

# **Datenschutz**

**Prüfung des Vertrages über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 und 29 DS-GVO für die Deutsche Software Engineering & Research GmbH, 02826 Görlitz**

6. Mai 2018

## Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO

Seitens Herrn Johann Horch wurden per E-Mail vom 03.05.2018 Vertragsunterlagen, im Rahmen der Verarbeitung personenbezogener Daten im Auftrag für Mandanten zur Prüfung vorgelegt.

Diese Unterlagen umfassen:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag
- Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP - Vertrag

Gemäß Art. 28 Abs. 1 DS-GVO ist der Auftragsverarbeiter, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, sorgfältig auszuwählen. Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Nach Art. 28 Abs. 3 Satz 1 DS-GVO erfolgt die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Der Vertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten muss, um den Anforderungen des Art. 28 Abs. 3 Satz 1 und 2 DS-GVO zu genügen, Festlegungen zu insbesondere folgenden Themen beinhalten:

### 1. Sind Gegenstand und Dauer des Auftrages nach Art. 28 Abs. 3 Satz 1 DS-GVO geregelt?

*Verständliche Bezeichnung des Vertrags oder des anderen Rechtsinstruments, aus dem der Umfang der Arbeiten, die vom Auftragsverarbeiter zu erledigen sind, und die Laufzeit, hervorgehen.*

Gibt es eine Regelung zum Gegenstand des Vertrages? (Art. 28 Abs. 3 Satz 1 DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. Präambel, § 1 Gegenstand und Dauer des Auftrags, Verweis auf „ASP Vertrag“
- Die Regelungen entsprechen den gesetzlichen Vorgaben.

Sind Beginn und Ende des Auftrages im Vertrag geregelt? (Art. 28 Abs. 3 Satz 1 DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 1 Gegenstand und Dauer des Auftrags, Verweis auf „ASP Vertrag“
- Die Regelungen entsprechen den gesetzlichen Vorgaben.

### 2. Sind Umfang, Art und Zweck der Datenverarbeitung nach Art. 28 Abs. 3 DS-GVO im Auftrag geregelt?

*Der Vertrag bzw. das andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter nach Art. 28 Abs. 3 Satz 2 lit. a DS-GVO die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbei-*

## Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO

tet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Möglichkeiten, insbesondere aber auch die Grenzen der Datenverarbeitung durch den Auftragsverarbeiter müssen den Regelungen entnommen werden können.

Umfang, Art und Zweck der Verarbeitung der Daten, die Art der personenbezogenen Daten (namentliche Nennung der betreffenden Datenarten sinnvoll), die Kategorien betroffener Personen (so konkret wie möglich) und die Pflichten und Rechte des Verantwortlichen sind nach Art. 28 Abs. 3 Satz 1 DS-GVO festzulegen.

Gibt es konkrete dokumentierte Weisungen des Verantwortlichen, welche Verarbeitungen vom Auftragsverarbeiter vorzunehmen sind? (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 2 Umfang der Weisungsbefugnisse des Verantwortlichen gegenüber dem Auftragsverarbeiter, § 3 Übersicht über Art und Zweck der vom Auftragsverarbeiter verarbeiteten Daten, Art der personenbezogenen Daten und Kategorien der betroffenen Personen gemäß der im Vertrag festgelegten Leistungsbeschreibung

Die Regelungen entsprechen den gesetzlichen Vorgaben.

Falls ja, gibt es eine Hinweispflicht des Auftragsverarbeiters an den Verantwortlichen auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation? (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 8 Pflichten des Auftragsverarbeiters Ziffer 3

Die Regelungen entsprechen den gesetzlichen Vorgaben.

Ist der Verwendungszweck im Vertrag oder in einem anderen Rechtsinstrument geregelt? (Art. 28 Abs. 3 Satz 1 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 3 Übersicht über Art und Zweck der vom Auftragsverarbeiter verarbeiteten Daten, Art der personenbezogenen Daten und Kategorien der betroffenen Personen gemäß der im Vertrag festgelegten Leistungsbeschreibung

Die Regelungen entsprechen den gesetzlichen Vorgaben.

Sind die Datenarten im Vertrag oder in einem anderen Rechtsinstrument festgehalten oder bestimmt bzw. bestimmbar? (Art. 28 Abs. 3 Satz 1 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 3 Übersicht über Art und Zweck der vom Auftragsverarbeiter verarbeiteten Daten, Art der personenbezogenen Daten und Kategorien der betroffenen Personen gemäß der im Vertrag festgelegten Leistungsbeschreibung Ziffer 4

Die Regelungen entsprechen den gesetzlichen Vorgaben.

