FAQ
Verantwortlicher / Auftragsverarbeiter

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Inhalt

Hinweis: Die Erläuterungen in diesem Dokument ergänzen die „Guidelines on the concepts of controller and processor in the GDPR“ des Europäischen Datenschutzausschusses (EDSA). Die angegebenen Randnummern beziehen sich auf diese Original-Leitlinien.

Teil I der Guidelines – Rechtliche Begriffe

1. Wer ist überhaupt „Verantwortlicher“ (Artikel 4 Nummer 7 DS-GVO)? [Randnummern 15-17]

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. Grundsätzlich gibt es keine Einschränkung, wer die Rolle eines Verantwortlichen übernehmen kann. Es kann sich um eine Organisation, aber auch um eine Einzelperson oder eine Gruppe von Einzelpersonen handeln. Bei der Datenverarbeitung innerhalb einer Firmengruppe ist besonders darauf zu achten, ob eine Einrichtung als Verantwortlicher oder als Auftragsverarbeiter auftritt, z.B. bei der Datenverarbeitung im Auftrag der Muttergesellschaft.

2. Was bedeutet „Bestimmung der Zwecke und Mittel“? [Randnummer 35]

Die Bestimmung der Zwecke und Mittel bedeutet, das „Warum“ bzw. das „Wie“ der Verarbeitung zu bestimmen: Der Verantwortliche ist derjenige, der bestimmt hat, warum die Verarbeitung erfolgt (d.h. zu welchem Zweck oder wozu) und wie dieses Ziel erreicht werden soll, d.h. welche Mittel oder sogar welche Datenverarbeitungen zur Erreichung des Ziels eingesetzt werden sollen.

3. Welche Situationen können eine Verantwortlichkeit begründen? [Randnummer 22-25]

Die Verantwortlichkeit kann aus einer ausdrücklichen rechtlichen Zuständigkeit abgeleitet werden, z.B. wenn der Verantwortliche oder die spezifischen Kriterien für seine Ernennung durch nationales oder Unionsrecht festgelegt sind. In der Regel wird das Gesetz den Verantwortlichen nicht direkt ernennen oder die Kriterien für seine Ernennung festlegen, sondern vielmehr eine Aufgabe festlegen oder jemandem die Pflicht auferlegen, bestimmte Daten zu sammeln und zu verarbeiten. Der Zweck der Verarbeitung wird dann häufig durch das Gesetz bestimmt. Der Verantwortliche ist dann derjenige, der vom Gesetz für die Verwirklichung dieses Zwecks bestimmt wurde.
Wenn sich die Rolle des Verantwortlichen nicht aus gesetzlichen Bestimmungen ergibt, muss sie auf Grundlage der tatsächlichen Umstände der Verarbeitung festgelegt werden, d.h. Verantwortlicher ist derjenige, der die Zwecke und Mittel der Datenverarbeitung tatsächlich festgelegt hat (s. Frage 2!).

4. Kann eine bestimmte Person zum Verantwortlichen ernannt werden? [Randnummern 18, 19]

Eine bestimmte Person kann damit betraut werden, die Verarbeitungsvorgänge durchzuführen. Doch selbst wenn eine bestimmte natürliche Person, damit betraut wird, die Einhaltung der Datenschutzbestimmungen zu gewährleisten, ist diese Person nicht der Verantwortliche im Sinne von Artikel 4 Nummer 7 DS-GVO, sondern handelt im Namen der juristischen Person (Unternehmen oder öffentliche Körperschaft), die im Falle eines Regelverstoßes letztendlich verantwortlich ist. Ebenso gilt: selbst wenn eine bestimmte Abteilung oder Einheit einer Organisation die operative Verantwortung für die Sicherstellung der Einhaltung bestimmter Verarbeitungstätigkeiten trägt, bedeutet dies nicht, dass diese Abteilung oder Einheit (und nicht die Organisation als Ganzes) zum Verantwortlichen wird.

