EUROPEAN DATA PROTECTION SUPERVISOR

Leitlinien des EDSB zu den Begriffen „Verantwortlicher“, „Auftragsverarbeiter“ und „gemeinsam Verantwortliche“ nach der Verordnung (EU) 2018/1725

7. November 2019

Zusammenfassung

Bei der Verarbeitung personenbezogener Daten **müssen Organe und Einrichtungen der EU (EU-Institutionen) spezifische Datenschutzvorschriften einhalten**. Ihre Pflichten unterscheiden sich je nach ihrer Rolle. **Die folgenden Leitlinien enthalten Erläuterungen und praktische Ratschläge für Organe und Einrichtungen der EU zur Einhaltung der Verordnung (EU) 2018/1725** (im Folgenden „Verordnung").

Nach dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) und der Verordnung (EU) 2018/1725 wurden zahlreiche Fragen zu den Änderungen bei den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" und insbesondere zu ihren jeweiligen Aufgaben und Zuständigkeiten aufgeworfen. **Diese Leitlinien sollen den EU-Institutionen praktische Ratschläge und Anweisungen zur Einhaltung der Verordnung (EU) 2018/1725 geben, indem sie konkrete Orientierungshilfen zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" auf der Grundlage der in der Verordnung enthaltenen Definitionen bieten.** EU-Institutionen werden klarer erkennen, welche Rolle diese Begriffe bei bestimmten Verarbeitungsvorgängen spielen können und welche Auswirkungen sie auf die Pflichten und Zuständigkeiten im Rahmen der Verordnung haben.

Diese Leitlinien richten sich zwar an Datenschutzbeauftragte, Datenschutzkoordinatoren und alle Personen, die innerhalb der EU-Institutionen für die Verarbeitung personenbezogener Daten verantwortlich sind, doch könnten sie auch für andere externe Organisationen nützlich sein.

Im Mittelpunkt der Leitlinien stehen:

- die Begriffe „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche";

- die Verteilung ihrer Pflichten und Zuständigkeiten, insbesondere im Hinblick auf die Ausübung der Rechte der betroffenen Person;

- konkrete Fallstudien zu den Konstellationen Verantwortlicher-Auftragsverarbeiter, einzelne Verantwortliche und gemeinsam Verantwortliche.

Die Beantwortung und Prüfung der Frage, ob EU-Institutionen als Verantwortliche, Auftragsverarbeiter oder gemeinsam Verantwortliche anzusehen sind, sowie ihre jeweiligen Pflichten werden in Flussdiagrammen und Checklisten dargestellt.

Diese Leitlinien helfen der oberen Führungsebene zudem dabei, von höchster Stelle der Organisation aus eine Datenschutzkultur zu fördern und den Grundsatz der Rechenschaftspflicht umzusetzen.

Der Zweck dieser Leitlinien besteht darin, EU-Institutionen die Erfüllung ihrer Pflichten zu erleichtern. Nach dem Grundsatz der Rechenschaftspflicht bleiben EU-Institutionen für die Einhaltung ihrer Verpflichtungen verantwortlich.

INHALTSVERZEICHNIS

1. Einleitung 4

2. Anwendungsbereich und Gliederung der Leitlinien 5

2.1 ANWENDUNGSBEREICH DER LEITLINIEN 5

2.2 AUFBAU DER LEITLINIEN 6

3. Der Begriff des „Verantwortlichen" 7

3.1 DEFINITION DES „VERANTWORTLICHEN" 7

3.1.1 „Das Organ oder die Einrichtung der Union, die Generaldirektion oder jede andere organisatorische Einheit" 7

3.1.2 „Bestimmt" 7

3.1.3 „Zwecke und Mittel" 9

3.1.4 „Allein oder gemeinsam mit anderen" 11

3.1.5 „Der Verarbeitung personenbezogener Daten" 12

3.2 PFLICHTEN UND HAFTUNG DES VERANTWORTLICHEN 13

3.3 SCHUTZ BETROFFENER PERSONEN 13

3.4 WANN IST EINE EU-INSTITUTION EIN VERANTWORTLICHER? EINE CHECKLISTE 14

4. Der Begriff des „Auftragsverarbeiters" 16

4.1 DIE DEFINITION DES „AUFTRAGSVERARBEITERS" 16

4.1.1 Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Einrichtung 16

4.1.2 Verarbeitung im Auftrag des Verantwortlichen 17

4.2 DIE WAHL DES AUFTRAGSVERARBEITERS DURCH DEN VERANTWORTLICHEN 19

4.3 HAFTUNG DES AUFTRAGSVERARBEITERS UND AUSÜBUNG DER RECHTE DER BETROFFENEN PERSON 21

4.4 WANN IST EINE EU-INSTITUTION EIN AUFTRAGSVERARBEITER? EINE CHECKLISTE 22

5. Der Begriff „gemeinsam Verantwortliche" 24

5.1 WANN SPRICHT MAN VON GEMEINSAM VERANTWORTLICHEN, UND WELCHES SIND HIER DIE ENTSCHEIDENDEN ELEMENTE? 24

5.2 WELCHE PFLICHTEN HABEN GEMEINSAM VERANTWORTLICHE? 29

5.2.1 Die Zuständigkeiten gemeinsam Verantwortlicher 29

5.2.2 Die Vereinbarung zwischen gemeinsam Verantwortlichen 30

5.2.3 Unterrichtung der betroffenen Personen über das Wesentliche der Vereinbarung 32

5.3 WAS BEDEUTET EINE GEMEINSAME VERANTWORTLICHKEIT FÜR DIE AUSÜBUNG DER RECHTE BETROFFENER PERSONEN? 33

5.4 WIE STEHT ES UM DIE HAFTUNG DER AN EINER GEMEINSAMEN VERANTWORTLICHKEIT BETEILIGTEN PARTEIEN? 34

6. Anhang 1 36

7. Anhang 2 37

8. Anhang 3 39

1. Einleitung

Nach dem Inkrafttreten der Datenschutz-Grundverordnung[1] (im Folgenden „DSGVO“) und der Verordnung (EU) 2018/1725[2] (im Folgenden „Verordnung“) wurden zahlreiche Fragen zu den Änderungen der Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“ und ihrer jeweiligen Aufgaben und insbesondere zu den Auswirkungen des Begriffs „gemeinsam Verantwortliche“ (im Sinne von Artikel 28 der Verordnung) aufgeworfen.

Bei der Verarbeitung personenbezogener Daten müssen Organe und Einrichtungen der EU (nachstehend „EU-Institutionen“) spezifische Datenschutzvorschriften einhalten. Ihre Pflichten unterscheiden sich je nach ihrer Rolle. Die folgenden Leitlinien sollen EU-Institutionen praktische Ratschläge und Anweisungen zur Einhaltung der Verordnung geben, indem sie Erläuterungen zu den Begriffen „Verantwortlicher“, „Auftragsverarbeiter“ und „gemeinsam Verantwortliche“ auf der Grundlage der in der Verordnung enthaltenen Definitionen bereitstellen. Wir hoffen, für mehr Klarheit bezüglich der Rolle dieser Akteure bei bestimmten Verarbeitungsvorgängen und ihrer Auswirkungen auf Pflichten nach der Verordnung zu sorgen.

Als unabhängige Aufsichtsbehörde mit Zuständigkeit für die Verarbeitung personenbezogener Daten durch EU-Institutionen kann der EDSB unter anderem Leitlinien zu bestimmten Aspekten im Zusammenhang mit der Verarbeitung personenbezogener Daten herausgeben.

Diese Leitlinien sollten von Datenschutzbeauftragten (DSB) und Datenschutzkoordinatoren oder -kontakten (DSK) sowie von allen Personen, die als Verantwortliche, Auftragsverarbeiter oder gemeinsam Verantwortliche für EU-Institutionen verantwortlich sind, herangezogen werden. Sie helfen der oberen Führungsebene zudem dabei, von höchster Stelle der Organisation aus eine Datenschutzkultur zu fördern und den Grundsatz der Rechenschaftspflicht umzusetzen.

Der Zweck dieser Leitlinien besteht darin, EU-Institutionen die Erfüllung ihrer Pflichten zu erleichtern. Nach dem Grundsatz der Rechenschaftspflicht bleiben EU-Institutionen für die Einhaltung ihrer Verpflichtungen verantwortlich. EU-Institutionen können sich unter Berücksichtigung ihres spezifischen Bedarfs auch für andere, nicht in diesem Dokument aufgeführte Maßnahmen entscheiden, die gleichermaßen wirksam sind. In diesem Fall müssen sie nachweisen, auf welche Weise sie durch diese anderen Maßnahmen einen gleichwertigen Schutz erreichen wollen.

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016. S. 1.

[2] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 vom 21.11.2018, S. 39.

2. Anwendungsbereich und Gliederung der Leitlinien

2.1 Anwendungsbereich der Leitlinien

Dieses Dokument bietet EU-Institutionen Leitlinien zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche", um für mehr Klarheit über deren Rolle bei der Verarbeitung personenbezogener Daten zu sorgen und so ihre Zuständigkeiten zu bestimmen und die Verordnung einzuhalten.

Ein weiterer Schwerpunkt liegt auf der Darstellung von Beispielen für diese Begriffe anhand zusätzlicher Fallstudien und Checklisten, um die Verordnung praxisnah zu erläutern.

Die Leitlinien befassen sich insbesondere mit

- den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" im Einklang mit den Rechtsvorschriften und der Rechtsprechung;

- der Verteilung ihrer Pflichten und Zuständigkeiten, insbesondere im Hinblick auf die Ausübung der Rechte der betroffenen Person;

- konkreten Fallstudien zu den Konstellationen Verantwortlicher-Auftragsverarbeiter, einzelne Verantwortliche und gemeinsam Verantwortliche.

Zur Untermauerung der Leitlinien sind in den Anhängen folgende Informationen zu finden:

- ein Flussdiagramm, aus dem hervorgeht, ob Ihr Organ oder Ihre Einrichtung als Verantwortlicher, Auftragsverarbeiter oder gemeinsam Verantwortlicher angesehen werden kann;

- Checklisten zu den Pflichten von Verantwortlichen und Auftragsverarbeitern.

Nicht Gegenstand dieses Dokuments sind:

- Musterklauseln für Verträge zwischen Verantwortlichen und Auftragsverarbeitern oder Vereinbarungen zwischen gemeinsam Verantwortlichen – der EDSB wird hierzu separate Leitlinien veröffentlichen;

- Garantien für Übermittlungen in Länder außerhalb der EU/des EWR – der EDSB wird hierzu separate Leitlinien veröffentlichen.

Dieses Dokument gilt auch unbeschadet etwaiger Aktualisierungen, die im Lichte künftiger Datenschutzvorschriften der EU, der Rechtsprechung und spezifischer Leitlinien zu den fraglichen Konzepten und ihren Auswirkungen in Bezug auf Verantwortlichkeiten und Haftung erforderlich sein könnten.

2.2 Aufbau der Leitlinien

Die Leitlinien sind wie folgt gegliedert:

- In Kapitel 1 wird der Zweck der Leitlinien erörtert.
- In Kapitel 2 sind Anwendungsbereich und Gliederung des Dokuments beschrieben.
- In Kapitel 3 wird der Begriff „Verantwortlicher“ erläutert, werden seine Aufgaben und Zuständigkeiten definiert und anschließend einige Fallstudien vorgestellt.
- Kapitel 4 befasst sich mit dem Begriff des Auftragsverarbeiters, definiert seine Aufgaben und Zuständigkeiten und stellt anschließend einige Fallstudien vor.
- In Kapitel 5 geht es um „gemeinsam Verantwortliche“, werden ihre Aufgaben und Zuständigkeiten definiert und anschließend einige Fallstudien vorgestellt.
- Anhang 1 enthält ein Diagramm, aus dem hervorgeht, ob es sich bei Ihrer Einrichtung um einen Verantwortlichen, einen Auftragsverarbeiter oder einen gemeinsam Verantwortlichen handelt.
- Anhang 2 enthält eine Checkliste, in der die Pflichten eines Verantwortlichen im Einzelnen aufgeführt sind.
- Anhang 3 enthält eine Checkliste, in der die Pflichten eines Auftragsverarbeiters beschrieben sind.

3. Der Begriff des „Verantwortlichen“

Gemäß Artikel 3 Absatz 8 der Verordnung bezeichnet der Ausdruck „Verantwortlicher“ „*das Organ oder die Einrichtung der Union oder die Generaldirektion oder sonstige Organisationseinheit, das bzw. die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten bestimmt; sind die Zwecke und Mittel dieser Verarbeitung durch einen besonderen Rechtsakt der Union bestimmt, so kann der Verantwortliche bzw. können die bestimmten Kriterien für seine Benennung nach dem Unionsrecht vorgesehen werden*“.

Ähnlich wie in Artikel 4 Absatz 7 DSGVO wird der „Verantwortliche“ durch fünf Elemente identifiziert, die jedes für sich in diesem Kapitel analysiert werden. In der DSGVO ist der „Verantwortliche“ mit etwas anderen Worten definiert, und zwar als „*die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (...)*“. Beide Begriffsbestimmungen heben jedoch im Wesentlichen auf die Funktion ab: Die Stelle, die, unabhängig von ihrem organisatorischen Status, über das „Was“ und „Wie“ der Verarbeitung entscheidet, ist der Verantwortliche.

3.1 Definition des „Verantwortlichen“

3.1.1 „Das Organ oder die Einrichtung der Union, die Generaldirektion oder jede andere organisatorische Einheit“

Der erste Teil der Begriffsbestimmung bezieht sich auf **die Art der Akteure, die nach der Verordnung Verantwortliche sein können, d. h. Organe und Einrichtungen der EU, eine Generaldirektion oder jede andere organisatorische Einheit**. Dieses Element unterstreicht die Tatsache, dass alle Organe, Agenturen, Einrichtungen oder Generaldirektionen (also organisatorische Einheiten, die in den meisten der größten EU-Institutionen anzutreffen sind) als für die Durchführung bestimmter Verarbeitungsvorgänge „Verantwortlicher“ angesehen werden können.

