PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Leitlinien zu ethischen und rechtlichen Fragen des Datenschutzes in der IKT-Forschung und -Innovation.

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) – HAUPTAKTEURE

Dieses Projekt wurde aus Mitteln des Forschungs- und Innovationsprogramms Horizont 2020 der Europäischen Union unter der Finanzhilfevereinbarung Nr. 788039 finanziert. Die Verantwortung für den Inhalt dieses Dokuments tragen allein die Verfasser; die Agentur haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

3 Hauptakteure

Frédéric Tronnier (GUF)

In diesem Abschnitt sollen die Hauptakteure erläutert werden, d. h. die Rollen, die Einzelpersonen, Organisationen oder anderen Einrichtungen in der Datenschutz-Grundverordnung zugewiesen werden können. In Art. 4 Absatzt 7 bis 10 werden einige dieser Akteure definiert, während andere später in der Datenschutz-Grundverordnung definiert werden[182]. Im Folgenden werden diese Akteure definiert, um die verschiedenen Aufgaben, Rechte und Verantwortlichkeiten zu verdeutlichen, die jeder Akteur besitzt. Für die Arbeit mit personenbezogenen Daten und die Einhaltung der Datenschutz-Grundverordnung ist es notwendig, die Rolle zu verstehen, die man bei der Arbeit mit personenbezogenen Daten einnimmt. Tabelle 1 gibt einen kurzen Überblick über die Hauptakteure. Im Hauptteil dieses Dokuments werden praktische Beispiele angeführt, um das Zusammenspiel zwischen den verschiedenen Kategorien von Akteuren zu veranschaulichen.

182 Für detailliertere Informationen zu den Hauptakteuren: Verantwortlicher, Auftragsverarbeiter und gemeinsam Verantwortliche, verweisen wir auf die Leitlinien des EDSB zu diesen Akteuren. Leitlinien des EDSB zu den Begriffen „Verantwortlicher“, „Auftragsverarbeiter“ und „gemeinsam Verantwortliche“ nach der Verordnung (EU) 2018/1725. Verfügbar unter: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_Verantwortlichen_processor_and_jc_reg_2018_1725_en.pdf (Zuletzt besucht: 03.12.2020)
Und die Leitlinien 07/2020 zu den Begriffen des Verantwortlichen und des Auftragsverarbeiters in der Datenschutz-Grundverordnung. Verfügbar unter: https://edpb.europa.eu/sites/edpb/files/consultation/EDSA_guidelines_202007_controllerprocessor_en.pdf (Zuletzt besucht: 03.12.2020)

Akteur	**Betroffene Person**	**Verantwortlicher**	**Auftragsverarbeiter**	**Gemeinsame Verantwortliche**	**Empfänger**	**Dritter**	**Datenschutzbeauftragter**	**Aufsichtsbehörde**
DSGVO	**Art. 4 Abs. 1**	**Art.4 Abs. 7**	**Art.4 Abs. 8**	**Art. 26**	**Art. 4 Abs. 9**	**Art.4 Abs. 10**	**Art. 37**	**Art. 51**
Kurzbeschreibung	Eine natürliche Person, die direkt oder indirekt durch personenbezogene Daten identifiziert werden kann.	Jede Stelle, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.	Verarbeitet die personenbezogenen Daten im Auftrag des Verantwortlichen. Bestimmt nicht die Zwecke dieser Verarbeitung.	Zwei oder mehr Verantwortliche, die gemeinsam die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegen.	Jede Stelle, an die personenbezogene Daten weitergegeben werden, mit Ausnahme von Behörden, die personenbezogene Daten in Übereinstimmung mit dem Gesetz erhalten.	Jede andere Stelle als der Verantwortliche, der Auftragsverarbeiter, die betroffene Person oder die zur Verarbeitung personenbezogener Daten befugten Personen.	Natürliche Person, die innerhalb einer Organisation unabhängig handelt, um die korrekte Anwendung der DSGVO sicherzustellen	Unabhängige öffentliche Behörde, die von den EU-Mitgliedstaaten eingerichtet wurde. Auch Datenschutzbehörden genannt.
Aufgaben	In der DSGVO sind keine Aufgaben festgelegt. Betroffene Personen können ihre	Hat die Kontrolle über die Daten und entscheidet, was mit ihnen gemacht wird. Will in der	Verarbeitet die Daten nach den Anweisungen des Verantwortlichen.	Die Aufgaben sind die gleichen wie die eines (einzelnen) Verantwortlichen, werden aber von allen gemeinsamen Verantwortlichen	Hat keine aktive Rolle. Ein Empfänger wird nur durch seinen Zugang zu personenbezogenen Daten	Hat keine aktive Rolle.	Stellt sicher, dass die Rechte der betroffenen Personen geschützt werden Bearbeitet und bearbeitet	Verantwortlich für die Überwachung und Durchsetzung der ordnungsgemäßen Anwendung der Datenschutzgrundverordnung.

	Rechte gemäß Art. 12–23 DSGVO geltend machen.	Regel ein Ziel mit den Daten erreichen.		gemeinsam ausgeführt.	definiert.		Beschwerden.	Fördert das Bewusstsein für Fragen der Datenverarbeitung. Bearbeitet Beschwerden von betroffenen Personen.
Rechte/Pflichten	Ausgestattet mit vielen Rechten wie dem Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und Auskunftsrecht.	Muss die Einhaltung der DSGVO bei der Verarbeitung der Daten sicherstellen und nachweisen können, dass die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO	Handelt auf Anweisung des Verantwortlichen mit einem gewissen Grad an Freiheit bei der Wahl der am besten geeigneten Methoden für die Verarbeitung. Garantiert, dass die Verarbeitung	Die gemeinsam Verantwortlichen müssen ihre jeweiligen Verantwortlichkeiten für die Einhaltung der Datenverarbeitungsvorschriften festlegen Es muss eine Kontaktstelle für die betroffenen Personen eingerichtet werden.	Keine Rechte und Pflichten. Wird zum Verantwortlichen für jede Verarbeitung, die für seine eigenen Zwecke durchgeführt wird.	Erhält personenbezogene Daten. Wird zum Verantwortlichen für jede Verarbeitung, die für seine eigenen Zwecke durchgeführt wird.	Handelt unabhängig mit eigenem Budget und eigenen Ressourcen Sollte sich nicht in einem Interessenkonflikt befinden, also kein Auftragsverarbeiter oder Verantwortlicher sein.	Durchsetzung der Anwendung der Datenschutz-Grundverordnung. Er kann Verwarnungen und Verweise aussprechen oder die Verarbeitung personenbezogener Daten durch andere Stellen verbieten oder einschränken.

		erfolgt. Muss hierfür geeignete technische und organisatorische Maßnahmen umsetzen.	den Anforderungen der Datenschutz-Grundverordnung entspricht.					

Tabelle 1. Kurze Zusammenfassung der Hauptakteure der DSGVO

3.1 Betroffene Person

3.1.1 Wer ist dieser Akteur?

Die betroffene Person wird in Artikel 4 Absatz 1 DSGVO indirekt eingeführt als „eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“); als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“ Eine betroffene Person ist also eine lebende Person, die durch personenbezogene Daten identifiziert wird. Verstorbene Personen und juristische Personen werden nicht als betroffene Personen definiert.

