Verarbeitungstätigkeiten zu führen oder einen Datenschutzbeauftragten (DSB) zu benennen, wenn die Bedingungen von Artikel 37 Absatz 1 erfüllt sind. Solche Anforderungen beziehen sich nicht auf die gemeinsame Verarbeitung, sondern gelten für sie als für die Verarbeitung Verantwortliche.

2.2 Die Zuweisung von Verantwortlichkeiten muss in Form einer Vereinbarung erfolgen

2.2.1 Form der Anordnung

171. Artikel 26(1) der DSGVO sieht als neue Verpflichtung für gemeinsam für die Verarbeitung Verantwortliche vor, dass sie ihre jeweiligen Verantwortlichkeiten "*durch eine Vereinbarung zwischen ihnen*" festlegen sollten. Die rechtliche Form einer solchen Vereinbarung ist in der DSGVO nicht festgelegt. Daher steht es den gemeinsam für die Verarbeitung Verantwortlichen frei, die Form der Vereinbarung zu vereinbaren.

172. Darüber hinaus ist die Vereinbarung über die Aufteilung der Verantwortlichkeiten für jeden der gemeinsam für die Verarbeitung Verantwortlichen verbindlich. Sie vereinbaren und verpflichten sich *gegenseitig*, für die Einhaltung der jeweiligen Verpflichtungen, die in ihrer Vereinbarung als ihre Verantwortung angegeben sind, verantwortlich zu sein.

173. Daher empfiehlt der EDSB aus Gründen der Rechtssicherheit, auch wenn die DSGVO keinen Vertrag oder einen anderen Rechtsakt vorschreibt, dass eine solche Vereinbarung in Form eines verbindlichen Dokuments wie eines Vertrags oder eines anderen verbindlichen Rechtsakts nach dem Recht der EU oder eines Mitgliedstaats, dem die für die Verarbeitung Verantwortlichen unterliegen, getroffen wird. Dies würde Gewissheit schaffen und könnte als Nachweis für Transparenz und Rechenschaftspflicht dienen. Im Falle der Nichteinhaltung der in der Vereinbarung vorgesehenen Aufteilung ermöglicht es der verbindliche Charakter der Vereinbarung einem für die Verarbeitung Verantwortlichen, den anderen für das haftbar zu machen, was in der Vereinbarung als unter seine Verantwortung fallend festgelegt wurde. Im Einklang mit dem Grundsatz der Rechenschaftspflicht ermöglicht die Verwendung eines Vertrags oder eines anderen Rechtsakts den gemeinsam für die Verarbeitung Verantwortlichen nachzuweisen, dass sie die ihnen durch die DSGVO auferlegten Pflichten erfüllen.

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

175. Um die Aufteilung der Verantwortlichkeiten zwischen den Parteien besser zu gestalten, empfiehlt der EDSB, dass die Vereinbarung auch allgemeine Informationen über die gemeinsame Verarbeitung enthält, indem insbesondere der Gegenstand und der Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen angegeben werden.

2.2.2 Verpflichtungen gegenüber betroffenen Personen

176. Die DSGVO sieht mehrere Verpflichtungen der gemeinsam für die Verarbeitung Verantwortlichen gegenüber den betroffenen Personen vor:

Die Vereinbarung muss die jeweiligen Rollen und Beziehungen der gemeinsam für die Verarbeitung Verantwortlichen *gegenüber den* betroffenen Personen angemessen widerspiegeln

177. Ergänzend zu dem, was oben in Abschnitt 2.1 der vorliegenden Leitlinien erläutert wird, ist es wichtig, dass die gemeinsam für die Verarbeitung Verantwortlichen in der Vereinbarung ihre jeweilige Rolle klären, "*insbesondere*" in Bezug auf die Ausübung der Rechte der betroffenen Person und ihre Pflichten zur Bereitstellung der in Artikel 13 und 14 genannten Informationen. Artikel 26 der DSGVO unterstreicht die Bedeutung dieser spezifischen Pflichten. Die gemeinsam für die Verarbeitung Verantwortlichen müssen daher organisieren und vereinbaren, wie und von wem die Informationen erteilt werden