Grundsätzlich kann davon ausgegangen werden, dass jede Verarbeitung personenbezogener Daten durch Mitarbeiter, die im Rahmen der Tätigkeiten einer Organisation erfolgt, unter der Kontrolle dieser Organisation stattfindet. In Ausnahmefällen kann es jedoch vorkommen, dass ein Mitarbeiter beschließt, personenbezogene Daten für seine eigenen Zwecke zu verwenden und damit die ihm übertragene Befugnis unrechtmäßig überschreitet. Dem muss die Organisation als verantwortliche Stelle durch geeignete technische und organisatorische Maßnahmen (wie z.B. Schulungen) entgegentreten, um die Einhaltung der DS-GVO zu gewährleisten.

5. Kann sich die Rolle des Verantwortlichen aus einem Vertrag ergeben? [Randnummer 28]

Vertragsklauseln können darstellen, wer in Bezug auf die Zwecke und Mittel der Verarbeitung eine Entscheidungsbefugnis hat. Ein Vertrag darf den Parteien jedoch nicht die Möglichkeit geben, die Verantwortlichkeit nach eigenem Ermessen zuzuweisen. Die tatsächlichen müssen von dem Vertrag abgebildet werden und sind für die Bestimmung der Verantwortung entscheidend. Ein Verantwortlicher kann sich nicht seiner Verantwortung entziehen, indem der Vertrag einfach in einer bestimmten Weise gestaltet wird, wenn das nicht den tatsächlichen Umständen entspricht.

6. Kann jemand gleichzeitig Verantwortlicher und Auftragsverarbeiter sein? [Randnummer 26]

Ja. Die Verantwortlichkeit ergibt sich nicht aus der Art der datenverarbeitenden Stelle, sondern aus ihren konkreten Aktivitäten in einem bestimmten Kontext. Ein und dieselbe Stelle kann also gleichzeitig als Verantwortlicher für bestimmte Datenverarbeitungen und als Auftragsverarbeiter für andere Datenverarbeitungen tätig sein. Dies muss jeweils mit Blick auf die spezifische Datenverarbeitungstätigkeit beurteilt werden.

7. Kann auch ein Auftragsverarbeiter bestimmte Entscheidungen über die Datenverarbeitung treffen? [Randnummern 36, 40]

Entscheidungen über die Zwecke der Verarbeitung sind stets dem Verantwortlichen vorbehalten. Dagegen können Entscheidungen über nicht-wesentliche Mittel der Verarbeitung auch durch den Auftragsverarbeiter getroffen werden. „Nicht-wesentliche Mittel“ betreffen eher praktische Aspekte

der Durchführung wie die Wahl einer bestimmten Hard- oder Software oder detaillierte Sicherheitsmaßnahmen, deren Entscheidung dem Auftragsverarbeiter überlassen werden kann, soweit diese nicht im Vertrag über die Auftragsverarbeitung vorgegeben sind.
Davon zu unterscheiden sind die wesentlichen Mittelder Verarbeitung. Die „wesentlichen Mittel" stehen in engem Zusammenhang mit dem Zweck und dem Umfang der Verarbeitung und sind daher prinzipiell dem Verantwortlichen vorbehalten. Beispiele für wesentliche Mittel sind die Art der personenbezogenen Daten, die verarbeitet werden, die Dauer der Verarbeitung, die Kategorien der Empfänger und die Kategorien der betroffenen Personen.

Beispiel: Hosting-Dienste

Arbeitgeber A beauftragt den Hosting-Dienst H, verschlüsselte Daten auf den Servern von H zu speichern. Der Hosting-Dienstleist H stellt weder fest, ob es sich bei den von ihm gehosteten Daten um personenbezogene Daten handelt, noch verarbeitet er die Daten auf eine andere Weise als durch Speicherung auf seinen Servern. Da die Speicherung ein Beispiel für eine Tätigkeit zur Verarbeitung personenbezogener Daten ist, verarbeitet der Hosting-Dienst H personenbezogene Daten im Auftrag von Arbeitgeber A und ist daher ein Auftragsverarbeiter. Arbeitgeber A muss H die erforderlichen Weisungen erteilen und eine Auftragsverarbeitungsvereinbarung nach Artikel 28 abschließen, der H zur Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen verpflichtet. H muss A dabei unterstützen, dass die erforderlichen Sicherheitsmaßnahmen getroffen werden, und ihn im Falle einer Verletzung des Schutzes personenbezogener Daten benachrichtigen.