Die Datenschutz-Grundverordnung zielt darauf ab, die betroffenen Personen zu schützen, indem sie ihnen die Kontrolle über sie betreffende personenbezogene Daten zurückgibt, indem sie ihnen Rechte einräumt, die sie dann ausüben können.

3.1.2 Was sind deren Rechte und Pflichten?

Die betroffenen Personen haben gemäß Artikel 14–23 DSGVO eine Vielzahl von Rechten. Betroffene Personen haben beispielsweise das Recht auf Auskunft, was bedeutet, dass sie von dem Verantwortlichen verlangen können, zu erfahren, ob personenbezogene Daten verarbeitet werden, welche Kategorien personenbezogener Daten verwendet werden, wofür die personenbezogenen Daten verarbeitet werden und wer die Empfänger der personenbezogenen Daten sind. Betroffene Personen haben darüber hinaus das Recht auf Löschung und Berichtigung, d. h. sie können verlangen, dass sie betreffende personenbezogene Daten berichtigt oder gelöscht werden. Betroffene Personen haben auch das Recht auf Datenübertragbarkeit, d. h. sie können die personenbezogenen Daten von dem Verantwortlichen in einem strukturierten Format erhalten und es steht ihnen dann frei, die Daten einem anderen Verantwortlichen zu übermitteln. Gemäß Artikel 12 und 13 DSGVO müssen die Verantwortlichen betroffenen Personen sie betreffende personenbezogene Daten zur Verfügung stellen, wenn die betroffenen Personen dies verlangen. Die personenbezogenen Daten können in schriftlicher oder elektronischer Form zur Verfügung gestellt werden, aber auch mündlich, wenn die Identität der betroffenen Person auf andere Weise bestätigt werden kann. Der Verantwortliche kann sich weigern, einer solchen Anfrage nachzukommen, oder eine angemessene Gebühr erheben, wenn sich die Anfrage nach personenbezogenen Daten als unbegründet oder überzogen erweist.

Wenn betroffene Personen der Ansicht sind, dass ihre Rechte durch einen Verantwortlichen oder einen Auftragsverarbeiter oder infolge der Verarbeitung personenbezogener Daten verletzt wurden, können sie eine Beschwerde bei einer Aufsichtsbehörde einreichen (Artikel 77 DSGVO). Sie haben in einer solchen Situation auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf (Art. 77 DSGVO). Wenn betroffenen Personen durch die Verletzung ihrer Rechte aus der DSGVO ein (nicht) materieller Schaden entstanden ist, können sie von dem Verantwortlichen oder dem Auftragsverarbeiter Ersatz für den erlittenen Schaden verlangen. Betroffene Personen können gemäß Artikel 80 DSGVO auch gemeinnützige Organisationen oder Einrichtungen beauftragen, diese Maßnahmen in ihrem Namen zu ergreifen.

Beispiel 1:

Die Person I ist Nutzer eines sozialen Netzwerks des Anbieters S. S erhebt personenbezogene Daten wie Wohnadresse, Name, Alter und Geschlecht von I, um I den gewünschten Dienst zur Verfügung zu stellen. Da I sich nicht sicher ist, welche Daten S genau erhoben hat, beantragr I unter Berufung auf das Auskunftsrecht nach Artikel 15 DSGVO Auskunft über die Daten. Da einige der Daten sachlich falsch sind, beantragt I die Berichtigung dieser unrichtigen personenbezogenen Daten gemäß Artikel 16 DSGVO.

3.2 Verantwortliche

3.2.1 Wer ist dieser Akteur?

Der Verantwortliche kann jede *„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 (...)".*[183] Daraus geht hervor, dass jede Stelle, die aus verschiedenen Gründen über personenbezogene Daten verfügt, als Verantwortlicher gilt, sei es, um beispielsweise wissenschaftliche Forschung auf der Grundlage personenbezogener Daten durchzuführen oder für Marketing- oder Geschäftszwecke. Der Verantwortliche hat Einfluss auf die Verarbeitung personenbezogener Daten, indem er die Verarbeitung durchführt oder die Möglichkeit hat, über die Verarbeitung zu entscheiden. Um festzustellen, ob eine Einrichtung ein Verantwortlicher ist, können die folgenden Fragen gestellt werden:

- Wer trifft die Entscheidungen über die Datenverarbeitung?
- Wer ist befugt, die Datenverarbeitung zu stoppen?
- Warum findet die Verarbeitung statt?
- Wer hat die Verarbeitung veranlasst?
- Wer profitiert von der Verarbeitung?[184]

Die Definition schließt auch die Möglichkeit ein, dass der Verantwortliche nicht allein handelt, sondern dass es mehrere Verantwortliche gibt, die gemeinsam die Verarbeitung personenbezogener Daten kontrollieren. Der Abschnitt „Gemeinsame Verantwortliche“ erläutert dies ausführlicher.

3.2.2 Was sind seine Aufgaben?

Der Verantwortliche bestimmt die Mittel und Zwecke der Datenverarbeitung. Das bedeutet, dass der Verantwortliche die Kontrolle über die Verarbeitung personenbezogener Daten hat und der Akteur ist, der tatsächlich entscheidet, was mit den personenbezogenen Daten geschieht. In der Regel will der Verantwortliche ein Ziel erreichen, z. B. ein Forschungsprojekt und -ziel oder einen Geschäftsprozess*, für den die Verarbeitung von Daten erforderlich ist.

3.2.3 Was sind seine Rechte und Pflichten?

Der Verantwortliche muss sicherstellen, dass Datenschutzvorschriften wie die DSGVO eingehalten werden. Mit anderen Worten ist der Verantwortliche dafür verantwortlich, was mit den personenbezogenen Daten geschieht, wie sie verarbeitet werden und ob die Verarbeitung im Einklang mit der DSGVO steht oder nicht. In der Praxis bedeutet dies, dass die Verantwortlichen Maßnahmen und Garantien einführen müssen, die darauf abzielen, die

183 Art. 4 Absatz 7 DSGVO

184 Siehe EDSB. eitlinien zu den Begriffen „Verantwortlicher“, „Auftragsverarbeiter“ und „gemeinsam Verantwortliche“ gemäß der Verordnung (EU) 2018/1725, S. 7, basierend auf der Rechtssache C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388, Rn. 40 und Schlussanträge des Generalanwalts Bot in der Rechtssache C-210/16, Wirtschaftsakademie, Rn. 64 und 65.