[78] Wie in Erwägungsgrund 79 der DSGVO ausgeführt, *"(...) erfordert die Verantwortung und Haftung der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter, auch in Bezug auf die Überwachung durch und Maßnahmen von Aufsichtsbehörden, eine klare Zuweisung der Zuständigkeiten nach dieser Verordnung, auch wenn ein für die Verarbeitung Verantwortlicher die Zwecke und Mittel der Verarbeitung gemeinsam mit anderen für die Verarbeitung Verantwortlichen festlegt*".

bereitgestellt werden und wie und von wem die Antworten auf die Anfragen der betroffenen Person bereitgestellt werden. Unabhängig vom Inhalt der Vereinbarung zu diesem speziellen Punkt kann sich die betroffene Person an einen der gemeinsam für die Verarbeitung Verantwortlichen wenden, um ihre Rechte gemäß Artikel 26 Absatz 3 auszuüben, wie nachstehend näher erläutert.

178. Die Art und Weise, wie diese Pflichten in der Vereinbarung organisiert sind, sollte die Realität der zugrunde liegenden gemeinsamen Verarbeitung "*ordnungsgemäß*", d. h. genau, widerspiegeln. Wenn beispielsweise nur einer der gemeinsam für die Verarbeitung Verantwortlichen mit den betroffenen Personen zum Zweck der gemeinsamen Verarbeitung kommuniziert, könnte dieser für die Verarbeitung Verantwortliche besser in der Lage sein, die betroffenen Personen zu informieren und möglicherweise ihre Anfragen zu beantworten.

Das Wesentliche der Vereinbarung muss der betroffenen Person zugänglich gemacht werden

179. Diese Bestimmung soll sicherstellen, dass die betroffene Person das "*Wesen der Vereinbarung*" kennt. So muss beispielsweise für eine betroffene Person völlig klar sein, welcher Datenverantwortliche als Ansprechpartner für die Ausübung der Rechte der betroffenen Person dient (ungeachtet der Tatsache, dass sie ihre Rechte in Bezug auf und gegenüber jedem gemeinsamen Verantwortlichen ausüben kann). Die Verpflichtung, das Wesen der Vereinbarung den betroffenen Personen zugänglich zu machen, ist im Falle der gemeinsamen Kontrolle wichtig, damit die betroffene Person weiß, welcher der für die Verarbeitung Verantwortlichen wofür verantwortlich ist.

180. Was unter den Begriff "*Wesen der Vereinbarung*" fallen sollte, ist in der DSGVO nicht festgelegt. Der EDSB empfiehlt, dass der Kern zumindest alle Elemente der in den Artikeln 13 und 14 genannten Informationen abdeckt, die der betroffenen Person bereits zugänglich sein sollten, und für jedes dieser Elemente sollte die Vereinbarung angeben, welcher für die Verarbeitung Verantwortliche für die Einhaltung dieser Elemente verantwortlich ist. Im Kern der Vereinbarung muss auch die Kontaktstelle angegeben werden, sofern eine solche benannt wurde.

181. Die Art und Weise, wie diese Informationen der betroffenen Person zur Verfügung gestellt werden sollen, ist nicht festgelegt. Im Gegensatz zu anderen Bestimmungen der Datenschutz-Grundverordnung (z. B. Artikel 30 Absatz 4 für das Verzeichnis der Verarbeitungen oder Artikel 40 Absatz 11 für das Register der genehmigten Verhaltenskodizes) wird in Artikel 26 nicht angegeben, dass die Verfügbarkeit "*auf Antrag*" oder "*mit geeigneten Mitteln öffentlich zugänglich*" sein sollte. Daher obliegt es den gemeinsam für die Verarbeitung Verantwortlichen, zu entscheiden, wie sie den betroffenen Personen den Kern der Vereinbarung am wirksamsten zugänglich machen (z. B. zusammen mit den Informationen in Artikel 13 oder 14, in der Datenschutzerklärung oder auf Anfrage beim Datenschutzbeauftragten, falls vorhanden, oder bei der gegebenenfalls benannten Kontaktstelle). Gemeinsam für die Verarbeitung Verantwortliche sollten jeweils sicherstellen, dass die Informationen auf einheitliche Weise bereitgestellt werden.