Somit ist klar, dass **Generaldirektionen und andere organisatorische Einheiten als Verantwortliche fungieren können (und als gemeinsam Verantwortliche**, wie in Kapitel 5 dieser Leitlinien noch betrachtet werden wird).

3.1.2 „Bestimmt“

Das zweite Element des Begriffs des Verantwortlichen bezieht sich auf den **faktischen Einfluss, den der Verantwortliche auf den Verarbeitungsvorgang nimmt**, indem er eine Entscheidungsbefugnis ausübt.[3]

Wie lässt sich dies in der Praxis prüfen? Um den „faktischen Einfluss“ eines Verantwortlichen auf den Verarbeitungsvorgang zu beurteilen, sollten die faktischen Elemente in ihrer Gesamtheit durch Beantwortung folgender Fragen beurteilt werden: ***„Warum findet die***

[3] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, S. 10.

Verarbeitung statt?“ , „Wer hat die Verarbeitung veranlasst?“[4] und ***„Wer zieht einen Nutzen aus der Verarbeitung?“***[5].

Eine solche Verantwortung kann abgeleitet werden:

a) Aus ausdrücklicher rechtlicher Zuständigkeit

Artikel 3 Absatz 8 der Verordnung besagt: “(...) *„(...); sind die Zwecke und Mittel dieser Verarbeitung durch einen besonderen Rechtsakt der Union bestimmt, so kann der Verantwortliche bzw. können die bestimmten Kriterien für seine Benennung nach dem Unionsrecht vorgesehen werden*”. Hat der EU-Gesetzgeber den Verantwortlichen in einem besonderen Rechtsakt der Union ausdrücklich benannt, sollte die Bestimmung des Verantwortlichen grundsätzlich einfach zu bewerkstelligen sein.

Der EDSB empfiehlt, den Verantwortlichen für (einen) bestimmte(n) Verarbeitungsvorgang/-vorgänge bereits im Basisrechtsakt zu bestimmen, damit die Bestimmung des Verantwortlichen von Anfang an geklärt ist und etwaige Auslegungsprobleme bei der Bewertung der Funktion vermieden werden.[6]

- Ein Beispiel für eine solche im Gesetz vorgesehene ausdrückliche rechtliche Zuständigkeit findet sich in Artikel 57 und 58 der ETIAS-Verordnung, in denen die Aufgaben des Verantwortlichen und des Auftragsverarbeiters für die Verarbeitung personenbezogener Daten ausdrücklich festgelegt sind.[7]

b) Aus impliziter Zuständigkeit

In Ermangelung einer ausdrücklichen Zuständigkeit **kann die Zuständigkeit einer Partei als Verantwortlicher aus impliziter Zuständigkeit abgeleitet werden**. In diesem Fall ist die Funktion des Verantwortlichen nicht ausdrücklich gesetzlich geregelt. Wenn einer Partei jedoch eine spezifische Aufgabe übertragen wird, in deren Rahmen sie bestimmten Verpflichtungen nachkommen muss, die mit der Verarbeitung personenbezogener Daten verbunden sind, würde sich die Rolle des Verantwortlichen letztlich aus den ihr übertragenen Aufgaben und Pflichten ergeben.

- Ein Beispiel einer solchen Funktion, die sich aus impliziter Zuständigkeit ergibt, ist die Verordnung über die Einrichtung der EMA[8]: In dieser Verordnung wird die EMA

[4] Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, S. 11.
[5] Siehe Rechtssache C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn. 40 und Schlussanträge von Generalanwalt Bot in der Rechtssache C-210/16, *Wirtschaftsakademie*, Rn. 64 und 65. Rechtssache C-40/17, *Fashion ID GmbH & Co.KG gegen Verbraucherzentrale NRW e.V.*, ECLI:EU:C:2019:629, Rn. 78-81 und Schlussanträge von Generalanwalt Bobek in der Rechtssache C-40/17, *Fashion ID*, Rn. 68-70.
[6] Eine solche Bestimmung muss natürlich mit den tatsächlichen Zuständigkeiten in Einklang stehen, die den verschiedenen Akteuren durch den Rechtsakt zugewiesen werden.
[7] Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226, Artikel 57 und 58.
[8] Verordnung (EG) Nr. 726/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Festlegung von Unionsverfahren für die Genehmigung und Überwachung von Human- und Tierarzneimitteln und zur Errichtung einer Europäischen Arzneimittel-Agentur, Abl. L 136 vom 30.4.2004, S. 1, z. B. Artikel 24.

zwar nicht ausdrücklich als „Verantwortlicher“ für bestimmte (Gruppen von) Verarbeitungsvorgänge(n) bezeichnet, doch werden ihr darin spezifische Aufgaben und damit verbundene Pflichten zugewiesen. Um diese Aufgaben (z. B. die Verwaltung bestimmter Datenbanken) wahrnehmen zu können, muss die Agentur personenbezogene Daten verarbeiten, was auch datenschutzrechtliche Zuständigkeiten mit sich bringt. Dies ist ein klarer Hinweis darauf, dass es sich bei der betreffenden Stelle um einen „Verantwortlichen“ handelt.

In Ermangelung ausdrücklicher oder impliziter Zuständigkeiten können die Verantwortung und die Rolle der Partei durch eine Beurteilung der tatsächlichen Umstände bestimmt werden, unter denen die Stelle im Rahmen eines bestimmten Verarbeitungsvorgangs tätig ist.[9]

3.1.3 „Zwecke und Mittel“

Das dritte Element der Definition bezieht sich auf den Wesensgehalt des Einflusses des Verantwortlichen, nämlich die Bestimmung der Zwecke und Mittel des Verarbeitungsvorgangs. **Die Ermittlung des „*Warum*“ und des „*Wie*“ eines Verarbeitungsvorgangs ist der Faktor, aufgrund dessen eine Stelle die Rolle des „Verantwortlichen“ im Sinne des Datenschutzrechts übernimmt**. Bei der Durchführung eines Verarbeitungsvorgangs ist **der Verantwortliche derjenige, der über den Zweck („*Warum*“) und über die Mittel („*Wie*“) der Verarbeitung bestimmt.[10]**

In dieser Hinsicht kann das Ausmaß des Einflusses einer Partei bei der Bestimmung sowohl des Zwecks als auch der Mittel ihre Rolle als Verantwortlicher bestimmen. Es sei darauf hingewiesen, dass eine Partei, auch wenn **Zwecke und Mittel** miteinander verknüpft sind, nicht über beides gleichermaßen bestimmen muss, um als Verantwortlicher für die Verarbeitung personenbezogener Daten zu gelten: *de facto* hängt dies auch von dem spezifischen Kontext ab, in dem der Verarbeitungsvorgang ablaufen soll.

Die entscheidende Frage lautet also, **wie detailliert** eine Partei die Zwecke und Mittel bestimmen sollte, um als Verantwortlicher zu gelten.

Bei der Beurteilung der **Bestimmung des Zwecks** ist der Akteur, der über den Grund bestimmt, aus dem eine bestimmte Verarbeitung stattfinden soll, also über das *„Wofür“* der Durchführung der Verarbeitung, der Verantwortliche im Sinne des Datenschutzrechts. Mit anderen Worten: Ein Verantwortlicher ist **die Stelle, die *de facto* über den Zweck („*Warum*“) eines Verarbeitungsvorgangs bestimmt.**

Was die **Bestimmung der Mittel** angeht, so umfasst der Begriff verschiedene Elemente und bezieht sich insbesondere auf die technischen und organisatorischen Maßnahmen, die bei der Durchführung einer bestimmten Verarbeitung ergriffen werden. Allerdings **hat die**

[9] Da es sehr wahrscheinlich ist, dass die Rolle von Organen und Einrichtungen der EU durch ausdrückliche oder implizite Zuständigkeit festgelegt ist, befassen sich diese Leitlinien mit diesen Aspekten nicht im Einzelnen. Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, S. 12 und 13.

[10] Siehe Rechtssache C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388, Rn. 34-36, sowie die Schlussanträge von Generalanwalt Bot in *Wirtschaftsakademie*, Rn. 46ff.

Bestimmung über die bei einer bestimmten Verarbeitung einzusetzenden Mittel die Funktion des Verantwortlichen nur dann zur Folge, wenn die Partei über die wesentlichen Elemente der Mittel entscheidet.[11] Gemäß dem von der Artikel 29-Datenschutzgruppe in ihrer Stellungnahme verfolgten Ansatz sind Beispiele für solche „wesentlichen Elemente der Mittel": die Art(en) der zu verarbeitenden Daten; der Zeitraum, für den sie gespeichert werden sollen; von welchen betroffenen Personen die Daten erhoben werden sollen; wer Zugriff auf die Daten hat (Zugangskontrolllisten, Nutzerprofile usw.) und die Empfänger der Daten usw., bei denen in der Regel die Bestimmung dem Verantwortlichen vorbehalten ist.

Im Hinblick auf die Bestimmung **eher praktischer Aspekte der Verarbeitung(en), die so genannten „nicht wesentlichen Elemente der Mittel"**, vertritt die Artikel 29-Datenschutzgruppe in derselben Stellungnahme die Auffassung, dass es sich hierbei um die eingesetzte Hardware oder Software oder die technischen Sicherheitsmaßnahmen handelt. Es kann durchaus vorkommen, dass diese vom Auftragsverarbeiter ermittelt und bestimmt werden, soweit dies nach den allgemeinen Weisungen des Verantwortlichen erfolgt. Auf die Rolle des Auftragsverarbeiters wird im nächsten Kapitel näher eingegangen.

Folglich **ist die Bestimmung des Zwecks ausschließlich dem für einen Verarbeitungsvorgang Verantwortlichen vorbehalten**. Andererseits wird von dem Verantwortlichen **nur verlangt, die „wesentlichen Elemente" der Mittel einer Verarbeitung festzulegen**. Denkbar ist, dass ein Auftragsverarbeiter, der im Interesse des Verantwortlichen handelt, die nicht wesentlichen Mittel der Verarbeitungsvorgänge, wie die zu verwendende Software oder die gegebenenfalls zu ergreifenden technischen und organisatorischen Maßnahmen, ermittelt und somit den Verantwortlichen bei der Erfüllung seiner datenschutzrechtlichen Verpflichtungen unterstützt.[12]

BEISPIEL:

Im Einklang mit den in seiner Gründungsverordnung festgelegten Befugnissen beschließt das OLAF, bei einer EU-Institution eine Untersuchung wegen Betrugsverdachts einzuleiten, und fordert diese auf, spezifische Informationen über einen Betrugsfall (der in der Regel personenbezogene Daten enthält) vorzulegen. Die Institution muss dem nachkommen, fragt sich jedoch, ob sie als gemeinsam Verantwortlicher im Sinne von Artikel 28 der Verordnung einzustufen ist.

Entscheidend für das Vorliegen einer gemeinsamen Verantwortlichkeit ist die gemeinsame Festlegung des Zwecks und der Mittel der Verarbeitungsvorgänge. Wenn die Beteiligten nicht gemeinsam dasselbe allgemeine Ziel (oder denselben allgemeinen Zweck) festlegen oder ihre Verarbeitungen nicht auf gemeinsam festgelegte Mittel stützen, dürfte ihr Verhältnis eher auf eine „getrennte Verantwortung" hindeuten.

[11] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter"(...) *wohingegen die Entscheidung über die Mittel nur dann die Verantwortung für die Verarbeitung impliziert, wenn über wesentliche Aspekte der Mittel entschieden wird*.", S. 17.

[12] Siehe z. B. die Verpflichtungen für Verantwortliche in der Verordnung, Artikel 26, 27 und 33.

Im vorliegenden Fall ist offensichtlich, dass die beiden Institutionen den Zweck der Verarbeitung nicht gemeinsam bestimmen. Das Organ/die Agentur/die Einrichtung verarbeitet personenbezogene Daten für einen bestimmten Zweck, z. B. ein Vergabeverfahren. Dies ist nicht deckungsgleich mit dem Zweck der Verarbeitungsvorgänge des OLAF, nämlich der Untersuchung mutmaßlichen Betrugs. Darüber hinaus verarbeitet jede der beteiligten Parteien personenbezogene Daten unabhängig von den Mitteln, die der andere Verantwortliche verwendet.

Daher läuft diese Situation auf eine getrennte Verantwortlichkeit hinaus.

Eine Stelle braucht keinen Zugang zu personenbezogenen Daten zu haben, um als Verantwortlicher zu gelten. Es reicht aus, wenn sie über die Zwecke und Mittel der Verarbeitung bestimmt, Einfluss auf die Verarbeitung hat, indem sie die Aufnahme der Verarbeitung personenbezogener Daten veranlasst (und diese einstellen kann), oder wenn sie anonyme Statistiken auf der Grundlage personenbezogener Daten erhält, die von einer anderen Stelle erhoben und verarbeitet werden.[13]

3.1.4 „Allein oder gemeinsam mit anderen“

Artikel 3 Absatz 8 der Verordnung (und genauso Artikel 4 Absatz 7 DSGVO) **räumt die Möglichkeit ein, dass der Zweck und die Mittel eines bestimmten Verarbeitungsvorgangs von mehr als einem Akteur festgelegt werden**. Mit dieser Spezifikation wird ausdrücklich klargestellt, dass sich der Begriff der Verantwortlichkeit nicht zwingend auf eine einzige Stelle bezieht, sondern auch mehrere Beteiligte einbeziehen kann, die bei einem Verarbeitungsvorgang eine Rolle spielen. Das bedeutet und wurde auch vom EuGH bestätigt, dass jeder beteiligte Akteur datenschutzrechtliche Pflichten hat.[14] In Kapitel 5 der Leitlinien wird näher auf die Situation „gemeinsame Verantwortlichkeit“ eingegangen.[15]

---

[13] Siehe hierzu Rechtssache C-25/17 *Jehovan todistajat* ECLI:EU:C:2018, Rn. 68 bis 72 sowie Rechtssache C-210/16 *Wirtschaftsakademie Schleswig-Holstein* und Rechtssache C-40/17 *FashionID & Co.KG gegen Verbraucherzentrale NRW e. V.* Darüber hinaus ist es nicht erforderlich, dass der Verantwortliche bei der Verarbeitung zwischen personenbezogenen Daten und anderen Arten von Informationen unterscheidet. Siehe hierzu Rn. 28 und 41 des Urteils in der Rechtssache C-131/12 *Google Spain*, in dem der Gerichtshof die Ansicht vertritt, dass
- die Suchmaschinen nicht zwischen personenbezogenen Daten und anderen Arten von Informationen unterscheiden, die sie erheben, indizieren und speichern, und dass
- die Verarbeitung von Informationen durch Suchmaschinen eine Verarbeitung personenbezogener Daten ist, wenn diese Informationen personenbezogene Daten enthalten.
Wenn ein Akteur die Zwecke und Mittel einer Verarbeitung festlegt, die Verarbeitung aber in keiner ihrer Phasen irgendwie mit personenbezogenen Daten zu tun hat, kann dieser Akteur nicht als Verantwortlicher im Sinne des Datenschutzrechts angesehen werden.