Anwendung der Datenschutz-Grundverordnung einzuhalten und solche Richtlinien nachzuweisen. In der Tat definiert Artikel 24 DSGVO die Verantwortung des Verantwortlichen in Bezug auf die Umsetzung:

> *„geeigneter technischer und organisatorischer Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert."*[185]

Diese technischen und organisatorischen Maßnahmen werden im Abschnitt „Grundsätze" (3.1.3) dieses Dokuments näher erläutert. Der Verantwortliche muss nachweisen können, dass die Grundsätze der Datenverarbeitung wie Datenminimierung, Speicherbegrenzung und Transparenz umgesetzt und gewährleistet werden. Dies wird in Art. 5 Absatz 2 DSGVO als Rechenschaftspflicht des Verantwortlichen bezeichnet. Es ist daher wichtig, dass der Verantwortliche in der Lage ist, die Einhaltung dieser Grundsätze nachzuweisen und zu dokumentieren (Art. 30 Absatz 2 DSGVO). [186][187] Bei der Durchführung und Umsetzung von Forschungsprojekten sollten die Grundsätze des „Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" (Art. 25 DSGVO) beachtet werden. Rechenschaftspflicht bedeutet dabei nicht nur, dass „… der Projektvorschlag eine vorgegebene Checkliste von Bedingungen erfüllen muss, sondern dass die Forschungsmethodik selbst ethisch-rechtskonform gestaltet sein muss"[188]. Praktische Beispiele sind die Einbeziehung eines interdisziplinären Teams, ein als DSB bestellter Rechts- und Ethiksachverständiger, eine IT-Infrastruktur, die der CIA-Trias entspricht, und die Aufzeichnung und Regelung des Datenflusses innerhalb des Forschungsteams und zwischen ihm und anderen Stellen.[189]

Der Verantwortliche kann andere Stellen beauftragen und ernennen, die die Verarbeitung in seinem Namen durchführen, die sogenannten Auftragsverarbeiter. Der Verantwortliche ist verpflichtet, nur Auftragsverarbeiter zu beauftragen, die hinreichende Garantien dafür bieten können, dass sie geeignete technische und organisatorische Maßnahmen für eine DSGVO-konforme Verarbeitung der Daten ergriffen haben. Diese Maßnahmen müssen ergriffen und nachgewiesen werden, um die Verarbeitung zu sichern und die Rechte der betroffenen Personen zu schützen.[190] Natürlich sind Forscher, die als Verantwortliche fungieren, daher verpflichtet, nur vertrauenswürdige Auftragsverarbeiter einzusetzen, die nachweisen können, dass sie die Verordnung einhalten.

Wenn die Rechte der betroffenen Person verletzt wurden, d. h. wenn personenbezogene Daten unrechtmäßig verarbeitet wurden und dadurch ein materieller oder immaterieller Schaden entstanden ist, können die betroffenen Personen ihre Rechte gemäß Artikel 16 bis 23 DSGVO geltend machen (siehe Abschnitt über die Rechte der betroffenen Person). Zu diesem Zweck ist der Verantwortliche die „letzte Anlaufstelle"[191], an die sich die betroffenen Personen

---

185 Siehe Art. 24 Absatz 1 DSGVO

186 EDSB, Vorläufige Stellungnahme zum Datenschutz und zur wissenschaftlichen Forschung, 6. Januar 2020, S.17.

187 EDSB, Leitlinien 07/2020 zu den Begriffen des Verantwortlichen und des Auftragsverarbeiters in der Datenschutz-Grundverordnung, 2. September 2020, S. 8.

188 D. Amram, Aufbau des *Modells* "*Accountable Ulysses*". The impact pf DSGVO and national implementations, ethics, and health-data research: Comparative remarks*, Computer Law and Security Review*, Juli 2020, Vol. 37, S. 2.

189 Ebd., S. 6. Der Autor dieses Artikels nennt weitere Merkmale, die zu berücksichtigen sind, um ein „akzeptables Maß an Übereinstimmung" zu erreichen.

190 EDSB, Leitlinien 07/2020 zu den Begriffen des Verantwortlichen und des Auftragsverarbeiters in der Datenschutz-Grundverordnung, September 2020, S.4.

wenden können, um ihre Rechte auszuüben. Art. 82 Absatz 1 DSGVO besagt, dass die betroffenen Personen unter solchen Umständen das Recht haben, von dem Verantwortlichen (oder dem Auftragsverarbeiter) Schadenersatz zu erhalten. Darüber hinaus sind die Verantwortlichen für Schäden haftbar, wenn sie gegen die DSGVO verstoßen (Artikel 82 Absatz 2). In Erwägungsgrund 146 heißt es, dass die betroffenen Personen einen wirksamen und vollständigen Ersatz des ihnen entstandenen Schadens erhalten müssen und dass „der Begriff des Schadens im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und

Checkliste: Wenn Sie eine der folgenden Aussagen mit „Ja“ beantworten, sind Sie wahrscheinlich ein Verantwortlicher

- Sie erheben oder verwenden personenbezogene Daten für Ihre eigenen persönlichen oder Forschungszwecke.
- Auch wenn eine andere Stelle personenbezogene Daten verarbeitet, bestimmen Sie, warum diese Daten verarbeitet werden sollen.
- Sie haben entschieden, welche Kategorien personenbezogener Daten genau erfasst werden sollen und von wem.
- Die personenbezogenen Daten, die Sie zu verarbeiten beabsichtigen, betreffen Ihre Mitarbeiter.
- Sie haben eine andere Stelle, z. B. ein anderes Unternehmen oder eine Forschungseinrichtung, damit beauftragt, personenbezogene Daten für Sie zu verarbeiten oder zu analysieren.

Weise ausgelegt werden sollte, die den Zielen dieser Verordnung in vollem Umfang entspricht.“

3.3 Gemeinsam Verantwortlichen

3.3.1 Wer ist dieser Akteur?

Gemeinsam Verantwortliche sind zwei oder mehr Verantwortliche, die gemeinsam die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegen. Für solche gemeinsam Verantwortliche werden in der Datenschutz-Grundverordnung spezifische Regeln eingeführt, um die Beziehung zwischen den gemeinsam Verantwortlichen zu regeln.

3.3.2 Was sind deren Aufgaben?

Die Aufgaben sind die gleichen wie die eines (einzelnen) Verantwortlichen, werden aber von allen gemeinsamen Verantwortlichen gemeinsam ausgeführt.

3.3.3 Wann liegt eine gemeinsame Verantwortlichkeit vor?

Eine gemeinsame Verantwortlichkeit liegt vor, wenn eine bestimmte Datenverarbeitung stattfindet, bei der mehrere Verantwortliche gemeinsam die Mittel und den Zweck der Verarbeitung bestimmen. Dies bedeutet, dass mehrere Verantwortliche gemeinsam über die Verarbeitung entscheiden. Hier unterscheidet der EDSA zwischen **gemeinsamen Entscheidungen** und **konvergierenden Entscheidungen**.

- **Gemeinsame Entscheidung**: Die Verantwortlichen entscheiden gemeinsam und in gemeinsamer Absicht über die Mittel und Zwecke der Verarbeitung.
- **Konvergierende Entscheidung**: „*Entscheidungen können als konvergierend in Bezug auf die Zwecke und Mittel angesehen werden, wenn sie einander ergänzen und für die Verarbeitung in einer Weise erforderlich sind, dass sie sich spürbar auf die Festlegung der Zwecke und Mittel der Verarbeitung auswirken.*“[192] Das bedeutet, dass die Verarbeitung durch jeden Verantwortlichen mit der Verarbeitung durch den anderen Verantwortlichen verknüpft ist und ohne diese nicht möglich wäre.

Eine gemeinsame Verantwortlichkeit kann auch entstehen, wenn eine Stelle keinen Zugang zu personenbezogenen Daten hat. Was die Mittel der Verarbeitung anbelangt, so muss nicht jeder für die Verarbeitung gemeinsam Verantwortlichen *immer alle* Mittel festlegen. Verschiedene Verantwortliche können in verschiedenen Phasen der Verarbeitung personenbezogener Daten unterschiedliche Mittel verwenden. Das Gleiche gilt für die Zwecke der Daten. Eine gemeinsame Verantwortlichkeit liegt vor, wenn die personenbezogenen Daten für alle Verantwortlichen zu demselben Zweck verarbeitet werden, aber auch, wenn die Zwecke der verschiedenen Verantwortlichen eng miteinander verbunden sind oder sich ergänzen. Das heißt, wenn die Verarbeitung allen Verantwortlichen zugutekommt und alle Verantwortlichen sich auf die Zwecke und Mittel geeinigt haben, liegt eine gemeinsame Verantwortlichkeit vor.