Die Vereinbarung kann eine Kontaktstelle für Betroffene benennen

182. Artikel 26 Absatz 1 bietet den gemeinsam für die Verarbeitung Verantwortlichen die Möglichkeit, in der Vereinbarung eine Kontaktstelle für die betroffenen Personen zu benennen. Eine solche Benennung ist nicht zwingend erforderlich.

183. Die Information über eine einzige Kontaktmöglichkeit für mögliche mehrere gemeinsam für die Verarbeitung Verantwortliche ermöglicht es den betroffenen Personen, zu wissen, an wen sie sich in Bezug auf alle Fragen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten wenden können. Darüber hinaus ermöglicht es mehreren gemeinsam für die Verarbeitung Verantwortlichen, ihre Beziehungen und ihre Kommunikation *mit den* betroffenen Personen effizienter zu koordinieren.

184. Aus diesen Gründen empfiehlt der EDPB den gemeinsam für die Verarbeitung Verantwortlichen, eine solche Kontaktstelle zu benennen, um die Ausübung der Rechte der betroffenen Personen nach der DSGVO zu erleichtern.

185. Bei der Kontaktstelle kann es sich um den behördlichen Datenschutzbeauftragten (falls vorhanden), den Vertreter in der Union (bei gemeinsam für die Verarbeitung Verantwortlichen, die nicht in der Union ansässig sind) oder jede andere Kontaktstelle handeln, bei der Informationen eingeholt werden können.

Unabhängig von den Bedingungen der Vereinbarung können die betroffenen Personen ihre Rechte gegenüber jedem der gemeinsam für die Verarbeitung Verantwortlichen geltend machen.

186. Gemäß Artikel 26 Absatz 3 ist eine betroffene Person nicht an die Bedingungen der Vereinbarung gebunden und kann ihre Rechte nach der DSGVO in Bezug auf und gegen jeden der gemeinsamen für die Datenverarbeitung Verantwortlichen ausüben.

187. Sind beispielsweise gemeinsame für die Verarbeitung Verantwortliche in verschiedenen Mitgliedstaaten niedergelassen oder ist nur einer der gemeinsamen für die Verarbeitung Verantwortlichen in der Union niedergelassen, kann sich die betroffene Person nach ihrer Wahl entweder an den für die Verarbeitung Verantwortlichen wenden, der in dem Mitgliedstaat niedergelassen ist, in dem sie ihren gewöhnlichen Aufenthalt oder ihren Arbeitsplatz hat, oder an den für die Verarbeitung Verantwortlichen, der in einem anderen Mitgliedstaat der EU oder im EWR niedergelassen ist.

188. Selbst wenn die Vereinbarung und der verfügbare Inhalt dieser Vereinbarung eine Kontaktstelle für die Entgegennahme und Bearbeitung aller Anfragen der betroffenen Personen vorsehen, können die betroffenen Personen selbst etwas anderes wählen.

189. Daher ist es wichtig, dass gemeinsam für die Verarbeitung Verantwortliche in ihrer Vereinbarung im Voraus organisieren, wie sie Antworten auf Anfragen, die sie von betroffenen Personen erhalten könnten, verwalten werden. In diesem Zusammenhang wird empfohlen, dass gemeinsam für die Verarbeitung Verantwortliche die anderen für die Verarbeitung Verantwortlichen oder die benannte Kontaktstelle über die eingegangenen Anfragen informieren, damit diese wirksam bearbeitet werden können. Von den betroffenen Personen zu verlangen, dass sie sich an die benannte Kontaktstelle oder den für die Verarbeitung Verantwortlichen wenden, würde eine übermäßige Belastung für die betroffenen Personen bedeuten, die dem Ziel der Erleichterung der Ausübung ihrer Rechte nach der DSGVO zuwiderlaufen würde.