[14] Siehe Rechtssache C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, Rn. 29.

[15] Als Zusatzspezifikation, wenn eine EU-Institution möglicherweise eine besondere Vereinbarung mit internationalen Organisationen eingehen muss, und in Anbetracht der Tatsache, dass diese einen Sonderstatus haben, kann auch eine Verwaltungsvereinbarung getroffen werden. Da dies zwangsläufig in den Bereich von **Datenübermittlungen** fallen würde, können gemäß Artikel 48 Absatz 3 Buchstabe a der Verordnung *„geeignete Garantien auch insbesondere bestehen in (...) Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, (...).“*

3.1.5 „Der Verarbeitung personenbezogener Daten“

Gemäß Artikel 3 Absatz 3 der Verordnung bezeichnet der Ausdruck „Verarbeitung“ *„jeden Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (...)“.* Dies bedeutet, dass **ein oder mehrere Verarbeitungsvorgänge mit dem Begriff des Verantwortlichen verknüpft werden können**. Legt man die Verordnung wörtlich aus, handelt es sich bei jeder Maßnahme (Erheben, Speicherung, Analyse, Verbreitung usw.) um einen gesonderten Verarbeitungsvorgang. In der Praxis werden Verarbeitungsvorgänge in Gruppen von Verarbeitungsvorgängen zusammengefasst, die einem bestimmten Zweck dienen. Verantwortliche verfügen bei der Festlegung der Grenzen von Gruppen von Verarbeitungsvorgängen über einen gewissen Ermessensspielraum.

So könnten Verantwortliche beispielsweise das Einstellungs- und Einstiegsverfahren für neues Personal (für EU-Institutionen bedeutet dies z. B. die Festlegung von Rechten nach dem Statut, Zugangsausweise für den physischen Zugang, Zugang zu IT-Ressourcen, die Veröffentlichung von Informationen im Intranet usw.) als einen integrierten Satz von Verarbeitungsvorgängen ansehen oder in verschiedene Gruppen von Vorgängen aufteilen. Als Faustregel sollten die Verantwortlichen dies aus der Sicht der betroffenen Personen betrachten: Ist für diese das Ganze als integrierter Prozess zu erkennen? So scheint beispielsweise die Aufteilung von Beurteilungsverfahren und Einlegung von Rechtsbehelfen in zwei Vorgänge zu eng zu sein, während eine Zusammenfassung aller Personalverwaltungsprozesse zu weit gefasst wäre.

Die Verantwortung eines bestimmten Akteurs kann sich auf die gesamte Verarbeitung erstrecken, aber auch auf einen ihrer spezifischen Vorgänge beschränkt sein.[16]

BEISPIEL:

Eine EU-Institution beschließt, die Bewachung ihrer Räumlichkeiten an ein externes Unternehmen zu vergeben. Dieses Unternehmen verwaltet sein eigenes Personal; die EU-Institution ist nicht an der Aufstellung der Dienstpläne usw. beteiligt, sondern verlangt lediglich, dass an bestimmten Kontrollpunkten eine bestimmte Anzahl von Wachleuten anwesend zu sein hat. Gelten nun die beiden Parteien als gemeinsam Verantwortliche für die Verarbeitung personenbezogener Daten des Wachpersonals für die HR-Verwaltung durch das externe Unternehmen, z. B. für die Leistungsbewertung? Würde sich etwas an der Situation ändern, wenn die EU-Institution dem externen Unternehmen auch die Registrierung von Besuchern in ihren Räumlichkeiten übertragen würde?

Es liegt auf der Hand, dass sowohl der Zweck als auch die Mittel der Verarbeitung personenbezogener Daten des Sicherheitspersonals nicht gemeinsam von den Beteiligten bestimmt werden, da diese vom externen Dienstleister autonom festgelegt werden. Somit bestimmen die Parteien nicht gemeinsam den Zweck und die Mittel der Verarbeitungen im Rahmen der HR-Verwaltung des Personals des externen Unternehmens (des Wachpersonals). Sie würden somit als getrennt Verantwortliche für verschiedene Vorgänge im Rahmen der Gesamtverarbeitung im Zusammenhang mit der Bewachung der Räumlichkeiten der EU-Institution gelten.

[16] Siehe hierzu die Schlussanträge von Generalanwalt Bobek in der Rechtssache *Fashion ID*, Rn. 99.

Sollte jedoch das externe Unternehmen personenbezogene Daten von Besuchern der Räumlichkeiten der Institution verarbeiten, würde es auf Weisung der Institution handeln. Mit anderen Worten: Der externe Dienstleister müsste gewährleisten, dass er auf Anforderung des Verantwortlichen technische und organisatorische Maßnahmen ergreift, und würde somit als Auftragsverarbeiter für die Institution im Sinne von Artikel 29 der Verordnung fungieren. Damit bliebe die Rolle des externen Unternehmens als eigenständiger Verantwortlicher bei der Verwaltung seines eigenen Personals unberührt.

3.2 Pflichten und Haftung des Verantwortlichen

Artikel 26 Absatz 1 der Verordnung besagt: *„Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“* Darüber hinaus heißt es in Artikel 26 Absatz 2: *„(...) müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.“* Damit liegt auf der Hand, dass **die Zuständigkeit für die Einhaltung der Vorschriften primär bei dem Verantwortlichen liegt. Im Hinblick auf den Grundsatz der Rechenschaftspflicht sind Verantwortliche daher generell verpflichtet, die Einhaltung der Verordnung nachzuweisen**.

Artikel 65 der Verordnung besagt: *„Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterielle Schaden entstanden ist, hat unter den in den Verträgen vorgesehenen Voraussetzungen Anspruch auf Schadenersatz gegen das Organ oder die Einrichtung der Union auf Ersatz des erlittenen Schadens.“*

Im Gegensatz zu Artikel 82 DSGVO sieht die Verordnung jedoch nicht ausdrücklich eine Haftung des Verantwortlichen (oder des Auftragsverarbeiters) für den Fall der Nichteinhaltung vor, sondern verweist stattdessen auf die in den Verträgen festgelegten Voraussetzungen.

In Artikel 340 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) heißt es: „Die Union ersetzt den durch ihre Organe (...) verursachten Schaden nach den allgemeinen Rechtsgrundsätzen, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind.“ Darüber hinaus haftet ein Verantwortlicher im Einklang mit den Datenschutzvorschriften gegenüber der betroffenen Person für den Gesamtschaden sowohl materieller als auch immaterieller Art (Artikel 65 der Verordnung[17]). Gemäß Artikel 268 AEUV ist der Gerichtshof der Europäischen Union für Streitsachen über den in Artikel 340 AEUV vorgesehenen Schadenersatz zuständig.

3.3 Schutz betroffener Personen

Gemäß der Verordnung (Artikel 4 Absatz 2 und Artikel 14 Absätze 1 und 2) ist es Aufgabe des Verantwortlichen, dafür zu sorgen, dass betroffene Personen die ihnen

[17] Siehe auch Artikel 82 DSGVO.

durch die Artikel 17 bis 24 der Verordnung eingeräumten Rechte ausüben können. Selbst wenn eine andere Stelle als Anlaufstelle für betroffene Personen benannt wird, **bleibt der Verantwortliche letztendlich der Ansprechpartner für diese Verpflichtung.** In der jüngsten Rechtsprechung des EuGH wird bestätigt, dass der Begriff des „Verantwortlichen" weit gefasst wurde, damit betroffenen Personen ein wirksamer und umfassender Schutz gewährt werden kann, indem ein möglicher Mangel an Verantwortung in dieser Hinsicht vermieden wird.[18]

3.4 Wann ist eine EU-Institution ein Verantwortlicher? Eine Checkliste

Wir fassen das Kapitel zusammen: Wann kann eine EU-Institution als Verantwortlicher im Sinne der Verordnung gelten? Die folgende Checkliste kann EU-Institutionen dabei helfen, die relevantesten Elemente zu ermitteln, anhand derer eine Stelle als Verantwortlicher identifiziert werden kann. Wenn die meisten Aussagen mit JA beantwortet werden, dürfte Ihre EU-Institution für bestimmte Verarbeitungsvorgänge Verantwortlicher im Sinne der Verordnung sein.

	JA	NEIN
• Sie haben beschlossen, personenbezogene Daten zu verarbeiten, oder haben veranlasst, dass eine andere Stelle sie verarbeitet.		
• Sie haben entschieden, zu welchem Zweck oder zu welchem Ergebnis die Verarbeitung erfolgen soll.		
• Sie haben die wesentlichen Elemente des Verarbeitungsvorgangs festgelegt, also welche personenbezogenen Daten erhoben werden sollen, über welche Personen, wie lange die Daten gespeichert werden sollen, wer Zugang zu den Daten hat, welche Empfänger es gibt usw.		
• Die von Ihren Verarbeitungen betroffenen Personen sind Ihre Mitarbeiter.		
• Sie haben die Verarbeitung der personenbezogenen Daten nach fachlichem Ermessen beurteilt.		
• Sie haben eine direkte Beziehung zu den betroffenen Personen.		
• Sie verfügen (im Rahmen der Ihnen als öffentliche Einrichtung übertragenen Aufgaben) über Autonomie und Unabhängigkeit in Bezug auf die Art und Weise, in der die personenbezogenen Daten verarbeitet werden.		
• Sie haben einen Auftragsverarbeiter mit der Durchführung von Verarbeitungstätigkeiten in Ihrem		

[18] Rechtssache C-131/12, *Google Spain SL e Google Inc. gegen Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, ECLI:EU:C:2014:317, Rn. 34. Siehe ferner Rechtssache C-2010/16, *Wirtschaftsakademie Schleswig-Holstein*, Rn. 27-28 und Rechtssache C-25/17 *Jehovan todistajat*, Rn. 66.

Namen beauftragt, auch wenn die zu diesem Zweck ausgewählte Stelle bestimmte technische und organisatorische Mittel einsetzt (nicht wesentliche Elemente).		

Es sollte bedacht werden, dass für EU-Institutionen in den meisten Fällen die Rolle als Verantwortlicher in EU-Rechtsvorschriften festgelegt ist, weil sie entweder ausdrücklich vorgesehen ist oder weil der EU-Institution eine spezifische Verpflichtung oder Erlaubnis zur Verarbeitung von Daten im Rahmen eines Gesetzgebungsakts übertragen wurde.

4. Der Begriff des „Auftragsverarbeiters“

Gemäß Artikel 3 Absatz 12 der Verordnung bezeichnet der Ausdruck „Auftragsverarbeiter“ „(…) *eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Namen des Verantwortlichen verarbeitet*“.

Ähnlich wie in Artikel 4 Absatz 8 DSGVO wird der „Auftragsverarbeiter“ durch zwei Elemente identifiziert, die jedes für sich in diesem Kapitel analysiert werden.

4.1 Die Definition des „Auftragsverarbeiters“

4.1.1 Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Einrichtung

Wie in der DSGVO umfasst die **Definition des Begriffs „Auftragsverarbeiter“ ein breites Spektrum von Akteuren, bei denen es sich um natürliche oder juristische Personen, Behörden, Agenturen oder andere Einrichtungen[19] handelt.** Die Existenz eines Auftragsverarbeiters hängt von einer Entscheidung des Verantwortlichen ab, der beschließen kann, bestimmte Verarbeitungsvorgänge selbst durchzuführen oder die Verarbeitung ganz oder teilweise an einen Auftragsverarbeiter zu delegieren.

Artikel 3 Absatz 12 der Verordnung führt die Generaldirektionen nicht ausdrücklich als Auftragsverarbeiter im Sinne des Datenschutzrechts auf. Aus rechtlicher Sicht und gegenüber den betroffenen Personen ist somit klar, dass die EU-Institution als Auftragsverarbeiter für jeden Verstoß gegen die Verordnung verantwortlich oder haftbar ist. Es ist jedoch darauf hinzuweisen, dass in bestimmten Institutionen bestimmte Generaldirektionen der EU als „unterstützende Generaldirektionen“ fungieren, die häufig auf strenge Weisung und im Auftrag anderer Generaldirektionen (die Eigentümer des Geschäftsprozesses sind) Verarbeitungsvorgänge durchführen. Dies wäre normalerweise **nicht** bei die ganze Organisation betreffenden Verarbeitungsvorgängen der Fall, sondern eher bei spezifischen Vorgängen, die nur einer bestimmten GD oder einem bestimmten Referat gehören. Verstärkt wird dies darüber hinaus durch Dienstleistungsvereinbarungen oder andere Arbeitsvereinbarungen zwischen Generaldirektionen, in denen der Steuerungsprozess und die Aufteilung der Aufgaben und Zuständigkeiten zwischen den verschiedenen an der Verarbeitung beteiligten Organisationseinheiten festgelegt sind.