Ist der Kreis der Betroffenen dem Vertrag oder einem anderen Rechtsinstrument zu entnehmen? (Art. 28 Abs. 3 Satz 1 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 3 Übersicht über Art und Zweck der vom Auftragsverarbeiter verarbeiteten Daten, Art der personenbezogenen Daten und Kategorien der betroffenen Personen gemäß der im Vertrag festgelegten Leistungsbeschreibung Ziffer 4

## Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO

Die Regelungen entsprechen den gesetzlichen Vorgaben.

Gehen aus dem Vertrag oder dem anderen Rechtsinstrument die Pflichten und Rechte des Verantwortlichen hervor? (Art. 28 Abs. 3 Satz 1 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 2 Umfang der Weisungsbefugnisse des Verantwortlichen gegenüber dem Auftragsverarbeiter, § 8 Pflichten des Auftragsverarbeiters, § 11 Kontrollrechte des Verantwortlichen; Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters, § 12 Informationspflichten des Auftragsverarbeiters

Die Regelungen entsprechen den gesetzlichen Vorgaben.

### 3. Sind die nach Art. 28 Abs. 3 Satz 2 lit. c i.V.m. Art. 32 DS-GVO (Sicherheit der Verarbeitung) zu treffenden technischen und organisatorischen Maßnahmen festgelegt?

*Im Zuge der EU DS-GVO ist grundsätzlich eine stärker am Einzelfall orientierte Maßnahmenfestlegung üblich. In der Regel werden die Vorschläge regelmäßig vom Auftragsverarbeiter eingereicht, der als unmittelbar Ausführer sachnäher ist, jedoch vom Verantwortlichen geprüft und durch eigene Vorstellungen ergänzt wird. Die in Art. 32 DS-GVO aufgeführten Maßnahmen sind nicht abschließend. Eine schlichte Wiedergabe von Art. 32 DS-GVO ist nicht hinreichend. Vielmehr muss der Maßnahmenkatalog individuell festgelegt und gegebenenfalls angepasst werden.*

*Nach Art. 28 Abs. 3 Satz 2 lit. c DS-GVO sieht der Vertrag bzw. das andere Rechtsinstrument insbesondere vor, dass der Auftragsverarbeiter alle gemäß Art. 32 erforderlichen Maßnahmen ergreift. Art. 32 DS-GVO betrifft die Sicherheit der Verarbeitung. Gemäß Art. 32 Abs. 1 DS-GVO treffen der Verantwortliche und der Auftragsverarbeiter, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:*

Gibt es Regelungen zur Zutrittskontrolle? (Art. 32 Abs. 1 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
- Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 2 Weitere getroffene technische und organisatorische Sicherheitsmaßnahmen soweit nicht unter § 1 genannt

Die Regelung ist ausreichend dargestellt.

Gibt es Regelungen zur Zugangskontrolle? (Art. 32 Abs. 2 DS-GVO)

*Bei der Beurteilung des angemessenen Schutzniveaus sind nach Art. 32 Abs. 2 DS-GVO insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.*

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
- Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 1 Getroffene technische und organisatorische Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus

Die Regelung ist ausreichend dargestellt.

Gibt es Regelungen zur Zugriffskontrolle? (Art. 32 Abs. 1 DS-GVO)

## Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl.§ 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
  - Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 1 Getroffene technische und organisatorische Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus
- Die Regelung ist ausreichend dargestellt.

### Gibt es Regelungen zur Weitergabekontrolle? (Art. 32 Abs. 1 lit. a DS-GVO)

*Maßnahmen nach Art. 32 Abs. 1 lit. a DS-GVO, wie Pseudonymisierung und Verschlüsselung personenbezogener Daten*

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl.§ 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
  - Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 2 Weitere getroffene technische und organisatorische Sicherheitsmaßnahmen soweit nicht unter § 1 genannt
- Die Regelung ist ausreichend dargestellt.

### Gibt es Regelungen zur Eingabekontrolle? (Art. 32 Abs. 1 DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl.§ 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
  - Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 2 Weitere getroffene technische und organisatorische Sicherheitsmaßnahmen soweit nicht unter § 1 genannt
- Die Regelung ist ausreichend dargestellt.

### Gibt es Regelungen zur Auftragskontrolle? (Art. 32 Abs. 1 DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl.§ 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
  - Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag
- Die Regelung ist ausreichend dargestellt.