Der Begriff der gemeinsamen Verantwortlichkeit bedarf jedoch einer sorgfältigen Prüfung und muss von Fall zu Fall entschieden werden. Ein klarer Überblick über die Beziehungen zwischen allen beteiligten Parteien sowie über den Datenfluss ist elementar, um festzustellen, ob eine gemeinsame Verantwortlichkeit vorliegt oder nicht. Der EDSA liefert in seinen Leitlinien zu diesem Thema mehrere Beispiele.[193]

3.3.4 Was sind deren Rechte und Pflichten?

Die Rechte und Pflichten der gemeinsam Verantwortlichen sind in Art. 26 Absatz 1–2 DSGVO festgelegt. Die gemeinsam Verantwortlichen:

> *„legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.“*

192 EDSA. Leitlinien 07/2020 zu den Begriffen des Verantwortlichen und des Auftragsverarbeiters in der Datenschutz-Grundverordnung. Version 1. Verabschiedet am 02. September 2020. Verfügbar unter: https://edpb.europa.eu/sites/edpb/files/consultation/EDSA_guidelines_202007_controllerprocessor_en.pdf S. 18. Letzter Zugriff am 30.10.2020.

193 Ebd. S.18ff für mehrere Beispiele für und gegen eine gemeinsame Verantwortlichkeit.

Zu diesem Zweck sollten Standardverträge zwischen den gemeinsam Verantwortlichen verwendet werden, um eindeutig festzulegen, welcher Verantwortliche genau welche Verantwortlichkeiten und Aufgaben zu erfüllen hat. Dazu gehört auch die Festlegung der Zwecke der Verarbeitung sowie der Mittel für die Verarbeitung.[194] Die betroffenen Personen sollten die Kontaktinformationen eines der Verantwortlichen erhalten, damit sie leichter feststellen können, an wen sie sich bei Fragen zur Datenverarbeitung wenden können. Außerdem sollten den betroffenen Personen die Aufteilung der Zuständigkeiten und die wesentlichen Ergebnisse der Vereinbarung (des Vertrags) zwischen den gemeinsam Verantwortlichen zur Verfügung gestellt werden. So sollte beispielsweise ein Datenschutzhinweis für die betroffene Person die gemeinsam Verantwortlichen sowie deren Aufgaben und Zuständigkeiten bei der Datenverarbeitung aufführen.

Diese klare Zuweisung von Verantwortung und Haftung wird in Erwägungsgrund 79 der Datenschutz-Grundverordnung als notwendige Voraussetzung für gemeinsam Verantwortliche genannt. Allerdings fügt Art. 26 Absatz 3 jedoch hinzu, dass die betroffenen Personen ihre Fragen und Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend machen können.[195]

Beispiel 1:

Die Universitäten A, B und C beschließen, ein gemeinsames Forschungsprojekt durchzuführen. Für dieses Projekt speist jede Universität personenbezogene Daten in eine Datenbank ein, die von einer der Universitäten für das gemeinsame Forschungsprojekt bereitgestellt wurde. A, B und C verarbeiten dann die personenbezogenen Daten in dieser Datenbank für ihr gemeinsames Forschungsprojekt, da sie zuvor über die Zwecke und Mittel der Verarbeitung entschieden haben. Das bedeutet, dass in diesem Forschungsprojekt Daten gesammelt werden, um ein vorher festgelegtes Ziel zu erreichen. Die Daten werden dann mit einer bestimmten, vorher festgelegten Softwarelösung analysiert. In diesem Szenario sind A, B und C gemeinsam Verantwortliche, da sie die Mittel und Zwecke der Verarbeitung gemeinsam festgelegt haben. Daher sollten alle Universitäten durch vertragliche Vereinbarungen die Rechte und Verantwortlichkeiten jeder Partei in Bezug auf die Datenverarbeitung auf transparente Weise festlegen.[196] Darüber hinaus sollten die betroffenen Personen immer sicher sein, an welche Partei sie sich wenden können und sollten, wenn sie Fragen haben oder ihre in der DSGVO festgelegten Rechte ausüben möchten.

Verarbeitet eine Universität A personenbezogene Daten in der Datenbank zu einem anderen Zweck als dem des gemeinsamen Forschungsprojekts, so wird diese Universität A für diesen besonderen Zweck zu einem gesonderten Verantwortlichen.

Beispiel 2:

Unternehmen A ist die Muttergesellschaft einer Gruppe von Unternehmen B, C und D. Zur Speicherung von Forschungsdaten verwenden die Tochtergesellschaften eine Datenbank, die von der Muttergesellschaft A gehostet und bereitgestellt wird.
Jedes Unternehmen B, C und D kann nur auf die personenbezogenen Daten zugreifen, die es

194 Ibid. p.3

195 Weitere Informationen zur gemeinsamen Verantwortlichkeit finden Sie in den Leitlinien des EDSB: Leitlinien des EDSB zu den Begriffen „Verantwortlicher“, „Auftragsverarbeiter“ und „gemeinsam Verantwortliche“ nach der Verordnung (EU) 2018/1725, S.22f f

196 Für weitere Informationen über die gemeinsam Verantwortliche siehe: EDSB, Leitlinien des EDSB zu den Begriffen „Verantwortlicher“, „Auftragsverarbeiter“ und „gemeinsam Verantwortliche“ nach der Verordnung (EU) 2018/1725, November 2019, S. 16 ff

selbst in die Datenbank eingegeben hat. Außerdem verarbeitet jedes Unternehmen die Daten nur für seine eigenen Zwecke. In diesem Szenario gibt es keine gemeinsame Verantwortlichkeit. Die Unternehmen B, C und D sind getrennte Verantwortliche, da sie die Zwecke ihrer Datenverarbeitung selbst bestimmen. Unternehmen A gilt als Auftragsverarbeiter, da es ein Mittel zur Verarbeitung bereitstellt, nämlich die Speicherung der personenbezogenen Daten in seiner Datenbank.

3.4 Auftragsverarbeiter

3.4.1 Wer ist dieser Akteur?

Ein Auftragsverarbeiter ist gemäß Art. 4 Absatz 8 DSGVO *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet."* Dies zeigt, dass eine Vielzahl von Einrichtungen als Auftragsverarbeiter angesehen werden kann, sofern es sich um eine **von dem Verantwortlichen getrennte Einrichtung** handelt und die Verarbeitung **im Auftrag des Verantwortlichen erfolgt**. Die Verantwortlichen können natürlich auch selbst personenbezogene Daten verarbeiten. Sie bleiben jedoch als Verantwortliche bestehen, wenn sie nicht nur personenbezogene Daten verarbeiten, sondern auch die Mittel und Zwecke der Verarbeitung bestimmen.

3.4.2 Was sind seine Aufgaben?

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Der Auftragsverarbeiter muss geeignete organisatorische und technische Maßnahmen ergreifen, um den Datenschutz zu gewährleisten. Bei der eigentlichen Verarbeitung kann es sich sowohl um eine spezifische und detaillierte Aufgabe als auch um eine allgemeinere Verarbeitung handeln. Ein Verantwortlicher kann daher auch beschließen, nur einen bestimmten Teil der Verarbeitung an einen externen Auftragsverarbeiter zu delegieren und Teile der eigentlichen Verarbeitung durchzuführen.

Die Verarbeitung personenbezogener Daten erfolgt nach den Anweisungen des Verantwortlichen. Daher sollten personenbezogene Daten nicht auf andere Weise verarbeitet werden als mit dem Verantwortlichen vereinbart.

Ein Auftragsverarbeiter kann Unterauftragsverarbeiter benennen, benötigt dafür aber die schriftliche Zustimmung des Verantwortlichen. Der/die Unterauftragsverarbeiter sollte/n die Daten zu denselben Bedingungen verarbeiten wie der ursprüngliche Auftragsverarbeiter.

3.4.3 Was sind seine Rechte und Pflichten?

Der Auftragsverarbeiter handelt nach den Anweisungen und Bedingungen des Verantwortlichen. Der Auftragsverarbeiter kann jedoch bis zu einem gewissen Grad die technischen und organisatorischen Mittel einsetzen und auswählen, die ihm für die Verarbeitung am geeignetsten erscheinen. Dieser **Grad der Einflussnahme**[197] des Auftragsverarbeiters ist jedoch nicht definiert, was bedeutet, dass die sicherste Option darin besteht, eine Reihe von Mitteln zwischen Auftragsverarbeiter und Verantwortlichem vertraglich zu vereinbaren. Es kann auch zwischen wesentlichen (welche Daten, von wem, wie lange, wer soll darauf zugreifen) und nicht wesentlichen (praktische, technische Aspekte

197 Weitere Informationen über dieses Kompetenzniveau und eine Unterscheidung zwischen wesentlichen und nicht wesentlichen Mitteln finden Sie unter: EDBP. https://edpb.europa.eu/sites/edpb/files/consultation/EDSA_guidelines_202007_controllerprocessor_en.pdf S.14

der Verarbeitung) Mitteln der Verarbeitung unterschieden werden. Die wesentlichen Mittel sind eindeutig von dem Verantwortlichen bereitzustellen, da sie mit den Zwecken der Verarbeitung verbunden sind. Die nicht wesentlichen Mittel können vom Auftragsverarbeiter erörtert werden, um die Verarbeitung zu implementieren und durchzuführen. Wie bereits erörtert, muss diese Frage jedoch von Fall zu Fall entschieden werden.

Im Hinblick auf die Verantwortlichkeiten muss der Auftragsverarbeiter *„hinreichende Garantien“* (Artikel 28 Absatz 1 DSGVO) dafür bieten, dass die Verarbeitung den Anforderungen der Datenschutz-Grundverordnung entspricht. Diese Garantien sind von wesentlicher Bedeutung, da der Verantwortliche verpflichtet ist, nur Auftragsverarbeiter einzusetzen, die solche Garantien bieten und die Einhaltung der DSGVO und den Schutz der betroffenen Personen nachweisen können. In Artikel 28 Absatz 3 Buchstaben a–h der DSGVO sind alle Informationen aufgeführt, die in einem schriftlichen Vertrag zwischen dem Auftragsverarbeiter und dem Verantwortlichen enthalten sein müssen, bevor Daten verarbeitet werden. Das bedeutet, dass der Auftragsverarbeiter nur nach den schriftlichen Anweisungen des Verantwortlichen handeln darf und die Sicherheit und Vertraulichkeit der Daten sowie die Dokumentation aller Verarbeitungstätigkeiten gewährleistet. In Artikel 30 Absatz 2 DSGVO heißt es, dass jeder Auftragsverarbeiter „ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung“ führen muss.

Beispiel:

Die Forschungseinrichtung A hat mithilfe eines Fragebogens eine große Datenbank mit personenbezogenen Daten der betroffenen Personen erfasst. Einrichtung A beauftragt das Datenanalyseunternehmen B mit der Analyse der Daten, um in den Daten verborgene Zusammenhänge zu finden. In diesem Beispiel handelt A als Verantwortlicher, da A die Zwecke und Mittel der Verarbeitung festlegt, während B als Auftragsverarbeiter handelt, der die Verarbeitung im Auftrag des Verantwortlichen durchführt. Das Datenanalyseunternehmen B beschließt nun, die personenbezogenen Daten für seine eigenen Zwecke zu verwenden, die nicht vertraglich vereinbart wurden.

Mit dieser Weiterverarbeitung der personenbezogenen Daten wird B zum Verantwortlichen für diese neue Art der Verarbeitung. Mit diesen Handlungen verstößt B auch gegen die Datenschutz-Grundverordnung.[198] Folglich kann gegen Einrichtung B ein Bußgeld wegen eines Verstoßes gegen die DSGVO verhängt werden, der sich aus der neuen Verarbeitung einschließlich einer möglichen Verletzung des Schutzes personenbezogener Daten ergeben könnte. Auch in diesem Fall trägt Einrichtung A keine Verantwortung für den genannten Vorfall. Einrichtung A hätte einen geeigneteren Auftragsverarbeiter wählen und sich im Vorfeld Garantien für eine konforme Verarbeitung der Daten geben lassen sollen. Vertragliche Vereinbarungen dienen dazu, die Rollen, Rechte und Pflichten/Zuständigkeiten aller Parteien bei der Verarbeitung personenbezogener Daten klar zu definieren.

3.5 Empfänger

3.5.1 Wer ist dieser Akteur?

Art. 4 Absatz 9 DSGVO definiert einen Empfänger als *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.“*

198 https://edpb.europa.eu/sites/edpb/files/consultation/EDSA_guidelines_202007_controllerprocessor_en.pdf S.25

Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, sind jedoch ausdrücklich von dieser Definition ausgenommen und gelten nicht als Empfänger (Art. 4 Absatz 9 Absatz 2 DSGVO).

Jede andere Person wird als Empfänger betrachtet, wenn sie personenbezogene Daten erhält. Daher gelten ein Auftragsverarbeiter oder ein Dritter, die beide in diesem Dokument als Hauptakteure behandelt werden, als Empfänger, wenn ein Verantwortlicher personenbezogene Daten an sie übermittelt.[199]

3.5.2 Was sind seine Aufgaben?

Der Empfänger hat keine aktive Rolle, da er nur durch den Zugang zu den Daten definiert ist. Erhält eine Stelle personenbezogene Daten und verarbeitet sie, wird sie natürlich zum Verantwortlichen. Dies zeigt, dass sich die Art und die Rolle des Akteurs mit dem Zugang zu und der Verarbeitung von personenbezogenen Daten ändern.

3.5.3 Was sind seine Rechte und Pflichten?

Den Empfängern werden keine besonderen Rechte gewährt. Wenn personenbezogene Daten an einen Empfänger weitergegeben werden, muss der Verantwortliche die betroffenen Personen über den Empfänger informieren. Im Falle einer Berichtigung oder Löschung durch die betroffene Person muss der Empfänger über solche Änderungen informiert werden[200]. Wenn die Empfänger jedoch selbst Verantwortliche oder Auftragsverarbeiter sind, können sie je nach dem räumlichen Geltungsbereich der Verordnung als Verantwortliche oder Auftragsverarbeiter unter die Bestimmungen der DSGVO fallen.

Beispiel:

Eine Privatperson bestellt bei einem Online-Lebensmittellieferdienst, Unternehmen C, eine Mahlzeit. Das Unternehmen C, das die Webschnittstelle anbietet, ist jedoch nicht das Restaurant, das die Mahlzeit herstellt, sondern handelt auf Wunsch der Person, indem es die Bestellung an ein Restaurant weiterleitet und das Essen dann selbst ausliefert. Sowohl C als auch R gelten als für die Verarbeitung der personenbezogenen Daten Verantwortliche, die sie vornehmen, um ihre jeweiligen Dienste anzubieten. Da C die personenbezogenen Daten, d. h. Bestellinformationen und Adresse, an das Restaurant R weitergibt, wird R als Empfänger der Daten angesehen. In diesem Szenario gibt es keine Beziehung zwischen dem Verantwortlichen und dem Empfänger.[201]

---

199 Siehe https://edpb.europa.eu/sites/edpb/files/consultation/EDSA_guidelines_202007_controllerprocessor_en.pdf S.29 für dieses Beispiel.

200 Art. 19 DSGVO Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

201 Beispiel ähnlich dem Beispiel auf S. 29 des EDSA, Guidelines 07/2020 on the concepts of controller and processor in the DSGVO, 2020. Verfügbar unter: https://edpb.europa.eu/sites/default/files/consultation/EDSA_guidelines_202007_controllerprocessor_en.pdf (Letzter Zugriff: 05.10.2021)

3.6 Dritter

3.6.1 Wer ist dieser Akteur?

Art. 4 Absatz 10 definiert einen Dritten als *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.“* Mitarbeiter, die nicht befugt sind, personenbezogene Daten zu verarbeiten, zu denen sie Zugang erhalten haben, werden daher als Dritte definiert.

Beispiel:

Eine Forschungseinrichtung oder ein Lehrstuhl an einer Universität, die bzw. der für die Verarbeitung personenbezogener Daten verantwortlich ist, beauftragt einen Reinigungsdienst. Das Reinigungspersonal kann nun technisch auf diese personenbezogenen Daten zugreifen, wenn es die Schreibtische der Organisation reinigt, auf denen die personenbezogenen Daten gespeichert sein könnten. Auch wenn das Reinigungspersonal die Daten nicht verarbeitet und dies auch nicht will, kann es mit den Daten in Kontakt kommen. Der Reinigungsdienst und sein Personal werden als Dritte betrachtet. Um als Verantwortlicher zu gelten, müsste das Reinigungspersonal in diesem Beispiel beispielsweise die Daten fotografieren oder ins Internet stellen. Dies würde dann als Verarbeitung der Daten gelten, wodurch das Reinigungspersonal zu einem Verantwortlichen wird. Als Verantwortlicher muss die Organisation technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass Unbefugte – Dritte – keinen Zugriff auf personenbezogene Daten haben. Dazu gehört die sichere Speicherung der Daten in einer Weise, dass andere Stellen, hier Dritte, nicht in der Lage sind, auf die Daten zuzugreifen, weder versehentlich noch absichtlich.

3.7 Datenschutzbeauftragter (DSB)

3.7.1 Wer ist der Akteur?

Der Datenschutzbeauftragte ist eine natürliche Person, die fachlich qualifiziert ist, um innerhalb einer Organisation unabhängig zu arbeiten und die Anwendung der DSGVO in dieser Organisation sicherzustellen. Die Datenschutzbeauftragten gewährleisten daher die korrekte Verarbeitung personenbezogener Daten innerhalb eines Unternehmens, seien es die personenbezogenen Daten seiner Mitarbeiter, seiner Kunden oder anderer betroffener Personen. Art. 37 Absatz 1 DSGVO listet die Umstände auf, unter denen ein DSB zu benennen ist, z. B. bei Behörden, die Daten verarbeiten, oder in Fällen, in denen betroffene Personen regelmäßig überwacht werden müssen. Art. 37 DSGVO besagt ferner, dass ein DSB die beruflichen Qualitäten zur Einhaltung seiner Aufgaben aufweisen sollte und dass die Kontaktdaten des DSB der Aufsichtsbehörde mitzuteilen sind. In der Folge haben alle EU-Organe und -Einrichtungen einen behördlichen Datenschutzbeauftragten benannt.[202] Der EDSB stellt fest, dass ein DSB „… ein Experte für Datenschutzrecht und -praktiken sein und in der Lage sein sollte, innerhalb der Organisation unabhängig zu agieren.“[203]

202 Eine Liste der Datenschutzbeauftragten in den EU-Organen und -Einrichtungen ist hier zu finden: DSB-Netzwerk, https://edps.europa.eu/node/53 (zuletzt besucht: 02.12.2020)

203 https://edps.europa.eu/data-protection/data-protection/glossary/d_en (zuletzt besucht: 02.12.2020)

3.7.2 Was sind seine Aufgaben?

Es ist die Aufgabe eines DSB, dafür zu sorgen, dass die Rechte der betroffenen Personen, wie Mitarbeiter, Kunden oder andere Personen, geschützt werden, indem er die korrekte Anwendung der DSGVO in einer Organisation sicherstellt. Der DSB sollte ein Verzeichnis der Verarbeitungstätigkeiten führen, die in dieser Organisation durchgeführt oder kontrolliert werden.

Außerdem muss der DSB sicherstellen, dass die Verantwortlichen und die betroffenen Personen über ihre Rechte und Pflichten Bescheid wissen. Dazu gehört auch, dass er das Bewusstsein für die DSGVO schärft und den Verantwortlichen berät, wie er sie innerhalb der Organisation am besten umsetzen kann. Dies geschieht, um Verantwortlichkeit für mögliche Verstöße zu schaffen.

Sollten Beschwerden oder Verstöße auftreten, muss der DSB diese Beschwerden bearbeiten und mit dem EDSB zusammenarbeiten, um die besten Lösungen zu finden. Darüber hinaus ist es die Aufgabe des DSB, die Organisation auf etwaige Versäumnisse bei der Einhaltung der DSGVO aufmerksam zu machen.

3.7.3 Was sind seine Rechte und Pflichten?

Es liegt in der Verantwortung eines DSB, die Einhaltung der DSGVO bei der Verarbeitung personenbezogener Daten sicherzustellen. Die DSB sind dafür verantwortlich sicherzustellen, dass die Rechte der betroffenen Personen, z. B. Art. 12–23 DSGVO, wie z. B. das Recht auf Auskunft und das Recht auf Berichtigung, nicht beeinträchtigt werden. Zu diesem Zweck müssen die Datenschutzbeauftragten ein Verzeichnis der Verarbeitungstätigkeiten führen, die in ihrer Organisation kontrolliert oder durchgeführt werden.

Um die oben genannten Aufgaben erfüllen zu können, sollten die DSB mit zusätzlichen Rechten innerhalb ihrer Organisation ausgestattet werden. Die DSB sollten sich nicht in einem Interessenkonflikt befinden, d. h. sie sollten nicht gleichzeitig Auftragsverarbeiter oder Verantwortlicher sein. Datenschutzbeauftragte sollten keine Angestellten mit einem befristeten Arbeitsvertrag sein und nicht einem direkten Vorgesetzten unterstellt sein, da diese Umstände einen Datenschutzbeauftragten daran hindern könnten, seine Aufgabe effektiv zu erfüllen. Stattdessen sollten die DSB in der Lage sein, ihre Arbeit unabhängig auszuführen, und sie sollten direkt an die oberste Führungsebene berichten. Darüber hinaus sollten die DSB für die Verwaltung ihres eigenen Budgets verantwortlich sein und die Ressourcen und das Personal erhalten, die sie für die Durchführung ihrer Arbeit benötigen.[204] Dazu gehört auch die Befugnis, innerhalb einer Organisation oder eines Forschungsprojekts unabhängig zu ermitteln.

3.8 Aufsichtsbehörde

3.8.1 Wer ist der Akteur?

Die Aufsichtsbehörde ist eine unabhängige Behörde, die von den Mitgliedstaaten der EU eingerichtet wurde. Gesetze sind nur dann wirksam, wenn ihre Einhaltung überwacht und Verstöße sanktioniert werden. Aus diesem Grund sieht die Datenschutz-Grundverordnung in Kapitel 6 unabhängige Aufsichtsbehörden vor. Weniger formell werden sie auch als Datenschutzbehörden (Data Protection Authorities, DPAs) bezeichnet. Datenschutzbehörden sind Teil der Exekutive und arbeiten unabhängig, um andere Regierungsbehörden beaufsichtigen zu können.

204 https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

3.8.2 Was sind ihre Aufgaben?

Die Aufsichtsbehörden oder Datenschutzbehörden sind für die Überwachung und Durchsetzung der Anwendung der Datenschutz-Grundverordnung verantwortlich. Darüber hinaus sollen sie das Bewusstsein und das Verständnis der Öffentlichkeit für Fragen der Datenverarbeitung fördern. Sie sollen auch das Bewusstsein für die Pflichten der Verantwortlichen und der Auftragsverarbeiter personenbezogener Daten im Rahmen der Datenschutz-Grundverordnung fördern.

Die Aufsichtsbehörde ist einer der Ansprechpartner für die betroffenen Personen, wenn sie sich über Missstände beschweren wollen, und sie ist berechtigt, solche Missstände zu untersuchen. Die Aufsichtsbehörde legt auch die Kriterien für die Zertifizierung des Nachweises der Einhaltung der Vorschriften fest.

Die genauen Aufgaben der Aufsichtsbehörden sind in Art. 57 DSGVO geregelt. Die folgende Teilmenge der 22 in Art. 57 Absatz 1 aufgeführten Aufgaben soll einen Überblick geben:

- Überwachung und Durchsetzung der Datenschutzgrundverordnung.
- Sensibilisierung der betroffenen Personen, der Öffentlichkeit, der Verantwortlichen und der Auftragsverarbeiter für ihre Rechte und Pflichten in Bezug auf den Datenschutz.
- Bearbeitung von Beschwerden der betroffenen Personen.
- Durchführung von Untersuchungen
- Annahme, Genehmigung oder Billigung verschiedener Arten von Vertragsklauseln, Bestimmungen oder verbindlichen Unternehmensregeln.

Zur Durchsetzung der DSGVO verfügen die Aufsichtsbehörden über „Abhilfebefugnisse" (Artikel 58 Absatz 2 DSGVO), die von einfachen Verwarnungen über Geldbußen bis hin zum Verbot der Verarbeitung reichen.

3.8.3 Was sind ihre Rechte und Pflichten?

Die Aufsichtsbehörde ist dafür verantwortlich, die korrekte Anwendung der DSGVO bei der Verarbeitung personenbezogener Daten durchzusetzen. Zu diesem Zweck sollte die Aufsichtsbehörde bei der Ausübung ihrer Befugnisse, einschließlich der Untersuchungsbefugnisse, der Abhilfebefugnisse und der Sanktionen, der Befugnis zur vorübergehenden oder endgültigen Einschränkung der Verarbeitung, einschließlich eines Verbots, sowie der Verhängung von Geldbußen, unabhängig handeln. Insbesondere sollte jede Maßnahme geeignet, erforderlich und verhältnismäßig sein, um die Einhaltung der DSGVO zu gewährleisten. Die EU-Mitgliedstaaten müssen sicherstellen, dass die Aufsichtsbehörde mit ausreichenden finanziellen, personellen und technischen Ressourcen ausgestattet ist.

3.8.4 Gibt es in jedem Mitgliedstaat eine Aufsichtsbehörde?

„*Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der [DSGVO] zuständig sind.*“ (Art. 51 Absatz 1 DSGVO).

In der Praxis bedeutet dies, dass einige Mitgliedstaaten eine einzige nationale Aufsichtsbehörde haben, während andere mehrere haben. In Frankreich gibt es zum Beispiel eine einzige Aufsichtsbehörde, die Commission nationale de l'informatique et des libertés (CNIL)[205]. In Deutschland hingegen gibt es mehrere Aufsichtsbehörden. Sie sind alle **auf der gleichen Ebene angesiedelt**, aber für unterschiedliche Arten von Verarbeitungstätigkeiten

205 https://www.cnil.fr/

verantwortlich und zuständig: Verarbeitungstätigkeiten von Bundesbehörden und bestimmte Arten von Verarbeitungen fallen in den Zuständigkeitsbereich des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)[206]; die Zuständigkeit für andere öffentliche und private Verarbeitungstätigkeiten ist geografisch nach Bundesländern unterteilt; spezielle Datenschutzbehörden der Kirchen sind für die Verarbeitungstätigkeiten der Kirchen zuständig.

3.8.5 Kann ich die Entscheidungen der Aufsichtsbehörde anfechten? Welches ist das höchste Berufungsgericht?

Die Entscheidungen einer Aufsichtsbehörde können vor Gericht angefochten werden (Art. 78 DSGVO). Dies geschieht in der Regel vor einem nationalen Verwaltungsgericht. Gegen die Entscheidung dieser ersten Instanz kann bei übergeordneten Gerichten bis hin zum obersten nationalen Gericht Berufung eingelegt werden. Darüber hinaus ist die höchste gerichtliche Instanz der Europäische Gerichtshof (EuGH).

Beachten Sie, dass es für die Verantwortlichen oder die Auftragsverarbeiter keinen Mechanismus gibt, um gegen die Entscheidung einer Aufsichtsbehörde eines Mitgliedstaates beim Europäischen Datenschutzausschuss Beschwerde einzulegen.

3.9 Europäischer Datenschutzausschuss (EDSA)

3.9.1 Wer ist der Akteur?

Der Europäische Datenschutzausschuss (EDSA[207]) ist eine *„Einrichtung der Union" mit „Rechtspersönlichkeit*“, die auf der Grundlage von Art. 68 DSGVO eingerichtet wurde. Er setzt sich aus einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten (EDSB) zusammen, der später noch vorgestellt wird. Der EDSB hat mit Inkrafttreten der Datenschutz-Grundverordnung die Artikel-29-Datenschutzgruppe (WP29) ersetzt. Dabei hat er auch einige der Stellungnahmen der Datenschutzgruppe zu den Leitlinien übernommen[208].

Der Europäische Datenschutzbeauftragte ist für eine große Anzahl von Aufgaben zuständig, die in Art. 70 DSGVO aufgeführt sind. Zu diesen Aufgaben gehören unter anderem die Herausgabe von Leitlinien, Stellungnahmen, Empfehlungen und bewährten Praktiken für die Anwendung der DSGVO, die Beratung der Europäischen Kommission in Fragen der DSGVO und die Förderung des Wissens- und Informationsaustauschs zwischen den verschiedenen Aufsichtsbehörden.