8. Umfasst die „Bestimmung der Zwecke und Mittel" durch den Verantwortlichen immer ein ganzes Verarbeitungssystem? [Randnummer 42]

Nein. Artikel 4 Nummer 2 DS-GVO definiert die Verarbeitung personenbezogener Daten als „jeden Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten". Demzufolge kann der Begriff des Verantwortlichen entweder bezüglich einem einzelnen Verarbeitungsvorgang oder einer Reihe von Vorgängen vorliegen. Die Verantwortlichkeit kann sich also auf die Gesamtheit der fraglichen Prozesse erstrecken, aber auch auf einen bestimmten Abschnitt beschränkt sein.

9. Umfasst die gemeinsame „Bestimmung der Zwecke und Mittel" bei der gemeinsamen Verantwortlichkeit immer die gesamten Verarbeitungsvorgänge eines Projekts? [Randnummer 56-57]

Nein. Eine Stelle ist nur in Bezug auf diejenigen Vorgänge als gemeinsam mit der/den anderen Stelle(n) verantwortlich anzusehen, für die sie tatsächlich gemeinsam mit anderen die Mittel und Zwecke der Verarbeitung bestimmt. Wenn eine andere Stelle allein über die Zwecke und Mittel von Vorgängen entscheidet, die der Verarbeitungskette vorausgehen oder in ihr nachfolgen, muss diese hierfür als alleinige Verantwortliche angesehen werden. Der EuGH hat auch klargestellt, dass die Stellen in verschiedenen Abschnitten der Verarbeitung und in unterschiedlichem Ausmaß beteiligt sein können, so dass der Grad der Verantwortlichkeit immer im Einzelfall beurteilt werden muss.

10. Muss der Verantwortliche Zugang zu (allen) verarbeiteten personenbezogenen Daten haben? [Randnummer 45]

Nein. Wie der EuGH in seinen Urteilen Wirtschaftsakademie (Az. C-201/16, Randnummer 38) oder im Urteil Jehovas Zeugen (Az. C-25/17, Randnummer 75) ausführt, reicht eine bestimmende Einflussnahme auf den Zweck und die (wesentlichen) Mittel der Verarbeitung aus (z.B. durch die Einstellung von Parametern, die Einfluss auf die Frage haben, wessen personenbezogene Daten verarbeitet werden sollen). Daher kann auch jemand, der eine Verarbeitungstätigkeit auslagert, als Verantwortlicher angesehen werden, wenn er einen solchen Einfluss ausübt, auch wenn er niemals tatsächlich Zugang zu den Daten hat oder haben wird.

Beispiel: Marktforschung

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

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

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

11. Wie kann die Mitwirkung bei gemeinsamer Verantwortlichkeit ausgestaltet sein? [Randnummern 54, 55]

Gemeinsame Verantwortlichkeit kann sich beispielsweise durch gemeinsame Entscheidungen oder konvergierende Entscheidungen von zwei oder mehr Stellen ergeben. Im ersten Fall werden zusammen Entscheidungen unter einer gemeinsamen Absicht getroffen. Im zweiten Fall ergänzen sich die jeweiligen Entscheidungen derart, dass die Verarbeitung ohne die Beteiligung beider Parteien in dem gewünschten Sinne nicht möglich wäre.

12. Scheidet gemeinsame Verantwortlichkeit aus, wenn ein Verantwortlicher ein technisches System zur Verfügung stellt und ein anderer es nutzt? [Randnummern 64-67]

Nein, auch dann kann eine gemeinsame Verantwortung gegeben sein: Vor allem, wenn Systeme von einem Unternehmen zur Verfügung gestellt werden, aber andere diese Systeme nutzen und dabei über die Einrichtung bzw. Einstellungen entscheiden können. Zu solchen Systemen können Plattformen, standardisierte Hilfsmittel oder ähnliches gehören. Entscheidend ist, ob die Nutzer des Systems so über Einstellungen entscheiden können, dass sie einen ausschlaggebenden Einfluss auf die Datenverarbeitung haben. Dies hat der EuGH für Facebook Fanpages (Urteil Wirtschaftsakademie) und im Fashion ID-Urteil bejaht.

Beispiel: Analyse von Gesundheitsdaten

Unternehmen ABC hat eine App zur Blutdrucküberwachung entwickelt. Unternehmen XYZ ist ein Anbieter von Apps für medizinisches Fachpersonal. Beide möchten untersuchen, wie Blutdruckveränderungen zur Vorhersage bestimmter Krankheiten beitragen können. Die Unternehmen beschließen, ein gemeinsames Projekt ins Leben zu rufen und wenden sich an das Krankenhaus DEF, damit sich dieses ebenfalls beteiligt.

Die personenbezogenen Daten, die in diesem Projekt verarbeitet werden, setzen sich aus personenbezogenen Daten zusammen, die Unternehmen ABC, Krankenhaus DEF und Unternehmen XYZ als einzelne Verantwortliche getrennt verarbeiten. Die Entscheidung, diese Daten zur Bewertung von Blutdruckveränderungen zu verarbeiten, wird von den drei Akteuren gemeinsam getroffen. Unternehmen ABC, Krankenhaus DEF und Unternehmen XYZ haben gemeinsam die Zwecke der Verarbeitung festgelegt. Unternehmen XYZ ergreift die Initiative und schlägt die wesentlichen Mittel der Verarbeitung vor. Sowohl Unternehmen ABC als auch das Krankenhaus DEF akzeptieren diese wesentlichen Mittel, nachdem auch sie an der Entwicklung einiger Funktionen der App beteiligt waren, damit die Ergebnisse von ihnen ausreichend genutzt werden können. Die drei Organisationen einigen sich also auf einen gemeinsamen Verarbeitungszweck, nämlich die Beurteilung, wie Blutdruckveränderungen zur Vorhersage bestimmter Krankheiten beitragen können. Sobald die Untersuchung abgeschlossen ist, können Unternehmen ABC, Krankenhaus DEF und Unternehmen XYZ von der Auswertung profitieren, indem sie die Ergebnisse für ihre eigenen Aktivitäten nutzen. Aus all diesen Gründen sind sie für diese spezielle gemeinsame Verarbeitung als gemeinsame Verantwortliche im Sinne des Artikels 26 DS-GVO anzusehen.

Wäre Unternehmen XYZ von den anderen lediglich gebeten worden, diese Bewertung durchzuführen, ohne dass XYZ einen eigenen Zweck verfolgt, und hätte es lediglich Daten im Auftrag der anderen verarbeitet, würde Unternehmen XYZ als Auftragsverarbeiter gelten, selbst wenn es mit der Bestimmung der nicht wesentlichen Mittel betraut wäre.

13. Wer ist bei „Kettenverarbeitungen“ wann verantwortlich? [Randnummer 72]

Bei sogenannten Kettenverarbeitungen, wenn also verschiedene Akteure nacheinander die gleichen personenbezogenen Daten verarbeiten, gilt: Wenn jeder von diesen Akteuren in „seinem“ Teil der Kette unabhängige Zwecke verfolgt und eigenständige Mittel einsetzt, liegt keine gemeinsame Verantwortlichkeit vor. Die Akteure sind dann vielmehr aufeinanderfolgende, voneinander unabhängige Verantwortliche.

Beispiel: Statistische Analyse für eine Aufgabe öffentlichen Interesses

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

14. Wer ist überhaupt „Auftragsverarbeiter“ (Artikel 4 Nummer 8 DS-GVO)? [Randnummer 73]

„Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Ähnlich wie beim Begriff des „Verantwortlichen“ (s. Frage 1) sieht auch die Definition des Auftragsverarbeiters ein breites Spektrum von Akteuren vor. Es kann sich um eine Organisation, aber auch um eine Einzelperson oder eine Gruppe von Einzelpersonen handeln.

15. Welche Grundvoraussetzungen müssen vorliegen, damit jemand als Auftragsverarbeiter gilt? [Randnummer 76-81]

Die beiden Grundvoraussetzungen sind:

1) Der Auftragsverarbeiter muss eine vom Verantwortlichen **getrennte Einheit** sein und

2) er muss personenbezogene Daten **im Namen des Verantwortlichen** verarbeiten.

Dies bedeutet, dass der Verantwortliche beschließt, alle oder einen Teil der Verarbeitungstätigkeiten an eine externe Organisation zu delegieren. Der Auftragsverarbeiter verarbeitet personenbezogene Daten zugunsten des Verantwortlichen, indem er seine Anweisungen (zumindest) in Bezug auf den Zweck der Verarbeitung und die wesentlichen Teile der Mittel umsetzt und die Daten nur im Rahmen dieser Anweisungen verarbeitet.

Eine Auftragsverarbeitung liegt nicht vor, wenn der externe Dienstleister die Daten zu eigenen Zwecken verarbeitet. Dies wäre ein Verstoß gegen Artikel 28 Absatz 10 DS-GVO.

Teil II der Guidelines – Folgen der jeweils zugeschriebenen Rollen (alleinige/gemeinsame Verantwortlichkeit, Auftragsverarbeitung)

16. Wie legen gemeinsame Verantwortliche fest, wer welche Pflichten hat? Braucht man einen Vertrag? [Randnummern 160-161, 172]

Artikel 26 Absatz 1 DS-GVO sieht vor, dass die gemeinsam Verantwortlichen in transparenter Weise festlegen sollen, wer von ihnen welche Verpflichtung aus der DS-GVO erfüllt. Die gemeinsam Verantwortlichen müssen also festlegen, wer was tut, indem sie untereinander entscheiden, wer welche Aufgaben zu erfüllen hat.

Die DS-GVO legt dazu keine Form fest und sagt nicht, dass gemeinsam Verantwortliche dazu einen Vertrag abschließen müssen. Ohne Vertrag oder andere rechtliche Vereinbarung gibt es jedoch keine Rechtssicherheit, wer was zu tun hat. Deswegen empfiehlt der Europäische Datenschutzausschuss allen gemeinsam Verantwortlichen, ein rechtlich bindendes Dokument abzuschließen. Nur dann entsteht auch eine Haftung desjenigen, der sich gegebenenfalls nicht an die Vereinbarung hält.

Darüber hinaus hat eine bindende Vereinbarung über die gemeinsame Verantwortlichkeit den Vorteil, dass die Parteien nachweisen können, dass sie die Verpflichtungen aus der Datenschutz-Grundverordnung einhalten. So kommen sie ihrer Rechenschaftspflicht nach.

17. Wer kümmert sich bei gemeinsamer Verantwortlichkeit um Anfragen von Personen zur Ausübung ihrer Betroffenenrechte? [Randnummern 176, 181-184]

Artikel 26 DS-GVO betont, dass die Verantwortlichkeiten und Aufgaben „insbesondere“ in Bezug auf die Wahrnehmung der Rechte der betroffenen Person und die Informationspflichten gemäß den Artikeln 13 und 14, festzulegen sind. Die gemeinsam Verantwortlichen müssen daher vereinbaren und organisieren, wer die Informationen und die Antworten auf Anfragen zu Betroffenenrechten erteilt und wie dies geschieht. Die gemeinsam Verantwortlichen können auch eine bestimmte Kontaktperson als Anlaufstelle für betroffene Personen benennen.

Beachten sollte man dabei aber, dass betroffene Personen trotzdem stets ein Wahlrecht haben, an welchen der Verantwortlichen sie sich wenden, um ihre Rechte wahrzunehmen (Artikel 26 Absatz 3 DS-GVO).

18. Welche Pflichten werden dem Auftragsverarbeiter durch die DS-GVO auferlegt? [Randnummer 93]

Auftragsverarbeiter haben in Artikel 28 Absatz 3 a) bis h) DS-GVO unter anderem folgende Pflichten:

- Sicherzustellen, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben (Artikel 28 Absatz 3 Buchstabe b),

-Über alle Kategorien der Verarbeitungstätigkeiten Aufzeichnungen zu führen (Artikel 30 Absatz 2) und

- geeignete technische und organisatorische Maßnahmen zu ergreifen (Artikel 32).