### Gibt es Regelungen zur Verfügbarkeitskontrolle?

*Maßnahmen nach Art. 32 Abs. 1 lit. b DS-GVO, welche die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.*

*Maßnahmen nach Art. 32 Abs. 1 lit. c DS-GVO, um die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.*

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl.§ 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
  - Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 1 Getroffene technische und organisatorische Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus, § 2 Weitere getroffene technische und organisatorische Sicherheitsmaßnahmen soweit nicht unter § 1 genannt

## Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO

---

Die Regelung ist ausreichend dargestellt.

Gibt es Regelungen zum Trennungsgebot (bzw. Zweckbindung)? (Art. 32 Abs. 1 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
- Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 2 Weitere getroffene technische und organisatorische Sicherheitsmaßnahmen soweit nicht unter § 1 genannt

Die Regelung ist ausreichend dargestellt.

Gibt es Regelungen bzw. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung? (Art. 32 Abs. 1 lit. d DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
- Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 1 Getroffene technische und organisatorische Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus

Die Regelung ist ausreichend dargestellt.

Liegen i. S. d. Art. 32 Abs.3 DS-GVO u.a. Nachweise für die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder ein genehmigtes Zertifizierungsverfahren gemäß Art. 42 DS-GVO vor, um der Erfüllung der in Art. 32 Abs.1 DS-GVO genannten Anforderungen gerecht zu werden?

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
- Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 1 Getroffene technische und organisatorische Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus

Die Regelung ist ausreichend dargestellt.

Gibt es eine Regelung zur Sicherstellung, dass die dem Verantwortlichen und dem Auftragsverarbeiter unterstellte natürliche Personen, die Zugang zu den personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet? (Art. 32 Abs.4 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 4 Nach Artikel 32 DSGVO zu treffende technische und organisatorische Maßnahmen
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 2 Umfang der Weisungsbefugnisse des Verantwortlichen gegenüber dem Auftragsverarbeiter

Die Regelung ist ausreichend dargestellt.

## Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO

---

### 4. Sind Regelungen zur Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten im Auftrag enthalten?

Regelungen zur Berichtigung, Löschung und Sperrung von Daten bemessen sich nach Art. 28 Abs. 3 Satz 2 lit. e i. V. m. Art. 16 ff. DS-GVO. Nach Art. 28 Abs. 3 Satz 2 lit. e DS-GVO sieht der Vertrag bzw. das andere Rechtsinstrument insbesondere vor, dass der Auftragsverarbeiter angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Art. 16 ff. DS-GVO genannten Rechte der betroffenen Person nachzukommen.

Gibt es eine Regelung zur unverzüglichen Berichtigung von Daten – auch mittels einer ergänzenden Erklärung? (Art. 28 Abs. 3 Satz 2 lit. e i. V. m. Art. 16 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 14 Rückgabe überlassener Auftragsmaterialien; Berichtigung, Löschung und Einschränkung von Daten durch den Auftragsverarbeiter

Die Regelung ist ausreichend dargestellt.

Gibt es eine Regelung zur unverzüglichen Löschung („Recht auf Vergessenwerden“) von Daten, sofern einer der in Art. 17 Abs. 1 lit. a-f DS-GVO genannten Gründe zutrifft? (Art. 28 Abs. 3 Satz 2 lit. e i. V. m. Art. 17 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 14 Rückgabe überlassener Auftragsmaterialien; Berichtigung, Löschung und Einschränkung von Daten durch den Auftragsverarbeiter

Die Regelung ist ausreichend dargestellt.

Falls ja, gibt es eine Regelung, dass der Verantwortliche unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, trifft, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat? (Art. 28 Abs. 3 Satz 2 lit. e i. V. m. Art. 17 Abs. 2 DS-GVO)

Nein

- Keine Relevanz

Ja. Die Regelung ist im Vertrag zu finden unter:

- [Quellenangabe]

Die Regelung ist ausreichend dargestellt.

Gibt es eine Regelung zur Einschränkung der Verarbeitung, sofern eine der in Art. 18 Abs. 1 lit. a-d DS-GVO benannten Voraussetzungen gegeben ist? (Art. 28 Abs. 3 Satz 2 lit. e i. V. m. Art. 18 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 14 Rückgabe überlassener Auftragsmaterialien; Berichtigung, Löschung und Einschränkung von Daten durch den Auftragsverarbeiter

Die Regelung ist ausreichend dargestellt.