Vor allem geht es dem EDSB um die kohärente Anwendung und Auslegung der Datenschutz-Grundverordnung in allen Mitgliedstaaten. Gemäß Art. 65 Absatz 1 DSGVO erlässt der EDSB verbindliche Entscheidungen, wenn eine federführende Aufsichtsbehörde einer Stellungnahme des EDSB nicht folgt oder wenn verschiedene Aufsichtsbehörden widersprüchliche Ansichten über die Anwendung der DSGVO vertreten.[209] In solchen Fällen wird das *„**Kohärenzverfahren**“* ausgelöst, in dessen Rahmen der EDSB Stellungnahmen

206 https://www.bfdi.bund.de

207 Weitere Informationen über den EDSA finden Sie auf der offiziellen EU-Website: https://edpb.europa.eu/about-edpb/about-edpb_en

208 Europäischer Datenschutzausschuss, (EDSA), Endorsement 1/2018, https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf (zuletzt besucht am 24.11.2020).

209 Art. 65 Absatz 1 DSGVO „Streitbeilegung durch den Ausschuss"

dazu abgeben kann, wie die Datenschutz-Grundverordnung in mehreren Mitgliedstaaten anzuwenden ist. Wenn die Aufsichtsbehörden dieser Mitgliedstaaten eine Stellungnahme des EDSB nicht respektieren, kann der EDSB verbindliche Entscheidungen treffen, die von den Aufsichtsbehörden respektiert werden müssen, um Streitigkeiten zu lösen[210].

3.9.2 Was sind seine Aufgaben?

Der EDSA hat die Aufgabe, die Europäische Kommission in Fragen des Schutzes personenbezogener Daten, des Formats und der Verfahren für den Informationsaustausch zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden sowie der Zertifizierung zu beraten. Darüber hinaus fördert er die Zusammenarbeit und den effektiven bilateralen und multilateralen Austausch von Informationen und bewährten Verfahren zwischen den Aufsichtsbehörden. Er gibt Leitlinien, Empfehlungen und bewährte Praktiken heraus und prüft alle Fragen zu diesen oder zur DSGVO. Die Akkreditierung von Zertifizierungsstellen und deren regelmäßige Überprüfung wird vom EDSA durchgeführt. Außerdem erstellt er einen Jahresbericht über den Schutz natürlicher Personen, die Verarbeitung in der Union, in Drittländern und bei internationalen Organisationen.

3.9.3 Was sind seine Rechte und Pflichten?

Der EDSA handelt bei der Einhaltung seiner Aufgaben unabhängig.

Um seine Aufgaben zu erfüllen, kann der EDSA verbindliche Entscheidungen, Stellungnahmen und Leitlinien veröffentlichen und erstellen. So hat der EDSA beispielsweise die Leitlinien der Artikel-29-Datenschutzgruppe, etwa zu Einwilligung, Transparenz und vielem mehr[211], gebilligt und zusätzliche Leitlinien veröffentlicht[212]. Wie bereits erwähnt, kann der EDSA Stellungnahmen und verbindliche Entscheidungen über die Anwendung der Datenschutz-Grundverordnung in den Mitgliedstaaten abgeben.

3.10 Europäischer Datenschutzbeauftragter (EDSB)

3.10.1 Wer ist dieser Akteur?

Der Europäische Datenschutzbeauftragte (EDSB[213]) ist die Aufsichtsbehörde für die Verarbeitungstätigkeiten der europäischen Organe und Einrichtungen. Er ist eine unabhängige Aufsichtsbehörde der Europäischen Union. Im Gegensatz zu den anderen Akteuren wurde der EDSB nicht durch die Datenschutz-Grundverordnung, sondern durch die Verordnung (EU) Nr. 2018/1725 eingerichtet.

3.10.2 Was sind seine Aufgaben?

Die Aufgaben des EDSB sind die Überwachung und der Schutz personenbezogener Daten, wenn diese von EU-Institutionen verarbeitet werden, und die Beratung anderer EU-Institutionen in Bezug auf solche Verarbeitungen sowie die damit verbundenen

210 Siehe „Consistency Findings“, EDSA, verfügbar unter https://edpb.europa.eu/our-work-tools/consistency-findings_en (zuletzt besucht am 25.11.2020)

211 Endorsement 1/2018, EDSA, verfügbar unter https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf (zuletzt besucht: 25.11.2020)

212 Siehe „GDPR: Guidelines, Recommendations, Best Practices", https://edpb.europa.eu/our-work-tools/general-guidance/DSGVO-guidelines-recommendations-best-practices_en für eine Liste von Leitlinien und Empfehlungen des EDSA

213 Weitere Informationen über den EDSB finden Sie auf der offiziellen EU-Website: https://edps.europa.eu/about-edps_en. (Zuletzt besucht am 30.10.2020)

Rechtsvorschriften und Rechtsakte. Darüber hinaus überwacht er Technologien, die den Datenschutz beeinflussen könnten, und arbeitet mit den nationalen Aufsichtsbehörden im Bereich des Datenschutzes zusammen. Darüber hinaus berät der EDSB EU-Institutionen wie die Europäische Kommission in Angelegenheiten, die die Datenverarbeitung betreffen, wie etwa neue Rechtsvorschriften und Vereinbarungen. Er überwacht auch neue Technologien, die sich auf den Datenschutz auswirken könnten, und arbeitet mit den nationalen Aufsichtsbehörden zusammen.[214]

3.10.3 Was sind seine Rechte und Pflichten?

Der EDSB kann Untersuchungen über den Schutz von Anwendungsdaten durchführen. Daher kann er die Verantwortlichen und die Auftragsverarbeiter auffordern, Informationen bereitzustellen oder Schutzaudits durchzuführen. Darüber hinaus kann der EDSB Warnungen aussprechen, wenn Verstöße wahrscheinlich sind, oder Verweise aussprechen, wenn Verstöße festgestellt werden, und spezifische Maßnahmen zur Behandlung von Verstößen anordnen. Darüber hinaus kann er Geldbußen für die unrechtmäßige Verarbeitung von Daten verhängen oder die Verarbeitung ganz verbieten.

DOs

- Prüfen Sie, welche Art von Akteur oder Rolle Sie oder Ihre Organisation bei der Arbeit mit personenbezogenen Daten im Rahmen der Datenschutz-Grundverordnung darstellen. Jeder Akteur hat bestimmte Rechte und Pflichten.
- Vergewissern Sie sich, dass Sie wissen, welche Art von Akteur andere Stellen sind, mit denen Sie zusammenarbeiten. Dies kann je nach dem Datenfluss zwischen verschiedenen Einrichtungen und Organisationen unterschiedlich sein.
- Verstehen Sie die Aufgaben, Rechte und Pflichten, die jeder Akteur bei der Arbeit mit personenbezogenen Daten hat.
- Stellen Sie sicher, dass die Rollen, Zuständigkeiten und Aufgaben der verschiedenen Organisationen im Zusammenhang mit der Verarbeitung personenbezogener Daten vertraglich festgelegt werden.
- Konsultieren Sie zusätzliche Literatur wie die Leitlinien des EDSB zu den Begriffen „Verantwortliche“, „Auftragsverarbeiter“ und der „gemeinsam Verantwortliche“ nach der Verordnung (EU) 2018/1725 und die Leitlinien 07/2020 zu den Begriffen des Verantwortlichen und des Auftragsverarbeiters in der Datenschutzgrundverordnung.

214 Ebd.