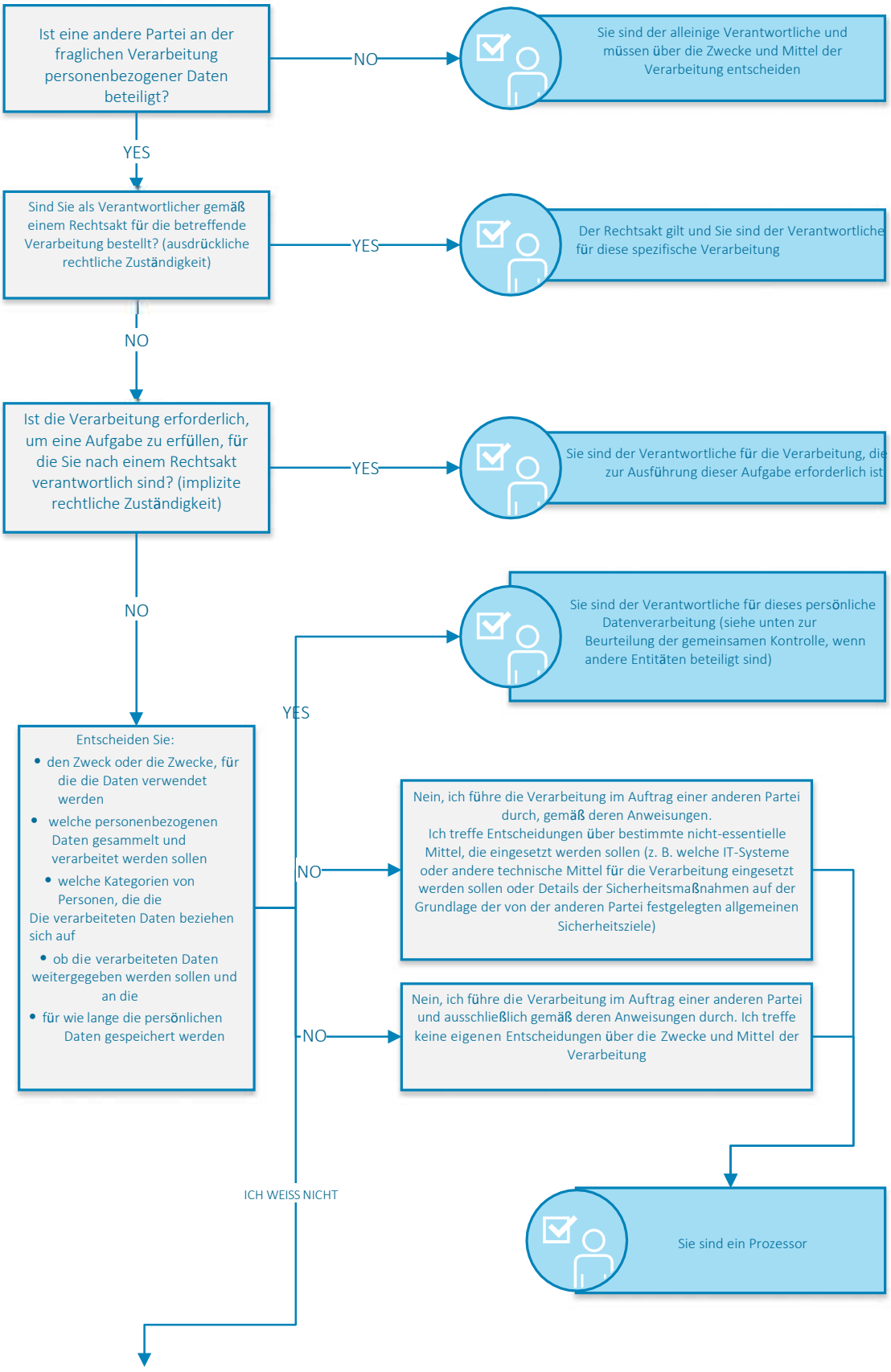
2.3 Pflichten gegenüber Datenschutzbehörden

190. Gemeinsam für die Verarbeitung Verantwortliche sollten in der Vereinbarung regeln, wie sie mit den zuständigen Datenschutzaufsichtsbehörden kommunizieren werden. Diese Kommunikation könnte eine mögliche Konsultation gemäß Artikel 36 der DSGVO, die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten und die Benennung eines Datenschutzbeauftragten umfassen.