Ein Auftragsverarbeiter muss unter bestimmten Bedingungen auch einen Datenschutzbeauftragten benennen (Artikel 37) und ist verpflichtet, den für die Verarbeitung Verantwortlichen unverzüglich zu benachrichtigen, wenn er von einer Datenpanne Kenntnis erlangt hat (Artikel 33 Absatz 2). Die weiteren Vorgaben von Artikel 28 Absatz 3 a) bis h) DS-GVO sind ebenfalls zu beachten.

Darüber hinaus gelten die Vorschriften über die Übermittlung von Daten in Drittländer (Kapitel V) für Auftragsverarbeiter in gleicher Weise wie für Verantwortliche. Der EDSA ist der Ansicht, dass Artikel 28 Absatz 3 DS-GVO den Auftragsverarbeitern direkte Verpflichtungen auferlegt, einschließlich der Pflicht, den Verantwortlichen bei der Einhaltung der datenschutzrechtlichen Vorgaben zu unterstützen.

19. Wie wird eine Auftragsverarbeitungsvereinbarung (AVV) erstellt? [Randnummern 100-115]

Jede Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter muss durch eine rechtliche Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter geregelt werden (Artikel 28 Absatz 3 DS-GVO), die sogenannte Auftragsverarbeitungsvereinbarung (AVV). Eine solche Vereinbarung muss schriftlich erfolgen, wobei hier auch ein elektronisches Format genügt (Artikel 28 Absatz 9). Darüber hinaus muss die Vereinbarung rechtlich bindend sein, also verbindlich sowohl die Verpflichtungen für den Auftragsverarbeiter als auch die Pflichten des Verantwortlichen regeln. Daher sollte die Vereinbarung nicht lediglich die DS-GVO wiedergeben, sondern gezielte und konkrete Informationen darüber enthalten, wie die Anforderungen erfüllt werden und welches Sicherheitsniveau für die Verarbeitung der betroffenen personenbezogenen Daten erforderlich ist.

Um die Verpflichtung zum Abschluss einer AVV zu erfüllen, können Auftragsverarbeiter und Verantwortliche entweder ihren eigenen Vertrag aushandeln oder – ganz oder teilweise – auf die sogenannten Standardvertragsklauseln zurückgreifen. (Besonderheiten zu dem Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020, Rechtssache C-311/18 („Schrems II“) finden Sie in der Orientierungshilfe des LfDI BW zu „Schrems II“.)

Verträge, die vor Inkrafttreten der DS-GVO (25. Mai 2018) geschlossen wurden, hätten nach Artikel 28 Absatz 3 aktualisiert werden müssen. Anderenfalls liegt ein Verstoß vor.

20. Was soll ein Auftragsverarbeiter tun, wenn er Anfragen zur Ausübung der Betroffenenrechte bekommt? [Randnummern 130-132]

Der Verantwortliche muss zwar selbst dafür sorgen, dass die Anträge der betroffenen Personen bearbeitet werden. Mit der Auftragsverarbeitungsvereinbarung (AVV) muss der Auftragsverarbeiter aber auch dazu verpflichtet werden, dies „durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist“, zu unterstützen. Dabei kann es im Einzelfall genügen, einfach unverzüglich jeden eingegangenen Antrag weiterzuleiten. Unter bestimmten Umständen werden dem Auftragsverarbeiter aber auch spezifischere technische Aufgaben übertragen, insbesondere wenn er in der Lage ist, die personenbezogenen Daten zu extrahieren und zu verwalten. Die Einzelheiten über die zu leistende Unterstützung sollten daher in die AVV oder in deren Anhang aufgenommen werden.

Unbedingt zu beachten ist dabei aber: Die praktische Verwaltung einzelner Anfragen kann zwar an den Auftragsverarbeiter ausgelagert werden. Die Verantwortung für die Erfüllung solcher Aufgaben trägt jedoch immer der Verantwortliche selbst.

21. Wie geht man als Auftragsverarbeiter mit Datenpannen um? [Randnummer 136]

Der Auftragsverarbeiter muss den Verantwortlichen auch bei der Erfüllung der Verpflichtung unterstützen, Datenpannen der Aufsichtsbehörde sowie den betroffenen Personen mitzuteilen. Dazu muss er den Verantwortlichen benachrichtigen, wenn er eine Datenpanne feststellt, die sich auf die Einrichtungen / IT-Systeme des Auftragsverarbeiters oder eines Unterauftragsverarbeiters auswirkt. Außerdem muss er den Verantwortlichen mit den Informationen unterstützen, die in der Meldung an die Aufsichtsbehörde angegeben werden müssen.