Um eine wirksame Aufteilung der Zuständigkeiten zu gewährleisten und einen besseren Schutz natürlicher Personen im Einklang mit den Datenschutzvorschriften zu gewährleisten, empfiehlt der EDSB, in internen Vereinbarungen die Rollen und Zuständigkeiten solcher GD festzulegen.

Interne Vereinbarungen innerhalb einer Institution müssen nicht so detailliert sein wie Vereinbarungen mit externen Auftragsverarbeitern, solange die Zuständigkeiten festgelegt

[19] „Andere Einrichtung“ bedeutet „jede andere Stelle“ im Sinne der DSGVO und nicht eine Einrichtung der Union.

sind. Eine solche klare Aufteilung der Aufgaben und Zuständigkeiten auf die verschiedenen an der Verarbeitung beteiligten Organisationseinheiten steht auch im Einklang mit der Notwendigkeit, die Einhaltung der Datenschutzvorschriften in vollem Umfang zu gewährleisten und zu verhindern, dass das durch die Verordnung garantierte Schutzniveau für natürliche Personen durch mangelnde Klarheit in Bezug auf die Zuständigkeiten untergraben wird.

BEISPIEL:

In einer EU-Institution ist eine GD nur für die Entwicklung und das technische Management eines IT-Tools zuständig, das eine andere Generaldirektion nutzt. Die das Tool verwendende Generaldirektion legt die Anforderungen an das IT-Tool fest. Welche Rolle hätte die GD, die das IT-Tool entwickelt?

Wie bereits erläutert, nimmt eine GD, die ein IT-Tool für andere Generaldirektionen entwickelt, betreibt und pflegt, eine Rolle wahr, die der eines Auftragsverarbeiters sehr ähnlich ist. Diese GD sollte nicht die Zwecke oder die wesentlichen Elemente der Mittel für die Verarbeitung festlegen, also das IT-Tool (z. B. Speicherfristen, Zugang zu den Daten und Datenempfänger).[20] Dies hindert die unterstützende GD nicht daran, Mittel vorzuschlagen, solange die als Verantwortlicher fungierende GD die Entscheidung trifft.

Darüber hinaus sieht die Verordnung wie bei einem Verantwortlichen auch die Möglichkeit vor, einen Auftragsverarbeiter in einem bestimmten Rechtsakt der Union zu benennen:

- Siehe z. B. Artikel 58 Absatz 1 der Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226.[21]

4.1.2 Verarbeitung im Auftrag des Verantwortlichen

Das Wesentliche der Rolle eines „Auftragsverarbeiters“ liegt darin, dass **personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet werden**. In der Praxis bestimmt der Verantwortliche den Zweck (im Rahmen der gesetzlich zugewiesenen Aufgaben) und die wesentlichen Elemente der Mittel, während der Auftragsverarbeiter eine ausführende Funktion hat. **Mit anderen Worten bedeutet „im Auftrag des Verantwortlichen handeln“, dass der Auftragsverarbeiter dem Interesse des Verantwortlichen dient, indem er eine bestimmte Aufgabe wahrnimmt und sich dabei an die Weisungen des Verantwortlichen hält, zumindest in Bezug auf den Zweck und die wesentlichen Elemente der Mittel.**

[20] Sollte dies der Fall sein, wären die Stellen gemeinsam Verantwortliche.

[21] ABl. L 236 vom 19.9.2018, S. 1. *„Artikel 58* **Auftragsverarbeiter:** Im Hinblick auf die Verarbeitung personenbezogener Daten im ETIAS-Informationssystem ist eu-LISA als Auftragsverarbeiter gemäß Artikel 2 Buchstabe e der Verordnung (EG) Nr. 45/2001 anzusehen.“

Die Hauptverpflichtung zur Einhaltung der Vorschriften liegt bei dem Verantwortlichen. Es muss jedoch gesehen werden, dass der Auftragsverarbeiter nicht zwangsläufig der „Untergebener“ des Verantwortlichen ist. Die Tatsache, dass der Auftragsverarbeiter „im Auftrag des Verantwortlichen“ handelt, beeinträchtigt nicht unbedingt seine Unabhängigkeit bei der Wahrnehmung der ihm übertragenen spezifischen Aufgaben. Der Auftragsverarbeiter kann bei der Erbringung seiner Dienstleistungen über ein erhebliches Maß an Autonomie verfügen und ermittelt möglicherweise die nicht wesentlichen Elemente des Verarbeitungsvorgangs.

So ist beispielsweise eine Agentur oder Einrichtung, die Untersuchungsleistungen erbringt und im Auftrag einer anderen EU-Institution handelt (und somit über eingeführte Arbeitsverfahren verfügt), im Rahmen eines Einzelvertrags oder eines anderen Rechtsinstruments berechtigt, ihre operative und organisatorische Unabhängigkeit bei der Erfüllung ihrer Kernaufgaben zu wahren, da die Art ihres Auftrags ein gewisses Maß an Unabhängigkeit erfordert. Dies ist jedoch darauf zurückzuführen, dass sich der Verantwortliche dafür entschieden hat, dem Auftragsverarbeiter diese operative Unabhängigkeit zu gewähren. Es ist Sache der beiden beteiligten Parteien, sich über die Akzeptanz der eingeführten Verfahren sowie über die Rollen und Modalitäten zu einigen, in deren Rahmen bestimmte Verarbeitungsvorgänge durchgeführt werden. Der Auftragsverarbeiter kann bestimmte Maßnahmen (insbesondere in seinem Fachbereich) anraten oder vorschlagen, doch ist es Sache des Verantwortlichen, zu entscheiden, ob er diesen Rat oder Vorschlag akzeptiert, nachdem er umfassend über die Gründe für die Maßnahmen, die Art der Maßnahmen und ihre Umsetzung informiert wurde. Mit anderen Worten, damit eine Organisation „im Auftrag“ eines Verantwortlichen handeln und somit als Auftragsverarbeiter gelten kann, ist es nicht erforderlich, dass der Verantwortliche alle Modalitäten vorschreibt, nach denen ein bestimmter Verarbeitungsvorgang durchgeführt werden sollte.

Handelt ein Auftragsverarbeiter jedoch über sein Mandat hinaus, indem er gegen den Vertrag oder ein anderes Rechtsinstrument verstößt oder Entscheidungen über den Zweck und die wesentlichen Elemente der Mittel eines bestimmten Verarbeitungsvorgangs trifft, kann er als Verantwortlicher (oder gemeinsam Verantwortlicher) eingestuft werden.

In der Praxis kommt es durchaus vor, dass der Auftragsverarbeiter über seine Rolle hinausgeht, indem er außerhalb der Vereinbarung handelt oder Entscheidungen über den Zweck und die wesentlichen Elemente der Mittel eines bestimmten Verarbeitungsvorgangs trifft. Ob dies nun bedeutet, dass ein Auftragsverarbeiter automatisch (mit allen damit verbundenen Verantwortlichkeiten) als Verantwortlicher eingestuft werden sollte, hängt unter anderem von der Art der Abweichung ab, ob also z. B. ein solches Verhalten dazu dient, die Einhaltung der Datenschutzgrundsätze zu gewährleisten. Wenn der Auftragsverarbeiter jedoch die Daten für seine eigenen Zwecke weiterverwendet und damit die in der Vereinbarung mit dem Verantwortlichen festgelegten allgemeinen Regeln und die Zwecke eindeutig überschreitet, würde dies einer klaren Verletzung seiner Pflichten gleichkommen.

BEISPIELE:

1. **Mit einer Richtlinie wird ein freiwilliges Netz aus von den Mitgliedstaaten benannten und für ein bestimmtes Thema zuständigen Behörden geschaffen. Die Richtlinie sieht ferner vor, dass Institution A als Sekretariat des Netzes fungiert. Eines der Hauptziele des Netzes ist die Verbesserung der Interoperabilität zwischen den nationalen IT-Systemen in diesem Bereich durch den Austausch personenbezogener Daten. Um einen solchen Austausch zu erleichtern, hat das Netz beschlossen, ein von Institution A entwickeltes und implementiertes IT-Tool einzurichten. Auf Ersuchen der Kontaktstellen der Mitgliedstaaten werden personenbezogene Daten an einen oder mehrere Mitgliedstaaten übermittelt. Die Art der Daten, die innerhalb des interoperablen IT-Instruments ausgetauscht werden sollen, ist in vom Netz angenommenen Leitlinien festgelegt und wird durch die Anwendung spezifischer Vereinbarungen zwischen den Kontaktstellen der Mitgliedstaaten geregelt. Institution A ist in ihrer Rolle als Sekretariat des Netzes nicht am Entscheidungsprozess in Bezug auf die Gestaltung und die Funktionen des Systems als solches beteiligt, sondern berät ausschließlich über die technische und rechtliche Durchführbarkeit der gewählten Option.**

Nach der Beschreibung des Falls ist der Zweck der Verarbeitung personenbezogener Daten innerhalb des Interoperabilitäts-IT-Tools in der Richtlinie festgelegt. Darüber hinaus wird mit derselben Richtlinie Institution A als Sekretariat des Netzes eingesetzt. Die Entscheidungen über die Arten der auszutauschenden Daten und das zu verwendende System werden in Leitlinien des Netzes und in spezifischen Vereinbarungen zwischen den Kontaktstellen der Mitgliedstaaten getroffen. Gehen wir ferner davon aus, dass in einem Durchführungsrechtsakt die spezifische Aufgaben von Institution A geregelt sind, also die Pflicht, das IT-Tool zu verwalten und seine Sicherheit zu gewährleisten, sowie die Pflicht, den Verantwortlichen die Informationen zur Verfügung zu stellen, die sie für den Nachweis der Erfüllung ihrer Pflichten benötigen.

Der bisherigen Beschreibung ist zu entnehmen, dass die IT-Plattform, über die personenbezogene Daten ausgetauscht werden, eigentlich ein Mittel zur Kommunikation zwischen Datenbanken der Mitgliedstaaten ist. Angesichts des Rechtsrahmens für die Festlegung der Zwecke und Mittel der Infrastruktur und in Anbetracht der strengen Beschränkung der Aufgaben von Institution A auf die Gewährleistung der Sicherheit der Kerndienste der interoperablen IT-Tool-Plattform kann Institution A in diesem Beispiel als Auftragsverarbeiter betrachtet werden, der im Auftrag der Mitgliedstaaten handelt.

4.2 Die Wahl des Auftragsverarbeiters durch den Verantwortlichen

In Artikel 29 Absatz 1 der Verordnung heißt es: *„(...) so arbeitet der Verantwortliche nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“* Damit **ist der Verantwortliche verpflichtet, zu prüfen, ob die vom Auftragsverarbeiter angebotenen Garantien hinreichend sind. Mit Blick auf den**

Grundsatz der Rechenschaftspflicht sollte der Verantwortliche nachweisen können, dass er alle in der Verordnung vorgesehenen Elemente ernsthaft bedacht hat.

Der Verantwortliche kann berücksichtigen, ob der Auftragsverarbeiter **angemessene Unterlagen** zum Nachweis der Konformität vorlegt, z. B. Datenschutzhinweise, Grundsätze für die Verwaltung von Aufzeichnungen, Strategien für die Informationssicherheit, externe Prüfberichte, Zertifizierungen usw. **Der Verantwortliche sollte das Fachwissen des Auftragsverarbeiters (z. B. technisches Fachwissen beim Umgang mit Datenschutzverletzungen und Sicherheitsmaßnahmen), die Zuverlässigkeit und seine Ressourcen berücksichtigen.** Nur wenn der Verantwortliche nachweisen kann, dass der Auftragsverarbeiter geeignet ist, kann er eine Vereinbarung abschließen, die den Anforderungen von Artikel 29 der Verordnung Genüge tut. Ungeachtet dessen muss der Verantwortliche weiterhin den Grundsatz der Rechenschaftspflicht einhalten und regelmäßig überprüfen, ob der Auftragsverarbeiter die Vorschriften einhält und welche Maßnahmen er anwendet.

Vor der Auslagerung der Verarbeitung und zur Vermeidung eventueller Probleme **sollte der Verantwortliche mit der anderen Stelle einen Vertrag, ein anderes Rechtsinstrument oder eine verbindliche Vereinbarung schließen, in dem/der bereits klare und präzise Datenschutzverpflichtungen festgelegt sind.**

Daher möchte der EDSB folgende Empfehlungen an die EU-Institutionen richten:

- Setzen Sie nur Auftragsverarbeiter ein, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet.
- Sorgen Sie dafür, dass der Auftragsverarbeiter ohne vorherige schriftliche Genehmigung des Verantwortlichen keine weitere Auslagerung/Unterauftragsvergabe vornimmt.
- Stellen Sie sicher, dass der Auftragsverarbeiter den Verantwortlichen über etwaige Änderungen auf dem Laufenden hält und ihm die Möglichkeit gibt, Widerspruch einzulegen.
- Unterzeichnen Sie einen schriftlichen Vertrag oder eine andere (verbindliche) Rechtsvereinbarung mit dem Auftragsverarbeiter mit spezifischen Datenschutzklauseln.
- Sorgen Sie dafür, dass dieselben vertraglichen Verpflichtungen an jeden ausgewählten Unterauftragnehmer weitergegeben werden.
- Im Fall von der DSGVO unterliegenden Auftragsverarbeitern sorgen Sie dafür, dass diese die Einhaltung der DSGVO als eines der Elemente vorsehen, die als Nachweis hinreichender Garantien zu verwenden sind.

Gestützt auf die Empfehlungen und die Beurteilung des möglichen Auftragsverarbeiters und im Einklang mit Artikel 29 der Verordnung **schließt der Verantwortliche eine verbindliche Vereinbarung mit dem Auftragsverarbeiter, der dieselben Verpflichtungen gemäß Verordnung und DSGVO erfüllen muss.**

Der Auftragsverarbeiter darf personenbezogene Daten nur nach dokumentierten Weisungen des Verantwortlichen verarbeiten, soweit er nicht nach dem Unionsrecht oder dem Recht eines Mitgliedstaats dazu verpflichtet ist. Der Auftragsverarbeiter ist ferner verpflichtet, den Verantwortlichen zu unterstützen

- bei der Erfüllung der Pflicht des Verantwortlichen, die Rechte der betroffenen Personen zu gewährleisten, und
- bei der Erfüllung der Pflichten des Verantwortlichen nach den Artikeln 33 bis 41 der Verordnung (Sicherheit und Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzung und vorherige Konsultation, Vertraulichkeit der elektronischen Kommunikation, Information und Konsultation des EDSB).

Der Verantwortliche muss daher klare Modalitäten für eine solche Unterstützung festlegen und dem Auftragsverarbeiter genaue Anweisungen geben, wie er diese zu leisten hat, z. B. in dem Vertrag oder einer anderen (verbindlichen) Vereinbarung.

Ist beispielsweise der Auftragsverarbeiter die einzige Stelle, die in der Praxis in der Lage sein könnte, betroffenen Personen die Ausübung ihrer Rechte zu gewähren, wird von ihm erwartet, dass er dem Verantwortlichen alle Informationen zur Verfügung stellt, damit der Verantwortliche der betroffenen Person antworten kann. Da sich zudem der Verantwortliche und der Auftragsverarbeiter ihrer jeweiligen Zuständigkeiten bewusst sind und diese durch einen spezifischen Vertrag, ein anderes Rechtsinstrument oder eine verbindliche Vereinbarung vereinbart haben, kann es für den Verantwortlichen außerdem möglich sein, einen Antrag an den Auftragsverarbeiter zu übermitteln, wenn dieser als einzige Stelle der betroffenen Person ihre Rechte gewähren kann. Wir empfehlen, dass sich in der Vereinbarung zwischen Verantwortlichen und Auftragsverarbeitern die beiden Parteien auf die Modalitäten einigen, nach denen betroffene Personen ihre Rechte in vollem Umfang wahrnehmen können, und dass diese Modalitäten in den Datenschutzhinweis aufgenommen werden, der betroffenen Personen zur Verfügung zu stellen ist.

Zu Verträgen zwischen Verantwortlichem und Auftragsverarbeiter, einschließlich Standardvertragsklauseln, wird der EDSB weitere Leitlinien herausgeben.

4.3 Haftung des Auftragsverarbeiters und Ausübung der Rechte der betroffenen Person

Im Vergleich zum früheren Rechtsrahmen für den Datenschutz wird durch die Verordnung (Erwägungsgründe 45 und 50 und Artikel 29) [22] **die Verantwortung des Auftragsverarbeiters gestärkt**.

Ungeachtet seiner Verpflichtungen deutet Artikel 29 der Verordnung jedoch wohl darauf hin, dass **die Haftung des Auftragsverarbeiters im Vergleich zur Haftung des Verantwortlichen nach wie vor begrenzter ist.** Mit anderen Worten: Während Verantwortliche grundsätzlich für Schäden haftbar gemacht werden können, die sich aus einem Verstoß im Zusammenhang mit der Verarbeitung personenbezogener Daten

[22] Mit Blick auf die DSGVO siehe die Erwägungsgründe 79 und 146 und Artikel 82.

(einschließlich der vom Auftragsverarbeiter begangenen Verstöße), einem Bruch eines Vertrags oder einer anderen (verbindlichen) Vereinbarung ergeben, kann der Auftragsverarbeiter haftbar gemacht werden, wenn er außerhalb des vom Verantwortlichen erteilten Auftrags gehandelt hat oder wenn er seinen eigenen Pflichten aus der Verordnung nicht nachgekommen ist.[23] Der Auftragsverarbeiter kann für den „Teil" des Verarbeitungsvorgangs, an dem er beteiligt ist, ganz oder teilweise haftbar gemacht werden.[24] Er kann nur dann in vollem Umfang haftbar gemacht werden, wenn er für den entstandenen Schaden in vollem Umfang verantwortlich ist.

Kann **ein Auftragsverarbeiter, der spezifische Weisungen des Verantwortlichen befolgt**, für die Befolgung dieser Weisungen haftbar gemacht werden? In Artikel 29 Absätze 3 und 4 der Verordnung geht es um die Pflichten des Auftragsverarbeiters im Zusammenhang mit der mit dem Verantwortlichen zu schließenden Vereinbarung. In der Praxis würde ein Auftragsverarbeiter, der bestimmte Verarbeitungsvorgänge nach strikten Weisungen des Verantwortlichen durchführt, nicht für einen Verstoß gegen die Verordnung haftbar gemacht, wenn er sich streng an die Weisungen des Verantwortlichen hält.[25] Zeigt sich jedoch, dass der Auftragsverarbeiter über die Weisungen und das Mandat des Verantwortlichen hinaus gehandelt hat, so kann er für den Verstoß gegen die Verordnung und/oder für Schäden haftbar gemacht werden oder wenn es sich um eine Verletzung der Pflichten des Auftragsverarbeiters handelt. Ist ferner der Verantwortliche eine EU-Institution und der Auftragsverarbeiter ein externer Akteur, so fällt letzterer sowohl unter die Verordnung (insbesondere hinsichtlich der Erfüllung der Bedingungen nach Artikel 29 der Verordnung) als auch unter die DSGVO (hinsichtlich seiner internen Organisation und der Anforderungen an die Einhaltung der Verordnung).

Gemäß Artikel 29 Absatz 1 der Verordnung trägt der Verantwortliche **gegenüber der betroffenen Person** die Hauptverantwortung für den Verarbeitungsvorgang und kann für Schäden haftbar gemacht werden. Die betroffene Person kann den Auftragsverarbeiter jedoch dennoch haftbar machen, wenn sie konkrete Gründe zu der Annahme hat, dass der Verstoß, der zu einem Schaden für sie geführt hat, von dem Auftragsverarbeiter begangen wurde.

4.4 Wann ist eine EU-Institution ein Auftragsverarbeiter? Eine Checkliste

Unter Berücksichtigung der Betrachtungen in diesem Kapitel stellt sich die Frage, wann eine EU-Institution als Auftragsverarbeiter im Sinne der Verordnung gilt. Die folgende Checkliste soll EU-Institutionen dabei helfen, die relevantesten Elemente zu ermitteln, anhand derer eine Stelle als Auftragsverarbeiter identifiziert werden kann. Wenn die meisten Aussagen mit JA

[23] Die Pflichten von Auftragsverarbeitern sind in zahlreichen Artikeln der Verordnung festgelegt, nicht nur in Artikel 29.

[24] Ein Beispiel: Im Rechenzentrum des Auftragsverarbeiters kam es zu einer Verletzung des Schutzes personenbezogener Daten, weil der Auftragsverarbeiter keine geeigneten Sicherheitsmaßnahmen ergriffen hat. Der Verantwortliche hat jedoch nicht geprüft, ob und welche Sicherheitsmaßnahmen getroffen wurden und ob sie geeignet sind, die Risiken zu mindern. Für die Verletzung des Schutzes personenbezogener Daten sind beide verantwortlich, und beide haften für den entstandenen Schaden.

[25] Dies gilt unbeschadet der Haftung für gleichzeitige Verstöße des Auftragsverarbeiters gegen eine seiner eigenen Pflichten.

beantwortet werden, dürfte Ihre EU-Institution für bestimmte Verarbeitungsvorgänge Auftragsverarbeiter im Sinne der Verordnung sein.

	JA	NEIN
• Sie befolgen bei der Verarbeitung personenbezogener Daten Weisungen einer anderen Partei.		
• Sie entscheiden nicht, ob personenbezogene Daten von natürlichen Personen erhoben werden.		
• Sie entscheiden nicht über die Rechtsgrundlage für die Erhebung und Verwendung dieser Daten.		
• Sie entscheiden nicht über den Zweck oder die Zwecke, für den/die die Daten verwendet werden.		
• Sie entscheiden nicht, ob oder an wen die Daten weitergegeben werden.		
• Sie entscheiden nicht über die Speicherfrist.		
• Sie treffen bestimmte Entscheidungen darüber, wie Daten verarbeitet werden, setzen diese jedoch im Rahmen eines Vertrags oder eines anderen Rechtsinstruments oder einer verbindlichen Vereinbarung mit dem Verantwortlichen um.		
• Sie sind nicht an dem Endergebnis der Verarbeitung interessiert.		

5. Der Begriff „gemeinsam Verantwortliche“

Die Unterscheidung zwischen den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ deckt nicht alle denkbaren Beziehungen ab. Es kann vorkommen, dass sich mehr Akteure die Zuständigkeiten des Verantwortlichen teilen. Wie es schon in der Stellungnahme 1/2010 der Artikel 29-Datenschutzgruppe heißt: *Artikel 2 Buchstabe b der Richtlinie schließt die Möglichkeit, dass verschiedene Akteure an verschiedenen Vorgängen oder Vorgangsreihen im Zusammenhang mit personenbezogenen Daten beteiligt sind, nicht aus*”.[26]

Das Konzept der gemeinsam Verantwortlichkeit war bereits in der Definition des Begriffs „für die Verarbeitung Verantwortlicher“ in Artikel 2 Buchstabe d der Verordnung (EG) Nr. 45/2001 vorgesehen. Dementsprechend wurde in Artikel 2 Buchstabe d der Richtlinie 95/46/EG der Begriff „gemeinsam für die Verarbeitung Verantwortlicher“ in die weiter gefasste Definition des Begriffs „für die Verarbeitung Verantwortlicher“ aufgenommen. Ähnlich heißt es in Artikel 26 DSGVO, dass für den Fall, dass zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, sie gemeinsam Verantwortliche sind. Daher ist der **Begriff „gemeinsam Verantwortliche“ kein neues Konzept**.

In Artikel 28 Absatz 1 der Verordnung heißt es: *„Legen zwei oder mehr Verantwortliche oder ein oder mehrere Verantwortliche zusammen mit einem oder mehreren anderen Verantwortlichen, die nicht Organe oder Einrichtungen der Union sind, gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. (...)”.*

Was bedeutet dies in der Praxis?

Im folgenden Kapitel geht es um zwei allgemeine Fragen: Wann spricht man von gemeinsam Verantwortlichen, und welche Pflichten haben gemeinsam Verantwortliche? Darüber hinaus befasst es sich schwerpunktmäßig mit den Rechten betroffener Personen und der Haftung der Parteien im Fall gemeinsam Verantwortlicher. Nachstehend werden wir einige Orientierungshilfen bieten, indem wir Elemente ermitteln, die für die Beurteilung der Situation gemeinsam Verantwortlicher nützlich sein könnten.

5.1 Wann spricht man von gemeinsam Verantwortlichen, und welches sind hier die entscheidenden Elemente?

Das entscheidende Element der Definition in Artikel 28 Absatz 1 der Verordnung ist, dass Verantwortliche *„gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen“.* Im folgenden Kapitel wird auf die Konsequenzen der Definition und auf daraus entstehende mögliche Auslegungsprobleme eingegangen.

Erstens wird in Artikel 28 Absatz 1 klargestellt, dass eine solche Situation nicht nur zwischen zwei oder mehr Verantwortlichen in EU-Institutionen eintreten kann. Gemeinsam Verantwortliche kann es auch in der Beziehung zwischen einer EU-Institution und einem externen Akteur geben (z. B. einem externen Anbieter eines Verwaltungsportals oder einer einzelstaatlichen Behörde usw.). Daher darf nicht vergessen werden, dass es

[26] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, S. 22.

gemeinsam Verantwortliche auch in der Beziehung zwischen einer EU-Institution und einem oder mehreren externen Akteuren geben kann, die der DSGVO unterliegen.[27] In diesem Fall **gelten vollumfänglich die Verpflichtungen nach Artikel 28 der Verordnung**.

Eine EU-Institution kann gemeinsam Verantwortlicher sein mit einer der DSGVO unterliegenden Einrichtung. So können beispielsweise EU-Institutionen bei der Wahrnehmung ihrer Aufgaben im öffentlichen Interesse gemeinsam mit Behörden der Mitgliedstaaten Verantwortliche sein (wie auch in den Fallstudien näher erläutert).

Der EDSB ermutigt jedoch EU-Institutionen, die Dienste privater Unternehmen in Anspruch nehmen, dafür zu sorgen, dass solche privaten Unternehmen nur als Auftragsverarbeiter für solche Verarbeitungsvorgänge fungieren. Zwar können EU-Institutionen bei der Wahrnehmung der ihnen im öffentlichen Interesse vom Gesetz übertragenen Aufgaben Dienstleistungen auslagern, doch wäre es nicht angemessen, dass eine private Partei die Art des Einflusses ausübt, der dazu führen würde, dass sie gemeinsam Verantwortlicher wird.

- Ein Beispiel wäre die Inanspruchnahme eines IT-Dienstleisters durch ein Organ oder eine Einrichtung. In einem solchen Fall sollte die EU-Institution in der Tat darauf abheben, über den Zweck und die wesentlichen Elemente der Verarbeitung zu entscheiden und somit die Kontrolle über die Verarbeitung aufrechtzuerhalten, und nur die nicht wesentlichen Elemente der Verarbeitung an den Diensteanbieter delegieren.

Zweitens sollte der Begriff der gemeinsamen Bestimmung als jede Situation verstanden werden, in der jeder Verantwortliche die Möglichkeit/das Recht hat, über die Zwecke und die wesentlichen Elemente der Mittel eines Verarbeitungsvorgangs zu bestimmen. Dies bedeutet, dass jeder Verantwortliche, bevor er eine spezifische Vereinbarung mit einer oder mehreren Parteien schließt, den allgemeinen Zweck und (wesentliche Elemente) der Verarbeitungsmittel kennt. Mit anderen Worten: **Durch den Abschluss einer solchen Vereinbarung bestimmen die Parteien in der Regel (oder einigen sich auf) den Zweck und die wesentlichen Elemente der Mittel zur Durchführung eines Verarbeitungsvorgangs; das allein genügt schon, um von gemeinsam Verantwortlichen sprechen zu können.**

Drittens müssen sowohl die Zwecke als auch (die wesentlichen Elemente) der Mittel der Verarbeitung bestimmt werden. In Kapitel 2 der Leitlinien wurde der Begriff der Mittel und Zwecke erläutert.[28]

[27] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4.5.2016, S. 89.