191. Es sei daran erinnert, dass die Datenschutzbehörden nicht an die Bedingungen der Vereinbarung gebunden sind, weder in der Frage der Qualifikation der Parteien als gemeinsam für die Verarbeitung Verantwortliche noch in Bezug auf die benannte Kontaktstelle. Daher können sich die Behörden an jeden der gemeinsam für die Verarbeitung Verantwortlichen wenden, um ihre Befugnisse gemäß Artikel 58 im Hinblick auf die gemeinsame Verarbeitung auszuüben.

Anhang I - Flussdiagramm für die Anwendung der Konzepte von Controller, Prozessor und gemeinsamen Controllern in der Praxis

Hinweis: Um die Rolle jeder beteiligten Stelle richtig zu beurteilen, muss man zunächst die spezifische personenbezogene Datenverarbeitung, um die es geht, und ihren genauen Zweck ermitteln. Wenn mehrere Stellen beteiligt sind, muss beurteilt werden, ob die Zwecke und Mittel gemeinsam festgelegt werden, was zu einer gemeinsamen Kontrolle führt.



ICH WEISS NICHT

Ich weiß nicht, wer entscheidet über die Zwecke oder Mittel von die Verarbeitung. :

Die folgenden Faktoren können helfen, die entsprechende Qualifikation der Rollen zu bestimmen:

Faktoren, die darauf hinweisen, dass Sie der Controller sind

Faktoren, die darauf hinweisen, dass Sie der Prozessor sind

- Sie ziehen einen Nutzen aus der Verarbeitung oder haben ein Interesse daran (abgesehen von der bloßen Bezahlung für Dienstleistungen, die Sie von einem anderen Verantwortlichen erhalten)
- Sie treffen im Rahmen oder als Ergebnis der Verarbeitung Entscheidungen über die betroffenen Personen (z. B. sind die betroffenen Personen Ihre Mitarbeiter)
- Die Verarbeitungstätigkeiten können als natürlich mit der Rolle oder den Tätigkeiten Ihrer Einrichtung verbunden angesehen werden (z. B. aufgrund traditioneller Rollen oder beruflicher Fachkenntnisse), was Verantwortlichkeiten aus Sicht des Datenschutzes mit sich bringt
- Die Verarbeitung bezieht sich auf Ihre Beziehung zu den betroffenen Personen als Mitarbeiter, Kunden, Mitglieder usw.
- Sie haben die volle Entscheidungsfreiheit über die Verarbeitung der personenbezogenen Daten
- Sie haben die Verarbeitung personenbezogener Daten einer externen Organisation anvertraut, die die personenbezogenen Daten in Ihrem Auftrag verarbeitet

- Sie verarbeiten die personenbezogenen Daten für die Zwecke einer anderen Partei und in Übereinstimmung mit deren dokumentierten Anweisungen - Sie haben keinen eigenen Zweck für die Verarbeitung.
- Eine andere Partei überwacht Ihre Verarbeitungsaktivitäten, um sicherzustellen, dass Sie die Anweisungen und Vertragsbedingungen einhalten.
- Sie verfolgen mit der Verarbeitung keinen anderen Zweck als Ihr eigenes Geschäftsinteresse an der Erbringung von Dienstleistungen.
- Sie wurden für die Durchführung bestimmter Verarbeitungstätigkeiten von jemandem beauftragt, der seinerseits beauftragt wurde, Daten im Namen einer anderen Partei und auf deren dokumentierte Anweisungen hin zu verarbeiten (Sie sind ein Unterverarbeiter)

Gemeinsame Verantwortlichkeit - Wenn Sie der Verantwortliche sind und andere Parteien an der Verarbeitung personenbezogener Daten beteiligt sind: