

## Kurzpapier Nr. 13

# Auftragsverarbeitung, Art. 28 DS-GVO

*Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.*

### **Begriff des Auftragsverarbeiters**

Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Begriff des Verantwortlichen und in der Folge die maßgebliche Unterscheidung zwischen Verantwortlichem und Auftragsverarbeiter ist in der DS-GVO nicht vollständig deckungsgleich mit dem Wortlaut des BDSG-alt. Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet. Hierbei kommt es maßgeblich auf die Entscheidung über die Verarbeitungszwecke an, während die Entscheidung über die technisch-organisatorischen Fragen der Verarbeitung auch auf den Auftragsverarbeiter delegiert werden kann (vgl. dazu schon WP 169 der Artikel-29-Gruppe, S. 17f. Dieses Arbeitsdokument bezieht sich zwar auf die Rechtslage unter der EU Datenschutzrichtlinie 95/46/EG [DS-RL], die grundsätzlichen Erwägungen zu diesen Fragestellungen sind aber auch für die Auslegung der DS-GVO heranziehbar<sup>1</sup>).

Unter BDSG-alt wurde häufig in Abgrenzung zur Auftrags(daten)verarbeitung die Figur der sog. Funktionsübertragung verwendet. Bei der Funktionsübertragung wurde anstelle einer Auftrags(daten)verarbeitung eine Übermittlung personenbezogener Daten an Dritte im Zuge des Outsourcings solcher „Funktionen“/Aufgaben angenommen, die über eine bloße Datenverarbeitung als sol-

che hinausgehen und bei denen dem Empfänger zumindest gewisse Entscheidungsspielräume zur Aufgabenerfüllung übertragen wurden. Die Figur der Funktionsübertragung ist jedoch in der DS-GVO nicht vorgesehen. Dies ergibt sich aus der Gesamtsystematik, insbesondere aus der speziell geregelten Figur der gemeinsam Verantwortlichen (Art. 26 DS-GVO) sowie aus dem Umstand, dass gewisse Entscheidungsspielräume eines Beauftragten - innerhalb des durch den Verantwortlichen gesteckten Rahmens - bezüglich der Mittel der Verarbeitung hinsichtlich der technisch-organisatorischen Fragen die Auftragsverarbeitung nicht ausschließen (WP 169, S. 17f.).

### **Fortbestehende Sonderregelung für Verarbeitungen von personenbezogenen Daten im Auftrag**

Wie schon bislang besteht auch unter der DS-GVO eine Sonderregelung für Verarbeitungen von personenbezogenen Daten im Auftrag. Allerdings legt die DS-GVO den Auftragsverarbeitern künftig mehr Verantwortung und mehr Pflichten auf.

Nach Art. 29 DS-GVO ist der aufgrund eines Auftrages tätige Dienstleister weisungsgebunden. Er führt daher die Verarbeitung für den Auftraggeber nicht als Dritter i. S. d. Art. 4 Nr. 10 DS-GVO durch. Es besteht vielmehr zwischen dem den Auftrag erteilenden Verantwortlichen und seinem Auftragsverarbeiter ein „Innenverhältnis“. Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet.

<sup>1</sup> [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169\\_de.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf)

Zu beachten ist, dass die Datenverarbeitung im Auftrag auch künftig keine Erlaubnis darstellt, Daten dem Auftragsverarbeiter zu offenbaren, die aufgrund gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, vertraulich zu behandeln sind (vgl. § 1 Abs. 2 S. 3 BDSG-neu).

Mit dem „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ wurden jedoch verschiedene Gesetze zu Berufsgeheimnissen novelliert. So dürfen nunmehr u.a. die in § 203 Abs. 1 oder 2 StGB genannten Berufsgeheimnisträger zum Beispiel externen Dienstleistern, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, Geheimnisse unter den Voraussetzungen des § 203 Abs. 3 und 4 StGB offenbaren. Im Gegenzug unterliegt der Auftragsverarbeiter nach § 203 Abs. 4 StGB nunmehr ebenfalls einer auch strafrechtlich sanktionierten Verschwiegenheitspflicht.

Für die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter bedarf es regelmäßig keiner weiteren Rechtsgrundlage im Sinne von Art. 6 bis 10 DS-GVO als derjenigen, auf die der Verantwortliche selbst die Verarbeitung stützt.

Möglich ist nach der DS-GVO auch eine Auftragsverarbeitung durch Dienstleister außerhalb des EU-/EWR-Raums, wenn die zusätzlichen Anforderungen der Art. 44 ff. DS-GVO für Verarbeitungen in Drittstaaten eingehalten werden (angemessenes Schutzniveau im Drittstaat, geeignete Garantien nach Art. 46 DS-GVO wie z.B. Standarddatenschutzklauseln, oder Ausnahmetatbestand nach Art. 49 DS-GVO).

Auftragsverarbeiter sind Empfänger im Sinne von Art. 4 Nr. 9 DS-GVO. Die Eigenschaft als Empfänger führt zu gesonderten Informations- (vgl. u. a. Art. 13 Abs. 1 lit. e DS-GVO) und Mitteilungspflichten (Art. 19 DS-GVO) des Verantwortlichen sowie zu

Auskunftsrechten (Art. 15 DS-GVO) der betroffenen Person gegenüber dem Verantwortlichen. Empfänger von Daten müssen im Verzeichnis von Verarbeitungstätigkeiten (vgl. Art. 30 Abs. 1 lit. d DS-GVO) geführt werden.

## **Regelungen für Auftragsverarbeitung in Art. 28 DS-GVO**

Die zentrale Vorschrift für Auftragsverarbeiter in der DS-GVO ist Art. 28, wonach dem Verantwortlichen gemäß Absatz 1 vor Auftragsvergabe zunächst eine Prüfung der Geeignetheit des Auftragsverarbeiters auferlegt wird. Der Verantwortliche darf sich danach nur solcher Auftragsverarbeiter bedienen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz anwenden, so dass die Verarbeitung im Einklang mit der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Zum Beleg solcher Garantien können auch genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 DS-GVO oder Zertifizierungen nach Art. 42 DS-GVO als Faktoren herangezogen werden.

## **Vertrag mit dem Auftragsverarbeiter**

Wie nach der bisherigen Rechtslage muss der Verantwortliche mit dem Auftragsverarbeiter einen Vertrag über die weisungsgebundene Tätigkeit schließen, der schriftlich oder in einem elektronischen Format abgefasst sein kann. Hierfür können sowohl individuelle Regelungen getroffen, als auch von der EU-Kommission oder von der zuständigen Aufsichtsbehörde verabschiedete Standardvertragsklauseln verwendet werden. Für den notwendigen Inhalt des Vertrags gilt in großen Teilen das Gleiche wie bisher. Die bestehenden Verträge können daher fortgelten, wenn sie den Anforderungen der DS-GVO entsprechen oder darüber hinausgehen. Beispielsweise muss ein Vertrag zur Auftragsverarbeitung eine Regelung zur Bereitstellung der Daten beinhalten und die Einhaltung der besonderen Bedingungen für den Einsatz von Subunternehmern regeln. Unter anderem muss der Vertrag außerdem

vorsehen, dass der Auftragsverarbeiter die gemäß Art. 32 DS-GVO erforderlichen Maßnahmen ergreift. Da der Verantwortliche für die Rechtmäßigkeit der Verarbeitung insgesamt verantwortlich ist und bleibt (s. Art. 24 DS-GVO), ist weiterhin anzuraten, die mindestens erforderlichen technischen und organisatorischen Maßnahmen darzustellen.

### **Subunternehmer-Einsatz**

Will sich der Auftragsverarbeiter zur Erbringung der vereinbarten Dienstleistung Subunternehmen als weiterer Auftragsverarbeiter bedienen, so bedarf dies der vorherigen (schriftlichen oder elektronischen) Genehmigung durch den Verantwortlichen (Art. 28 Abs. 2 DS-GVO). Später beabsichtigte Änderungen bei den eingesetzten Subunternehmen muss der Auftragsverarbeiter dem Auftraggeber als Verantwortlichem vorher mitteilen, wobei es dem Verantwortlichen vorbehalten bleibt, gegen die geplante Einbeziehung eines Subunternehmens Einspruch zu erheben. Kann nach dem Einspruch keine Einigung zwischen dem Verantwortlichen und dem Auftragsverarbeiter erreicht werden, hat der Verantwortliche die Unterbeauftragung per Weisung zu unterbinden oder die Auftragsverarbeitung zu beenden.

Der Vertrag zwischen dem Auftragsverarbeiter und dem Subunternehmer muss die gleichen vertraglichen Verpflichtungen enthalten, die der Auftragnehmer zugunsten des Auftraggebers übernommen hat.

### **Neue Verantwortlichkeiten und Pflichten für Auftragsverarbeiter sind insbesondere:**

Die Gesamtverantwortung für die Datenverarbeitung und Nachweispflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO umfasst auch die Verarbeitung durch den Auftragsverarbeiter. Hiervon kann sich der Verantwortliche nicht durch die Beauftragung eines Auftragsverarbeiters befreien.

Verstößt ein Auftragsverarbeiter gegen die Pflicht zur weisungsgebundenen Verarbeitung, indem er

die Daten des Auftraggebers ordnungswidrig für eigene Zwecke oder Zwecke Dritter verarbeitet, gilt er nach Art. 28 Abs. 10 DS-GVO insoweit selbst als Verantwortlicher – mit allen rechtlichen Folgen, z. B. auch der Pflicht zur Erfüllung der Betroffenenrechte. Neu hinzugekommen sind in Art. 82 DS-GVO auch spezielle Haftungsregelungen für Auftragsverarbeiter bei Datenschutzverletzungen. Demnach drohen nun Auftragsverarbeitern bei Verstößen gegen die in der DS-GVO speziell den Auftragsverarbeitern auferlegten Pflichten Schadensersatzforderungen von betroffenen Personen.

Des Weiteren besteht für Auftragsverarbeiter die neue Pflicht, künftig auch ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO für alle Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen. Das Verzeichnis muss der Aufsichtsbehörde auf Anfrage nach Art. 30 Abs. 4 DS-GVO, z. B. bei Kontrollen, zur Verfügung gestellt werden.

Nach Art. 33 Abs. 2 DS-GVO muss ein Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten nach Bekanntwerden unverzüglich dem Verantwortlichen melden.

### **Wartung und Fernzugriffe**

Ist Gegenstand des Vertrages zwischen Verantwortlichem und Auftragsverarbeiter die IT-Wartung oder Fernwartung (z. B. Fehleranalysen, Support-Arbeiten in Systemen des Auftraggebers) und besteht in diesem Rahmen für den Auftragsverarbeiter die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten, so handelt es sich im Hinblick auf die weite Definition einer Verarbeitung in Art. 4 Nr. 2 DS-GVO (z. B. Auslesen, Abfragen, Verwenden) ebenfalls um eine Form oder Teiltätigkeit einer Auftragsverarbeitung und die Anforderungen des Art. 28 DS-GVO – wie etwa der Abschluss eines Vertrages zur Auftragsverarbeitung – sind umzusetzen. Anders ist dies bei einer rein technischen Wartung der Infrastruktur einer IT durch Dienstleister (z. B. Arbeiten an Stromzufuhr, Kühlung, Hei-

zung), die nicht zu einer Qualifikation des Dienstleisters als Auftragsverarbeiter und einer Anwendung von Art. 28 DS-GVO führen.

### Folgen bei Verstößen

Ebenso sind die umfassenden Vorschriften über Geldbußen in Art. 83 Abs. 4, 5 und 6 DS-GVO zu berücksichtigen (bei Verstößen gegen die Vorgaben des Art. 28 DS-GVO können Geldbußen von bis zu 10.000.000,- Euro oder bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens verhängt werden). Diese Sanktionen können bei Verstößen nicht nur den Verantwortlichen selbst, sondern auch den Auftragsverarbeiter treffen, z. B. bei Verstößen des Auftragsverarbeiters gegen seine Verpflichtungen aus Art. 28 Abs. 2 bis 4 DS-GVO.

### Anhang:

#### Anhang A

Auftragsverarbeitung können regelmäßig z. B. folgende Dienstleistungen sein:

- DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren,
- Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist,
- Werbeadressenverarbeitung in einem Lettershop,
- Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume dort,
- Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten (z. B. Betreuung von Kontaktformularen oder Nutzeranfragen),
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten,
- Auslagerung der Backup-Sicherheitspeicherung und anderer Archivierungen,
- Datenträgerentsorgung durch Dienstleister,

- Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.
- Zentralisierung bestimmter „Shared Services-Dienstleistungen“ innerhalb eines Konzerns, wie Dienstreisen-Planungen oder Reisekostenabrechnungen (jedenfalls sofern kein Fall gemeinsamer Verantwortlichkeit nach Art. 26 DS-GVO vorliegt)

#### Anhang B

Keine Auftragsverarbeitung, sondern die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss, sind beispielsweise in der Regel die Einbeziehung eines

- Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer),
- Inkassobüros mit Forderungsübertragung,
- Bankinstituts für den Geldtransfer,
- Postdienstes für den Brieftransport,

und vieles mehr.

#### Anhang C

Keine Auftragsverarbeitung liegt ferner vor, wenn gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO gegeben ist, d.h. wenn mehrere Verantwortliche gemeinsam über die Verarbeitungszwecke und -mittel entscheiden. Hierunter können je nach Gestaltung eine Reihe von Verarbeitungen fallen, die bisweilen unter BDSG-alt als sog. Funktionsübertragung eingestuft wurden, etwa

- klinische Arzneimittelstudien, wenn mehrere Mitwirkende (z. B. Sponsor, Studienzentren/

Ärzte) jeweils in Teilbereichen Entscheidungen über die Verarbeitung treffen,

- gemeinsame Verwaltung bestimmter Datenkategorien (z.B. „Stammdaten“) für bestimmte gleichlaufende Geschäftszwecke mehrerer Konzernunternehmen.