[28] Schlussanträge von Generalanwalt Bobek in der Rechtssache *Fashion ID*, C-40/17, Rn. 105. Dies wurde vom EuGH im Urteil in der Rechtssache C-40/17 *Fashion ID GmbH & Co.KG gegen Verbraucherzentrale NRW e. V.* bestätigt.

Zusammenfassend lässt sich sagen, **dass ein „allgemeines" Maß an Komplementarität und Einheitlichkeit des Zwecks bereits zu einer Situation mit gemeinsam Verantwortlichen führen könnte, wenn die Zwecke und (wesentlichen Elemente der) Mittel des Verarbeitungsvorgangs gemeinsam festgelegt werden[29].**

In einigen Situationen entstehen regelmäßig Zweifel hinsichtlich des Vorliegens einer gemeinsamen Verantwortlichkeit.

- Es wurde argumentiert, dass ein fehlender Zugang zu personenbezogenen Daten im Rahmen eines Verarbeitungsvorgangs ausreicht, um eine gemeinsame Verantwortlichkeit auszuschließen. Der EuGH hat allerdings in der Rechtssache C-201/16 *Wirtschaftsakademie* (gestützt auf die Richtlinie 95/46/EG[30]) befunden, dass die Richtlinie „(...) *nicht verlangt, dass bei einer gemeinsamen Verantwortlichkeit mehrere Betreiber für dieselbe Verarbeitung jeder Zugang zu den betreffenden personenbezogenen Daten hat."*[31] Ferner hat der EuGH in der Rechtssache *Zeugen Jehovas* diesen Ansatz bestätigt, indem er die an der Verkündigungstätigkeit von Tür zu Tür beteiligten Mitglieder als gemeinsam Verantwortliche definiert, „(...) *ohne dass es hierfür erforderlich wäre, dass die Gemeinschaft Zugriff auf diese Daten hat* (...)".[32]

Diese Urteile unterstreichen, dass entscheidend für das Vorliegen einer gemeinsamen Verantwortlichkeit die gemeinsame Festlegung des Zwecks und der (wesentlichen Elemente der) Mittel der Verarbeitungsvorgänge ist. Der Umstand, dass eine Partei nur Zugang zu Informationen hat, die sich nicht auf eine bestimmte oder bestimmbare natürliche Person beziehen, oder zu personenbezogenen Daten, die so anonymisiert wurden, dass die betroffene Person nicht oder nicht mehr identifizierbar ist, wie es in der Rechtssache *Wirtschaftsakademie* der Fall war, wirkt sich nicht auf die Situation gemeinsamer Verantwortlichkeit aus. Dies kann jedoch bei der Bestimmung des Verantwortungsgrads der beteiligten Parteien von Bedeutung sein.

In der Praxis kann es schwierig sein, eine Situation gemeinsamer Verantwortlichkeit von einer Situation zu unterscheiden, in der zwei Verantwortliche getrennt handeln. Tatsächlich können mehrere Verantwortliche bei verschiedenen Verarbeitungsvorgängen interagieren, ohne notwendigerweise alle Zwecke und Mittel als solche zu teilen.

Fest steht aber, **dass in dem Fall, in dem die Beteiligten nicht gemeinsam dasselbe allgemeine Ziel (oder denselben allgemeinen Zweck) festlegen oder ihre Verarbeitungen nicht auf gemeinsam festgelegte (wesentliche Elemente der) Mittel stützen, ihr Verhältnis eher auf eine „getrennte Verantwortlichkeit" hindeuten dürfte.**

- So haben EU-Institutionen in der Regel CCTV-Kameras zur Aufrechterhaltung der Gebäudesicherheit installiert. Im Falle eines Vorfalls, der möglicherweise von den

[29] Rechtssache C-40/17, *Fashion ID GmbH & Co.KG gegen Verbraucherzentrale NRW e. V.*, Rn. 85.
[30] Es dürfte keinen Grund für die Annahme geben, dass dies im Rahmen der Verordnung oder der DSGVO anders entschieden worden wäre.
[31] Rechtssache C-210/16, *Wirtschaftskademie Schleswig-Holstein*, Rn. 38.
[32] Rechtssache C-25/17, *Jehovan todistajat*, Rn. 69 und 75. Dies wurde vom EuGH im Urteil in der Rechtssache C-40/17 *Fashion ID GmbH & Co.KG gegen Verbraucherzentrale NRW e. V.*, Rn. 69, bestätigt.

nationalen Strafverfolgungsbehörden untersucht werden muss, kann es erforderlich sein, die CCTV-Daten an die Ermittlungsbehörden zu übermitteln. In einem solchen Fall bestimmen die beiden Beteiligten nicht gemeinsam den Zweck und die Mittel der Verarbeitung. Folglich handelt es sich nicht um gemeinsam Verantwortliche.

BEISPIELE:

1. Zwei oder mehr Generaldirektionen haben beschlossen, eine IT-Anwendung für die Verwaltung von Forschungsprojekten zu entwickeln, die unter anderem deren Programmplanung, die Aufforderungen zur Einreichung von Vorschlägen, die Bewertung der Vorschläge, die Vergabe und Unterzeichnung von Verträgen, Zahlungen und Informationen über laufende Verträge abdeckt. Würden die beiden Generaldirektionen als gemeinsam Verantwortliche gelten?

Auf der Grundlage der Definition des Begriffs „Verantwortlicher" in Artikel 3 Absatz 8 der Verordnung können zwei oder mehr Generaldirektionen (GD), die dieselbe IT-Anwendung für die Verwaltung von Forschungsprojekten verwenden, intern als gemeinsam Verantwortliche innerhalb der EU-Institution betrachtet werden, da der Zweck und die Anwendung gemeinsam für die Verwaltung von Forschungsprojekten, die Auswahl ihrer eigenen Sachverständigen und der Finanzhilfeempfänger festgelegt und konzipiert wurden.

Wie bereits weiter oben in der Konstellation Verantwortlicher/Auftragsverarbeiter festgelegt, ist die GD, die die IT-Anwendung entwickelt und pflegt, der Auftragsverarbeiter, der die Weisungen der anderen Generaldirektionen ausführt. In der Praxis verwenden einige EU-Institutionen als Hilfe bei der Klärung der internen Zuständigkeiten die Begriffe „interner Verantwortlicher" (oder „Verantwortlicher in der Praxis") und „interner Auftragsverarbeiter" für Abteilungen oder Stellen innerhalb der EU-Institution.

Falls andere EU-Einrichtungen wie Exekutivagenturen oder andere Arten von EU-Agenturen oder gemeinsamen Unternehmen das oben genannte IT-Tool für die Verwaltung der ihnen übertragenen Forschungsprojekte nutzen, welche Rolle würden diese EU-Einrichtungen spielen? Der EDSB hat in seinen gemeinsamen Stellungnahmen zur Vorabkontrolle in Bezug auf die Verwaltung von Sachverständigen und die Verwaltung von Finanzhilfen im Teilnehmerportal bereits festgestellt, dass es sich hierbei um eine gemeinsame Verantwortlichkeit der Kommission und der Agenturen und Einrichtungen handelt, die das Teilnehmerportal nutzen.[33]

2. Zur Unterstützung eines Netzes virtueller Kontaktstellen der Mitgliedstaaten wird eine webbasierte Anwendung entwickelt, um Informationen und medizinische Studien zu seltenen und komplexen Krankheiten im Gebiet der EU auszutauschen. Das Netz wurde im Rahmen einer Richtlinie eingerichtet, und nach der gleichen Rechtsvorschrift ist Institution A verpflichtet, das Netz durch den Erlass von delegierten Rechtsakten und Durchführungsrechtsakten zu unterstützen. Diese Software ermöglicht den Informationsaustausch zwischen Gesundheitsdienstleistern in Europa und enthält die

[33] Gemeinsame Stellungnahme zur Vorabkontrolle in Bezug auf die Gewährung und Verwaltung von Finanzhilfen im Teilnehmerportal (unter H2020 ÏT-Tools) in einer Reihe von Einrichtungen der Europäischen Union - EDSB Fälle: C-2017-1080 REA, C- 2017-1076 SESAR, C-2017-1037 INEA, C- 2017-1068 CHAFEA, C-2017-0977 EASME and C-2017-1070 EIT.

medizinischen Daten von Patienten mit seltenen Krankheiten. Institution A hat die Anwendung, die von einem Unterauftragnehmer entwickelt wurde, eingerichtet und verwaltet sie. Diese Plattform wird daher in einem zentralen Speicher medizinische Daten von Patienten mit seltenen Krankheiten enthalten. Institution A entscheidet über die Kategorien der auf der Plattform verarbeiteten personenbezogenen Daten, während die nationalen Gesundheitsdienstleister die Daten außerhalb der Nutzung durch die Plattform zu dem Zweck verarbeiten, das System zu nutzen. Wäre es von Bedeutung, wenn Institution A keinen Zugang zum zentralen Speicher hätte?

Sowohl die Institution A als auch die Gesundheitsdienstleister bestimmen gemeinsam über den Zweck und die Mittel der Anwendung. Die Institution A ist vom Gesetz mit der Festlegung der technischen und nichttechnischen Maßnahmen beauftragt, die für die Verarbeitung von Patientendaten innerhalb der Plattform ergriffen werden können. Außerdem richtet sie die Plattform selbst ein und verwaltet sie. Andererseits verarbeiten die nationalen Gesundheitsdienstleister im Einklang mit dem gemeinsam festgelegten Zweck und den gemeinsam festgelegten Mitteln auch Gesundheitsdaten von Patienten auf nationaler Ebene, um das System zu nutzen und somit auch die Patienten zu informieren und ihre Rechte zu gewährleisten.

Sowohl Institution A als auch die nationalen Gesundheitsdienstleister bestimmen gemeinsam über den Zweck und die Mittel der Verarbeitungsvorgänge und handeln somit als gemeinsam Verantwortliche im Sinne von Artikel 28 der Verordnung. Ausschlaggebend ist eine „gemeinsame Festlegung" der Ziele und Mittel – auch wenn Institution A selbst keinen Zugang hätte, bliebe sie aufgrund ihrer Rolle bei der Definition des Systems weiterhin ein gemeinsam Verantwortlicher.

3. Mit einer Verordnung wird ein Informationssystem für benannte Behörden der Mitgliedstaaten eingerichtet, die Informationen einschließlich personenbezogene Daten über einen zentralen Speicher austauschen, der von einer EU-Agentur zwecks Erleichterung der grenzüberschreitenden Anerkennung von Entscheidungen in einem bestimmten Politikbereich betrieben wird. In derselben Verordnung werden bestimmte Aufgaben klar verschiedenen beteiligten Akteuren zugewiesen: So soll die EU-Agentur für die Informationssicherheit im Zentralspeicher und für die Bereitstellung einiger Analysen der Daten im System zuständig sein. Die Behörden der Mitgliedstaaten, die die Daten in das System eingeben, sind für die Richtigkeit der Daten verantwortlich. Die Agentur und die Behörden der Mitgliedstaaten entscheiden in einem Lenkungsausschuss über die Weiterentwicklung des Systems. Keine Angaben enthält die Verordnung dazu, wer die betroffenen Personen informieren würde.

Es liegt auf der Hand, dass keiner der an den Verarbeitungsvorgängen Beteiligten in der Lage wäre, den Zweck unabhängig zu erreichen. Darüber hinaus entwickeln die Parteien selbst gemeinsam die Mittel. Da Zweck und Mittel der Verarbeitungsvorgänge von den Parteien gemeinsam festgelegt werden, ist klar, dass es sich hier um gemeinsame Verantwortlichkeit handelt. Die Gründungsverordnung sieht nicht ausdrücklich vor, welche der Parteien betroffene Personen über die Verarbeitung personenbezogener Daten informiert: Dies legen die gemeinsam Verantwortlichen in ihrer Vereinbarung fest. In diesem speziellen Fall wäre es sinnvoll, wenn die nationalen Behörden die betroffenen Personen über die Verarbeitung

personenbezogener Daten in der europäischen Datenbank informierten, und zwar, sobald sie ihre Entscheidungen erlassen und sie den betroffenen Personen mitteilen.

5.2 Welche Pflichten haben gemeinsam Verantwortliche?

Eine Situation, in der gemeinsame Verantwortlichkeit besteht, bringt besondere Pflichten für die beteiligten Parteien mit sich. Artikel 28 Absatz 1 der Verordnung besagt, dass gemeinsam Verantwortliche *„(...) in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung für die Einhaltung ihrer Datenschutzpflichten hat, insbesondere was die Wahrnehmung der Rechte der betroffenen Person (...) angeht, sofern und soweit die jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die gemeinsam Verantwortlichen unterliegen, festgelegt sind (...)“.*

Während die Pflichten der gemeinsam Verantwortlichen recht umfangreich sind, sieht Erwägungsgrund 50 der Verordnung auch in der **„klaren Zuweisung der Verantwortlichkeiten“ eine *conditio sine qua non* für den *Schutz der Rechte und Freiheiten der betroffenen Personen***. Die schwerpunktmäßige Ausrichtung auf die betroffenen Personen wird auch in Artikel 28 deutlich, in dem insbesondere die Vorschriften über die Wahrnehmung der Rechte der betroffenen Personen und das Recht auf Information erwähnt werden. Der Grundrechtsansatz der Verordnung zeigt sich auch in der besonderen Möglichkeit für gemeinsam Verantwortliche, eine einzige Anlaufstelle einzurichten, um die Ausübung der Rechte der betroffenen Person zu erleichtern.