Gibt es eine Regelung die vorgibt, dass der Verantwortliche die betroffene Person, die eine Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 DS-GVO erwirkt hat unterrichtet, bevor die Einschränkung aufgehoben wird? (Art. 28 Abs. 3 Satz 2 lit. e i. V. m. Art. 18 DS-GVO)

## Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 12 Informationspflichten des Auftragsverarbeiters Ziffer 2
- Die Regelung ist ausreichend dargestellt.

Gibt es eine Regelung gem. Art. 19 DS-GVO Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung im Verhältnis Verantwortlicher und alle Empfänger, denen personenbezogene Daten offengelegt wurden, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden? (Art. 28 Abs. 3 Satz 2 lit. e i. V. m. Art. 19 DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 14 Rückgabe überlassener Auftragsmaterialien; Berichtigung, Löschung und Einschränkung von Daten durch den Auftragsverarbeiter
- Die Regelung ist ausreichend dargestellt.

### 5. Sind Regelungen zu den Pflichten nach Art. 28 Abs. 3 Satz 2 lit. b sowie Art. 37 Abs. 4 DS-GVO im Vertrag oder einem anderen Rechtsinstrument beinhaltet?

*Im Vertrag oder einem anderen Rechtsinstrument sind bestimmte Anforderungen, z. B. zum Datengeheimnis, zur Bestellung eines Datenschutzbeauftragten etc. zu regeln.*

Gibt es eine Regelung zur Verpflichtung der zur Verarbeitung der personenbezogenen Daten befugten Personen des Auftragsverarbeiters, zur Vertraulichkeit oder einer angemessenen gesetzlichen Verschwiegenheitspflicht? (Art. 28 Abs. 3 Satz 2 lit. b DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 7 Datengeheimnis / Bankgeheimnis / Fernmeldegeheimnis
- Die Regelung ist ausreichend dargestellt.

Gibt es eine Regelung zur Bestellung eines betrieblichen Datenschutzbeauftragten beim Verantwortlichen oder beim Auftragsverarbeiter oder bei Verbänden und anderen Vereinigungen? (Art. 37 Abs. 4 DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 9 Datenschutzbeauftragter des Auftragsverarbeiters
  - Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag, vgl. § 2 Weitere getroffene technische und organisatorische Sicherheitsmaßnahmen soweit nicht unter § 1 genannt → § 3 Datenschutzbeauftragter bzw. für die Einhaltung von Datenschutzvorschriften verantwortliche Person
- Die Regelung ist ausreichend dargestellt.

### 6. Sind Regelungen zu Unterauftragsverhältnissen nach Art. 28 Abs. 3 Satz 2 lit. d i. V. m. Art. 28 Abs. 2 und 4 DS-GVO im Vertrag oder einem anderen Rechtsinstrument enthalten?

*Das Ob und Wie einer Beauftragung von Unterauftragnehmern durch den Auftragsverarbeiter, bei der Verarbeitung von Daten für den Verantwortlichen, ist konkret zu regeln. Nach Art. 28 Abs. 2 DS-GVO nimmt der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen.*



## Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO

chen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Nach Art. 28 Abs. 4 DS-GVO: [...] Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

Gibt es eine Regelung zur Zulässigkeit von Unterauftragsverhältnissen? (Art. 28 Abs. 3 Satz 2 lit. d i. V. m. Art. 28 Abs. 2 und 4 DS-GVO)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 5 Zulässigkeit der Begründung von Unterauftragsverhältnissen (weitere Auftragsverarbeiter) und Bedingungen für deren Einsatz, § 7 Datengeheimnis / Bankgeheimnis / Fernmeldegeheimnis, § 12 Informationspflichten des Auftragsverarbeiters
- Anlage D 2 Datensicherheit (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO) zum ASP – Vertrag

Die Regelung ist ausreichend dargestellt.

Falls ja, gibt es eine Regelung dazu, wie der Unterauftragnehmer zu beauftragen ist?

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 5 Zulässigkeit der Begründung von Unterauftragsverhältnissen (weitere Auftragsverarbeiter) und Bedingungen für deren Einsatz

Die Regelung ist ausreichend dargestellt.

### 7. Gibt es Regelungen zu Kontrollrechten des Verantwortlichen und entsprechenden Duldungspflichten des Auftragsverarbeiters nach Art. 28 Abs. 3 Satz 1 lit. h DS-GVO?