Die Meldung des Auftragsverarbeiters an den Verantwortlichen muss unverzüglich nach Bekanntwerden der Datenpanne erfolgen (Artikel 33 Absatz 2). Deshalb empfiehlt der EDSA, einen bestimmten Zeitrahmen für die Meldung zu vereinbaren (z.B. Anzahl der Stunden) und die Kontaktstelle für solche Meldungen in der Auftragsvereinbarung anzugeben.

22. Was geschieht mit den personenbezogenen Daten nach Beendigung des Auftragsverarbeitungsverhältnisses? [Randnummern 139-142]

Die Vertragsbedingungen der AVV sollen sicherstellen, dass die personenbezogenen Daten auch dann noch angemessen geschützt sind, wenn die mit der Verarbeitung verbundenen Dienstleistungen beendet sind. Der Verantwortliche kann zu Beginn im Vertrag festlegen, ob personenbezogene Daten dann gelöscht oder an ihn zurückgegeben werden sollen. Entscheidet er sich für die Löschung der personenbezogenen Daten, sollte der Auftragsverarbeiter sicherstellen, dass die Löschung auf sichere Art und Weise erfolgt, auch um Artikel 32 DS-GVO einzuhalten. Der Auftragsverarbeiter bestätigt dem Verantwortlichen, dass die Löschung abgeschlossen ist. Der Auftragsverarbeiter muss alle vorhandenen Kopien der Daten löschen, es sei denn, dass es gesetzliche Vorgaben zu einer weiteren Speicherung gibt.

23. Darf ein Auftragsverarbeiter andere Parteien als Unterauftragsverarbeiter einsetzen? [Randnummern 128, 129, 154-156]

Ja, Artikel 28 Absatz 2 sieht diese Möglichkeit ausdrücklich vor. Er legt jedoch fest, dass der Auftragsverarbeiter keinen anderen Auftragsverarbeiter ohne vorherige schriftliche Genehmigung des Verantwortlichen beauftragen darf. Bei dieser Genehmigung besteht folgende Wahlmöglichkeit:

- eine spezifische Genehmigung, die sich auf einen bestimmten Unterauftragsverarbeiter für eine bestimmte Verarbeitungstätigkeit zu einem bestimmten Zeitpunkt bezieht, oder
- eine allgemeine Genehmigung.

Die Form sowie mögliche spezifische Kriterien, die der Verantwortliche für die Auswahl der Unterauftragsverarbeiter verlangt, sollten in der AVV festgelegt werden. Außerdem sollte eine Liste der zugelassenen Unterauftragsverarbeiter in die Vereinbarung oder einen Anhang dazu aufgenommen und stets auf dem neuesten Stand gehalten werden.

Beabsichtigt ein Auftragsverarbeiter, einen (zugelassenen) Unterauftragsverarbeiter zu beschäftigen, muss er mit diesem wiederum eine (Unter-)Auftragsverarbeitungsvereinbarung abschließen. Darin

muss er dem Unterauftragsverarbeiter die gleichen Verpflichtungen auferlegen, zu denen er sich als Erstauftragsverarbeiter gegenüber dem Verantwortlichen verpflichtet hat.

24. Kann ein Auftragsverarbeiter für Datenschutzverletzungen haftbar gemacht oder mit einem Bußgeld belegt werden? [Randnummern 74, 138]

Der Auftragsverarbeiter haftet nur bei einem Verstoß gegen Verpflichtungen, die ihm die DS-GVO auferlegt (siehe Frage 18) oder wenn er sich nicht an rechtmäßige Anweisungen des Verantwortlichen hält. Die Pflicht, den Verantwortlichen zu unterstützen, bedeutet gerade keine Verlagerung der Verantwortlichkeit, diese verbleibt beim Verantwortlichen selbst.

Stand: 14.07.2021