5.2.1 Die Zuständigkeiten gemeinsam Verantwortlicher

Die erste Verpflichtung besteht somit darin, die Verantwortlichkeiten für die Einhaltung der Datenschutzverpflichtungen festzulegen, ähnlich den in der Verordnung geregelten Zuständigkeiten eines Verantwortlichen.

Wenn also zwei oder mehr Parteien als gemeinsam Verantwortliche fungieren, müssen sie ihre jeweiligen Zuständigkeiten für spezifische Verpflichtungen im Rahmen der Verordnung eindeutig ermitteln und festlegen. In diesem Zusammenhang darf nicht vergessen werden, dass die **Verordnung gemeinsam Verantwortliche nicht dazu verpflichtet, ihre Verantwortlichkeiten gleichmäßig zu verteilen.** In Bezug auf die Verantwortlichen der Parteien stellt der EuGH in *Wirtschaftsakademie* klar, dass *„[...] das Bestehen einer gemeinsamen Verantwortlichkeit (...) aber nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure zur Folge hat, die von einer Verarbeitung personenbezogener Daten betroffen sind. Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist“.*[34]

[34] Rechtssache C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, Rn. 43; Rechtssache C-25/17, *Jehovan todistajat*, Rn. 66; Rechtssache C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW e. V.*, Rn. 70 und 85.

Daher **sollten die an den Verarbeitungsvorgängen beteiligten Parteien ihre Aufgaben und Zuständigkeiten unter Berücksichtigung der verschiedenen Phasen, in denen sie tätig sind, bewerten.**

Eine klare Zuweisung der Zuständigkeiten ist jedoch möglicherweise nicht immer sofort erkennbar. Daher muss eine Einzelfallprüfung durchgeführt werden, um festzustellen, welche Pflichten jedem einzelnen gemeinsam Verantwortlichen obliegen. Ein klares Verständnis davon, wer was tut, hilft bei einer sinnvollen Zuweisung von Zuständigkeiten – wenn z. B. einige der gemeinsam Verantwortlichen mit den betroffenen Personen Kontakt haben, andere hingegen nicht, ist es sinnvoll, die Verantwortung für die Unterrichtung der betroffenen Personen und die Bearbeitung von Anfragen ersterem Akteur zu übertragen.

Falls einer der gemeinsam Verantwortlichen (oder beide) beschließt/beschließen, einen Auftragsverarbeiter heranzuziehen, wie wirkt sich dies auf die gemeinsame Verantwortlichkeit und die bestehenden Zuständigkeiten aus? Kurz gesagt: gar nicht. Die Tatsache, dass einer der gemeinsam Verantwortlichen beschließt, bestimmte Verarbeitungsvorgänge von einem Auftragsverarbeiter durchführen zu lassen, berührt nicht seine eigenen Pflichten als gemeinsam Verantwortlicher. In der Praxis **möchten gemeinsam Verantwortliche möglicherweise spezifische Verfahren für den Einsatz von Auftragsverarbeitern in der Vereinbarung zwischen den gemeinsam Verantwortlichen vorsehen.** In diesen Verfahren könnte festgelegt werden, dass eine der Parteien, wenn sie beschließt, einen Auftragsverarbeiter zu beauftragen, den/die anderen Verantwortlichen zu konsultieren hat/haben, und zwar in Bezug auf den Teil der Verarbeitung, der einem Auftragsverarbeiter anvertraut werden soll, und in Bezug auf die Aspekte des Vertrags, der mit einem Auftragsverarbeiter geschlossen werden soll. Erst wenn die gemeinsam Verantwortlichen eine Einigung erzielt haben, sollte der Verantwortliche, der den Auftragsverarbeiter einschaltet, einen spezifischen Vertrag mit dem Auftragsverarbeiter schließen.

5.2.2 Die Vereinbarung zwischen gemeinsam Verantwortlichen

Gemeinsam für die Verarbeitung Verantwortliche müssen eine besondere Vereinbarung treffen, in der ihre Aufgaben und Zuständigkeiten, insbesondere gegenüber den betroffenen Personen, festgelegt sind. Dies ist eine Verpflichtung nach Artikel 28 der Verordnung, sofern und soweit diese Aufgaben und Zuständigkeiten nicht bereits in einem Gesetz festgelegt sind.

In manchen Fällen sind diese Aufgaben und Zuständigkeiten bereits (teilweise) gesetzlich geregelt, z. B. im Rechtsakt zur Errichtung eines Informationssystems. In Artikel 28 der Verordnung wird bestätigt, dass **EU-Rechtsvorschriften unmittelbar eine Zuweisung der Rollen und Zuständigkeiten zwischen den Parteien vorsehen können.** Ist dies der Fall, besteht keine Verpflichtung zum Abschluss einer Vereinbarung, sofern die jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen durch das Unionsrecht oder das Recht der Mitgliedstaaten festgelegt sind. Folglich sollte eine klare Aufteilung der Zuständigkeiten im verfügenden Teil des betreffenden Rechtsakts vorgenommen werden (oder – in Bezug auf das Unionsrecht – spätestens in einem Durchführungsrechtsakt oder delegierten Rechtsakt, wenn dies im Basisrechtsakt vorgesehen ist).

Der EDSB empfiehlt nachdrücklich, in den einschlägigen Rechtsakten eine klare Aufteilung der Zuständigkeiten vorzusehen, um eine klare Aufgabenverteilung zwischen den gemeinsam Verantwortlichen zu gewährleisten.

Wenn die Aufgaben und Zuständigkeiten von gemeinsam Verantwortlichen nur teilweise im Gesetz festgelegt sind, muss die Vereinbarung noch bestehende Lücken schließen.

Sofern nicht das Unionsrecht **bereits ihre Zuständigkeiten festlegt, müssen die gemeinsam Verantwortlichen eine besondere Vereinbarung treffen, die eine klare und transparente Aufteilung der Zuständigkeiten vorsieht.** Eine solche Vereinbarung kann in Form einer Absichtserklärung oder eines Vertrags geschlossen werden. Zusätzlich zu der Absichtserklärung kann eine Leistungsvereinbarung verwendet werden, die technische Spezifikationen enthält. Darüber hinaus kann eine Leistungsvereinbarung als ausreichende Vereinbarung zwischen gemeinsam Verantwortlichen betrachtet werden, solange sie alle Elemente im Einklang mit der Verordnung enthält.

Es ist nicht nur im Bereich des Datenschutzes, sondern auch im Hinblick auf eine gute Verwaltung[35] im Allgemeinen wichtig, sicherzustellen, dass alle Beteiligten ihre jeweiligen Aufgaben klar verstehen; es sorgt dafür, dass Anfragen bei den richtigen Leuten ankommen und hilft den EU-Institutionen, ihrer Rechenschaftspflicht nachzukommen.

Nachdem wir die verschiedenen Möglichkeiten skizziert haben, die den Abschluss einer spezifischen Vereinbarung erforderlich machen (und sofern dies nicht im Gesetz selbst geregelt ist), sei unbedingt betont, dass die Vereinbarungen

- von ALLEN gemeinsam Verantwortlichen erörtert werden sollten, die dann ihre Zustimmung geben;
- nicht einseitig von einer EU-Institution angenommen werden können;
- nur die maßgeblichen Verarbeitungsvorgänge abdecken und einen klar definierten Geltungsbereich haben sollten (insbesondere wenn es sich um einen Prozess handelt, der mit anderen Prozessen zusammenhängt, den die gemeinsam Verantwortlichen möglicherweise eingerichtet haben);
- den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung abdecken sollten;
- die Kategorien personenbezogener Daten und betroffener Personen abdecken, die an den Verarbeitungsvorgängen beteiligt sind.

[35] Siehe das Recht auf gute Verwaltung gemäß Artikel 41 der Charta sowie Der Europäische Kodex für gute Verwaltungspraxis.

Inhaltlich sollten die Vereinbarungen zumindest folgende Punkte behandeln:

- die jeweiligen Zuständigkeiten, Aufgaben und Beziehungen, so dass die Rechtmäßigkeit, Fairness und Verhältnismäßigkeit der bestehenden Verarbeitungsvorgänge festgestellt werden können;
- die jeweiligen Informationspflichten der gemeinsam Verantwortlichen nach den Artikeln 15 und 16 der Verordnung (Artikel 28 Absatz 1);
- die Zuständigkeiten für die Informationssicherheit, einschließlich der Meldung von Verletzungen des Schutzes personenbezogener Daten;
- eine Anlaufstelle für Anträge betroffener Personen;
- die Zusammenarbeit zwischen gemeinsam Verantwortlichen bei der Beantwortung von Anträgen betroffener Personen und bezüglich der Ausübung anderer Rechte betroffener Personen;
- die Zusammenarbeit zwischen gemeinsam Verantwortlichen bei der Durchführung von Datenschutz-Folgenabschätzungen[36];
- mögliche(r) Auftragsverarbeiter, der/die von einem (oder mehreren) der Verantwortlichen eingesetzt wird.

In der Praxis ist eine solche schriftliche Vereinbarung das Rechtsinstrument, mit dem die Beziehungen zwischen den verschiedenen an der gemeinsamen Verantwortlichkeit beteiligten Parteien geregelt werden. Gemäß Artikel 31 Absatz 1 Buchstabe a der Verordnung sollte im öffentlichen Teil des Verzeichnisses der Verarbeitungstätigkeiten auf die gemeinsame Verantwortlichkeit verwiesen werden. Darüber hinaus empfehlen wir, die Absichtserklärung oder jedes andere verwendete Instrument mit dem internen Teil des Verzeichnisses zu verknüpfen.

5.2.3 Unterrichtung der betroffenen Personen über das Wesentliche der Vereinbarung

In Artikel 28 Absatz 2 der Verordnung heißt es: *„Das Wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.“*

Diese Bestimmung verdeutlicht, wie wichtig es ist, die Rollen und Zuständigkeiten der gemeinsam Verantwortlichen zu bestimmen, damit in erster Linie betroffene Personen die Aufteilung der Zuständigkeiten klar nachvollziehen können und wissen, an welche Personen

[36] Bei der Durchführung einer Datenschutz-Folgenabschätzung sollten sich im Fall gemeinsamer Verantwortlichkeit die Verantwortlichen auf eine gemeinsame Methodik einigen und die Datenschutz-Folgenabschätzung gemeinsam vornehmen. In dem sehr wahrscheinlichen Fall, dass die Verantwortlichen nicht an denselben Phasen der betreffenden Verarbeitung beteiligt sein, können sich die Parteien auf eine gemeinsame Methodik einigen, führen aber dennoch eine gesonderte Datenschutz-Folgenabschätzung für die spezifische Phase des Verarbeitungsvorgangs durch, an der sie beteiligt sind.

sie sich zuerst wenden sollten. **Diese Informationen sollten betroffenen Personen im Wege des Datenschutzhinweises zur Verfügung gestellt werden.** Jeder Verantwortliche kann einen gesonderten Datenschutzhinweis haben. Gemeinsam Verantwortlichen können sich jedoch auch über einen gemeinsamen Datenschutzhinweis abstimmen, der betroffenen Personen zur Verfügung gestellt wird. Nach Artikel 15 Absatz 4 und Artikel 16 Absatz 5 Buchstabe a der Verordnung reicht es aus, betroffene Personen einmalig im Wege eines Datenschutzhinweises zu informieren. In der Vereinbarung kann auch einem der gemeinsam Verantwortlichen die Aufgabe übertragen werden, betroffene Personen zu informieren.

BEISPIEL:

Eine EU-Agentur beschließt, mit einer anderen Institution eine Veranstaltung zu einem bestimmten Thema zu organisieren. Sie entscheiden sich für eine Aufteilung ihrer Aufgaben und Zuständigkeiten, insbesondere in Bezug auf die Verarbeitung personenbezogener Daten der Teilnehmer der Veranstaltung.

Damit steht fest, dass der Gesamtzweck von den Beteiligten gemeinsam festgelegt wird. Die Tatsache, dass die Zuständigkeiten und Aufgaben je nach Durchführung der betreffenden Verarbeitungsvorgänge unterschiedlich sein können, hat keinen Einfluss auf die gemeinsame Festlegung des allgemeinen Zwecks. Darüber hinaus können auch die Mittel als gemeinsam festgelegt betrachtet werden, da sich die beiden beteiligten Parteien darauf einigen, wie diese Mittel im Zusammenhang mit der Organisation der Veranstaltung und der Verarbeitung personenbezogener Daten der Teilnehmer eingesetzt werden. Obwohl eine Partei bestimmte Einzelaufgaben wahrnehmen soll (z. B. Führen einer Mailingliste, Zugangskontrolle usw.), sind solche Schritte nur aufgrund eines gemeinsam festgelegten übergeordneten Zwecks (Veranstaltungsorganisation als solche) vorgesehen. Es liegt daher auf der Hand, dass es sich bei den Beteiligten um gemeinsam Verantwortliche im Sinne von Artikel 28 der Verordnung handelt. Darüber hinaus wird in der Vereinbarung zwischen den Parteien die Ausübung der Rechte der betroffenen Personen eindeutig geregelt, insbesondere im Hinblick auf die Kooperationspflichten zwischen ihnen bei der Bearbeitung entsprechender Anträge. Solche Kooperationspflichten können beispielsweise die Einrichtung einer Anlaufstelle umfassen, an die betroffene Personen ihre Anträge richten können.

5.3 Was bedeutet eine gemeinsame Verantwortlichkeit für die Ausübung der Rechte betroffener Personen?

Das Wesentliche der Vereinbarung muss betroffenen Personen zur Verfügung gestellt werden, damit ihnen die Aufgaben und Zuständigkeiten der gemeinsam Verantwortlichen klar sind. Die Verordnung geht, so wie die DSGVO, noch einen Schritt weiter und sieht Folgendes vor: *„Ungeachtet der Einzelheiten der Vereinbarung (...) kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen Verantwortlichen geltend machen.“*[37] Anders ausgedrückt: Die Bestimmungen der Vereinbarung dürfen betroffene Personen nicht daran hindern, ihre Rechte im Rahmen der Verordnung wahrzunehmen, die in Kapitel III ausdrücklich geregelt sind (wie das Recht auf Auskunft und das Recht auf

[37] Verordnung, Artikel 28 Absatz 3.

Berichtigung, Löschung, Datenübertragbarkeit und Widerspruch gegen die Datenverarbeitung).

Sieht jedoch eine Vereinbarung zwischen den gemeinsam Verantwortlichen spezifische Aufgaben und Zuständigkeiten vor, so kann es in der Praxis für die zwei (oder mehr) Parteien schwierig sein, den betroffenen Personen die uneingeschränkte Ausübung ihrer Rechte zu gewähren. Es ist nämlich sehr wahrscheinlich, dass die festgelegten Aufgaben und Zuständigkeiten den gemeinsam Verantwortlichen nicht die gleichen Mittel bieten, um betroffenen Personen die Ausübung ihrer Rechte im Sinne der Verordnung (wie das Recht auf Auskunft, Löschung oder Einschränkung) zu ermöglichen. In diesem Zusammenhang gilt Folgendes: **Wenn die Aufgaben und Zuständigkeiten in der Vereinbarung zwischen gemeinsam Verantwortlichen festgelegt sind, sollten dabei auch zwischen ihnen die Kooperationspflichten bezüglich des Umgangs mit solchen Anträgen betroffener Personen geregelt sein.** Solche Kooperationspflichten können beispielsweise die Angabe einer gemeinsamen E-Mail-Adresse einer Anlaufstelle umfassen, an die betroffene Personen ihre Anträge richten können. In der Praxis sollte die Vereinbarung die Modalitäten der allgemeinen Zuständigkeiten enthalten, während die Einzelheiten zu konkreten Weisungen in den zugrunde liegenden Dokumenten festgelegt werden können.

Daher muss unbedingt **sichergestellt werden, dass eine betroffene Person stets jeden gemeinsam Verantwortlichen kontaktieren kann, um Auskunft, Löschung oder Einschränkung zu beantragen**. Damit diese Rechte ausgeübt werden können, ist die Festlegung der genauen Rollen und Zuständigkeiten der gemeinsam Verantwortlichen von grundlegender Bedeutung für eine angemessene Organisation der Ausübung der Rechte.

Ungeachtet der Möglichkeit für betroffene Personen, ihre Anträge an jeden beliebigen gemeinsam Verantwortlichen zu richten, empfiehlt der EDSB, eine Anlaufstelle einzurichten, an die betroffene Personen ihre Anträge im Rahmen der Ausübung ihrer Rechte richten können.

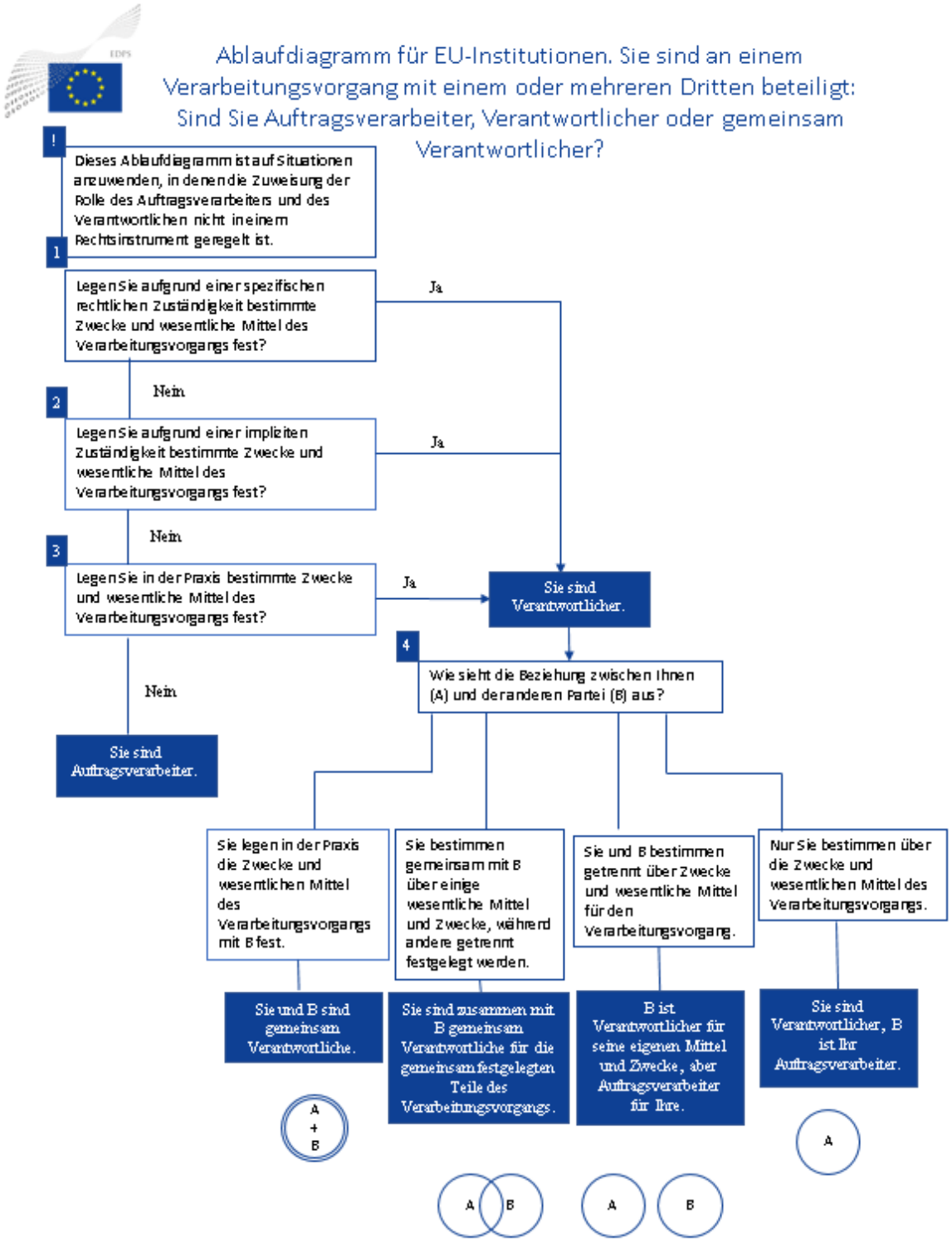
5.4 Wie steht es um die Haftung der an einer gemeinsamen Verantwortlichkeit beteiligten Parteien?

Artikel 65 der Verordnung gewährt das Recht auf Schadenersatz. Demnach hat jede Person, der wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, *„unter den in den Verträgen vorgesehenen Voraussetzungen“* Anspruch auf Schadenersatz gegen die EU-Institution auf Ersatz des erlittenen Schadens. Zu diesen Voraussetzungen sei verwiesen auf Artikel 340 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der besagt: *„Im Bereich der außervertraglichen Haftung ersetzt die Union den durch ihre Organe oder Bediensteten in Ausübung ihrer Amtstätigkeit verursachten Schaden nach den allgemeinen Rechtsgrundsätzen, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind.“*[38]

[38] AEUV, Artikel 340 Absatz 2.

Anders als die Artikel 26 und 82 DSGVO **befasst sich die Verordnung nicht speziell mit der Haftung bei Verstößen**. Artikel 340 AEUV spricht von den „allgemeinen Rechtsgrundsätzen, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind“. Wie bereits in dem Kapitel über Verantwortlichkeit erwähnt, ist nach Artikel 268 AEUV der Gerichtshof der Europäischen Union für Streitsachen über den in Artikel 340 AEUV vorgesehenen Schadenersatz zuständig. Daher unterscheiden sich die Grundsätze für die Haftung der Parteien bei einer gemeinsamen Verantwortlichkeit von der Regelung in der DSGVO.

6. Anhang 1



Hinweis: Mit diesem Ablaufdiagramm soll verdeutlicht werden, wer eigentlich als Verantwortlicher oder Auftragsverarbeiter bezeichnet werden kann; es soll nicht dargestellt werden, was passiert, wenn ein Auftragsverarbeiter seinen Auftrag/seine Rolle zu großzügig auslegt, indem er sich an der Bestimmung wesentlicher Mittel der Verarbeitung beteiligt.

7. Anhang 2

Checkliste 1: Welche Pflichten hat ein Verantwortlicher?

Bei der Verarbeitung personenbezogener Daten sind folgende Grundsätze zu wahren:

- Die Verarbeitung sollte rechtmäßig, nach Treu und Glauben und transparent ablaufen („**Rechtmäßigkeit**“, „**Verarbeitung nach Treu und Glauben**“, „**Transparenz**“);
- die Verarbeitung sollte an bestimmte Zwecke gebunden sein („**Zweckbindung**“);
- die verarbeiteten personenbezogenen Daten sollten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“);
- die personenbezogenen Daten sollten sachlich richtig sein („**Richtigkeit**“);
- die personenbezogenen Daten sollten nicht länger als erforderlich gespeichert werden („**Speicherbegrenzung**“);
- die personenbezogenen Daten müssen sorgfältig gesichert und vertraulich bleiben („**Integrität und Vertraulichkeit**“).

Siehe die Leitlinien des EDSB „Rechenschaftspflicht vor Ort“, Teil I S. 20-22, sowie Teil II, S. 11-15, für weiterführende Fragen zu diesen Grundsätzen des Datenschutzes.

Der Verantwortliche ist für die Einhaltung dieser Grundsätze verantwortlich und sollte diese Einhaltung nachweisen können („Grundsatz der Rechenschaftspflicht“). Hierzu müssen Verantwortliche in der Praxis insbesondere

- ihre Verarbeitungsvorgänge mit **Aufzeichnungen** dokumentieren;
  (Hinweis: Der EDSB empfiehlt nachdrücklich, diese Aufzeichnungen in einem **zentralen und öffentlich zugänglichen Verzeichnis** zu führen);
- vor Vorgängen, die ein hohes Risiko für die Rechte und Freiheiten betroffener Personen bergen, eine **Datenschutz-Folgenabschätzung** durchführen;
- unter bestimmten Umständen vor solchen mit hohem Risiko behafteten Verarbeitungsvorgängen **den EDSB konsultieren**;
- bei der Gestaltung von Verarbeitungsvorgängen die Grundsätze des **„Datenschutzes durch Technik“** und des **„Datenschutzes durch datenschutzfreundliche Voreinstellungen“** beachten;
- **angemessene Sicherheitsmaßnahmen** zum Schutz personenbezogener Daten ergreifen;
- im Fall einer **Verletzung des Schutzes personenbezogener Daten** den EDSB sowie unter bestimmten Umständen die betroffenen Personen benachrichtigen;
- **Vereinbarungen / Verträge mit Auftragsverarbeitern** abschließen (nur mit solchen, die hinreichend Garantien bieten);
- mit anderen Auftragsverarbeitern im Fall **gemeinsamer Verantwortlichkeiten** Vereinbarungen abschließen;
- personenbezogene Daten innerhalb der EU-Institution, an andere EU-Institutionen, in Drittländer oder internationale Organisationen **übermitteln** nur, wenn die Bedingungen der Verordnung erfüllt sind;
- **mit dem EDSB zusammenarbeiten**.

Siehe die Leitlinien des EDSB „Rechenschaftspflicht vor Ort“ zu Aufzeichnungen, Datenschutz-Folgenabschätzungen, vorheriger Konsultation und anderen Themen.

Schließlich muss der Verantwortliche betroffenen Personen **klare und zugängliche Informationen** über die Verarbeitung zur Verfügung stellen, **die Rechte der betroffenen Personen achten** und ihre Verfügbarkeit in der Praxis sicherstellen.

Siehe die Leitlinien des EDSB zu Transparenz und anderen Rechten und Pflichten.

8. Anhang 3

Checkliste 2: Welche Pflichten hat ein Auftragsverarbeiter?

Um der Verordnung Genüge zu tun, müssen Auftragsverarbeiter insbesondere

- personenbezogene Daten nur auf **dokumentierte Weisungen des Verantwortlichen** verarbeiten, soweit sie nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten dazu verpflichtet sind;

- personenbezogene Daten **gemäß einem Vertrag oder Rechtsinstrument** verarbeiten, der/das für den Auftragsverarbeiter verbindlich ist und in dem die notwendigen Voraussetzungen für die Verarbeitung festgelegt sind;

- **KEINE Weiterverarbeitung** der Daten zu mit dem ursprünglichen Zweck der Verarbeitung nicht zu vereinbarenden Zweck vornehmen;

- **dem Verantwortlichen behilflich sein** bei der Erfüllung der Pflicht, die **Rechte betroffener Personen zu wahren** und die **Pflichten des Verantwortlichen nach den Artikeln 33-41** der Verordnung wahrzunehmen (Sicherheit und Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzung und vorherige Konsultation, Vertraulichkeit der elektronischen Kommunikation, Information und Konsultation des EDSB);

- alle rechtsverbindlichen **Anträge auf Offenlegung** der im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten **melden** und nur mit vorheriger schriftlicher Genehmigung des Verantwortlichen Zugang zu den Daten gewähren;

- **Aufträge auslagern/Unteraufträge vergeben NUR mit vorheriger schriftlicher Genehmigung** des Verantwortlichen; den Verantwortlichen über alle Änderungen unterrichten, dem Verantwortlichen Gelegenheit zum Einspruch geben; an etwaige Unterauftragnehmer dieselben vertraglichen Pflichten weitergeben;

- **ein Verzeichnis führen** aller Kategorien von im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten;

- **angemessene Sicherheitsmaßnahmen** zum Schutz der personenbezogenen Daten ergreifen;

- den Verantwortlichen unverzüglich über eine **Verletzung des Schutzes personenbezogener Daten** unterrichten;

- auf Anfrage mit dem EDSB bei der Wahrnehmung seiner Aufgaben **zusammenarbeiten**.

Brüssel, den 7. November 2019

Wojciech Wiewiorowski

Stellvertretender Datenschutzbeauftragter