Um eine wirksame Kontrolle vornehmen zu können, müssen die Kontrollrechte des Verantwortlichen vertraglich vereinbart werden. Damit einhergehen entsprechende Duldungspflichten des Auftragsverarbeiters. Nach Art. 28 Abs. 3 Satz 1 lit. h DS-GVO sind dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen.

Gibt es eine Regelung zur Nachweispflicht gegenüber dem Verantwortlichen im Hinblick auf die Einhaltung der Anforderungen aus Art. 28 Abs. 3 Satz 1 lit. h DS-GVO?

(z.B. Kontrolle vor Ort, Herausgabe von Informationen etc.)

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 8 Pflichten des Auftragsverarbeiters

Die Regelung ist ausreichend dargestellt.

Sind damit einhergehende Duldungspflichten des Auftragsverarbeiters geregelt?

Nein

Ja. Die Regelung ist im Vertrag zu finden unter:

- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 11 Kontrollrechte des Verantwortlichen; Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters

Die Regelung ist ausreichend dargestellt.

## Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO

### 8. Gibt es Regelungen zu Meldepflichten des Auftragsverarbeiters bei Verletzungen des Schutzes personenbezogener Daten gegenüber dem Verantwortlichen nach Art. 28 Abs. 3 Satz 1 lit. f DS-GVO i. V. m. Art. 32-36 DS-GVO?

*Insbesondere damit der Auftragsverarbeiter seinen etwaigen Pflichten nach Art. 33 Abs. 2 DS-GVO nachkommen kann, müssen entsprechende Meldepflichten des Auftragsverarbeiter bei Unregelmäßigkeiten bzw. Verstößen gegen Rechtsvorschriften oder vertragliche Pflichten gegenüber dem Verantwortlichen geregelt sein. Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.*

Gibt es eine Regelung, aus der sich die Pflicht des Auftragsverarbeiters ergibt, Verletzung des Schutzes personenbezogener Daten dem Verantwortlichen unverzüglich zu melden? (Art. 28 Abs. 3 Satz 1 lit. f DS-GVO i. V. m. Art. 32-36 DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, § 12 Informationspflichten des Auftragsverarbeiters
- Die Regelung ist ausreichend dargestellt.

### 9. Ist das ausschließliche Weisungsrecht des Verantwortlichen nach Art. 29 DS-GVO im Vertrag oder einem anderen Rechtsinstrument geregelt?

*Nach Art. 29 DS-GVO dürfen der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.*

Gibt es eine Regelung, aus der sich die Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters ergibt? (Art. 29 DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 2 Umfang der Weisungsbefugnisse des Verantwortlichen gegenüber dem Auftragsverarbeiter
- Die Regelung ist ausreichend dargestellt.

### 10. Gibt es gemäß Art. 28 Abs. 3 Satz 2 lit. g DS-GVO Regelungen zur Rückgabe bzw. Löschung von Daten nach Auftragsbeendigung?

*Es muss gewährleistet sein, dass nach Beendigung des Auftrags keine personenbezogenen Daten mehr beim Auftragsverarbeiter verbleiben, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Hierzu bedarf es entsprechender Regelungen, die sich nach Art. 28 Abs. 3 Satz 2 lit. g DS-GVO bemessen, wonach der Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.*

Gibt es eine Regelung, aus der sich die Pflicht des Auftragnehmers ergibt, überlassene Datenträger zurückzugeben bzw. für den Auftraggeber gespeicherte Daten zu löschen? (Art. 28 Abs. 3 Satz 2 lit. g DS-GVO)

- Nein
- Ja. Die Regelung ist im Vertrag zu finden unter:
- Vertrag Anlage D 1 Datenschutzvertrag (Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO) zum laufenden ASP Vertrag, vgl. § 14 Rückgabe überlassener Auftragsmaterialien; Berichtigung, Löschung und Einschränkung von Daten durch den Auftragsverarbeiter
- Die Regelung ist ausreichend dargestellt.

### 11. Sonstiges / Ergebnis

Es ergeben sich keine Anmerkungen.

## **Vertragsprüfung Auftragsverarbeitung im Sinne des Art. 28 und 29 DS-GVO**

---

Sämtliche Angaben sind in hinreichender Form dokumentiert.  
Der Vertrag weist, unserer Einschätzung nach, die für eine Verarbeitung im Auftrag erforderlichen und wesentlichen Punkte nach Artikel 28 und 29 DS-GVO auf.

06.05.2018

Aysegül Kalkan (LL.M.)  
Betrieblicher Datenschutzbeauftragter  
der Deutsche Software Engineering & Research GmbH