

Anlage 7 Vereinbarung zur Auftragsverarbeitung

Inhalt

1	Gegenstand der Verarbeitung	2
2	Dauer der Verarbeitung	2
3	Art und Zweck der Verarbeitung	2
4	Art der personenbezogenen Daten (Datenkategorien)	2
5	Kategorien betroffener Personen	2
6	Ort der Leistungserbringung	2
6.1	Datenübermittlung in ein Drittland oder an internationale Organisationen	2
7	Weisungsgebundenheit des Auftragnehmers	2
8	Weisungsbefugnis des Auftraggebers	3
9	Wahrung der Vertraulichkeit	3
10	Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	3
11	Genehmigte Verhaltensregeln, Zertifizierung	4
12	Unterstützung des Auftraggebers bezüglich seiner Pflichten gegenüber betroffenen Personen durch den Auftragnehmer	4
13	Unterstützung des Auftraggebers bei der Einhaltung der Pflichten gemäß den Artikeln 32 bis 36 DS-GVO durch den Auftragnehmer	5
14	Behandlung der personenbezogenen Daten bei Vertragsende	5
15	Nachweis der Einhaltung der vereinbarten Pflichten	5
16	Kontrollrechte des Auftraggebers	6
17	Weitere Auftragsverhältnisse	6
18	Ansprechpartner des Auftragnehmers	8
19	Zusammenarbeit mit der und Kontrollen durch die Aufsichtsbehörde	8
20	Haftung und Schadensersatz	8
21	Informationspflichten, Schriftformklausel, Rechtswahl	8
22	Aussetzen und Beendigung der Leistungsvereinbarung	9

1 Gegenstand der Verarbeitung

Der Gegenstand der Verarbeitung ergibt sich aus dem/der dieser Vereinbarung zugrunde liegenden Leistungsvereinbarung (im Folgenden „Leistungsvereinbarung“).

2 Dauer der Verarbeitung

Die Dauer der Verarbeitung entspricht der Laufzeit der Leistungsvereinbarung.

Unbeschadet der vorstehenden Regelungen unter Pkt. 2 gilt die Vereinbarung solange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet, einschließlich Backups.

3 Art und Zweck der Verarbeitung

Für alle mit §1 (Vertragsgegenstand) der zusätzlichen Vertragsbedingungen in Verbindung stehenden Tätigkeiten.

4 Art der personenbezogenen Daten (Datenkategorien)

Die Datenkategorien sind in der Leistungsvereinbarung konkret beschrieben unter:

Kundenstammdaten (Namen, Vornamen, Adressen, Telefonnummern, E-Mail-Adressen)

5 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Kunden des Auftraggebers

6 Ort der Leistungserbringung

Die vereinbarten Leistungen werden ausschließlich von in der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum ansässigen Unternehmen im Geltungsbereich der DS-GVO erbracht.

6.1 Datenübermittlung in ein Drittland oder an internationale Organisationen

Soweit der Auftraggeber eine Datenübermittlung in ein Drittland oder an eine internationale Organisation anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

Jede Übermittlung personenbezogener Daten durch den Auftragnehmer in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers oder einer gesetzlichen Verpflichtung, der der Auftragnehmer unterliegt. Dies betrifft auch Übermittlungen an genehmigte Unterauftragnehmer nach Ziff. 17 dieser Vereinbarung. Beauftragungen zu Datenübermittlungen im Rahmen weiterer Auftragsverhältnisse können innerhalb des dieser Vereinbarung zugrundeliegenden Vertrags erfolgen.

7 Weisungsgebundenheit des Auftragnehmers

Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu den personenbezogenen Daten hat, darf Daten des Auftraggebers nur im Rahmen der Leistungsvereinbarung und der Weisungen des Auftraggebers verarbeiten, es sei denn, er ist durch Unions- oder nationales Recht, dem er unterliegt, zur Verarbeitung verpflichtet. Der Auftragnehmer teilt dem Auftraggeber vor der Verarbeitung unaufgefordert diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Jedwede Verwertung für andere Zwecke sowie eigene Zwecke des Auftragnehmers, insbesondere das Scannen, Speichern, Kopieren, Ausdrucken und Vervielfältigen, ist nicht gestattet. Der Auftragnehmer gewährleistet, dass die Daten des Auftraggebers nicht an unberechtigte Dritte weitergegeben oder sonst verwertet werden.

8 Weisungsbefugnis des Auftraggebers

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nur auf der Basis dokumentierter Weisungen des Auftraggebers verarbeiten.

Die in der Leistungsvereinbarung enthaltenen Weisungen können vom Auftraggeber in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Beziehen sich die Weisungen auf Leistungen, die in der Leistungsvereinbarung nicht vorgesehen sind, werden sie als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder andere Datenschutzbestimmungen verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

9 Wahrung der Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die mit den Bestimmungen zum Datenschutz vertraut gemacht und auf die Verschwiegenheit verpflichtet wurden, oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

Der Auftragnehmer gewährt seinen Beschäftigten nur insoweit Zugriff auf die Daten des Auftraggebers, wie dies für die Durchführung, Verwaltung und Überwachung der vereinbarten Tätigkeiten unbedingt erforderlich ist.

Stellt einer der Vertragspartner Verletzungen des Schutzes von Daten fest, die von der Leistungsvereinbarung betroffen sind, informiert der Feststellende unverzüglich den jeweils anderen Vertragspartner und leitet erste Maßnahmen zur Gefahrenabwendung ein. Auftraggeber und Auftragnehmer ermitteln anschließend den Umfang des Schadens und treffen unverzüglich alle erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

Der Auftragnehmer dokumentiert von ihm zu verantwortende Verletzungen des Schutzes personenbezogener Daten und stellt die Dokumentation dem Auftraggeber zur Verfügung.

10 Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Der Auftragnehmer hat in seinem Verantwortungsbereich unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der entsprechend der Leistungsvereinbarung durchzuführenden Datenverarbeitung technische und organisatorische Maßnahmen getroffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Diese Maßnahmen umfassen den Schutz der Daten vor einer Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führen kann. Bei der Festlegung der Maßnahmen hat der Auftragnehmer insbesondere die Eintrittswahrscheinlichkeit eines schädigenden Ereignisses und die Schwere des Risikos für die Rechte und

Freiheiten der betroffenen Personen berücksichtigt. Außerdem hat der Auftragnehmer angemessene Maßnahmen getroffen, um bei einem Zwischenfall die Verfügbarkeit der und den Zugang zu den Daten schnellstmöglich wieder herzustellen.

Sofern die Verarbeitung besondere Kategorien personenbezogener Daten nach Art. 9 oder Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO betrifft, vereinbaren Auftraggeber und Auftragnehmer spezielle Beschränkungen und/oder zusätzlichen Garantien, die anzuwenden sind.

Die konkreten technischen und organisatorischen Maßnahmen sind im Anhang 1 dieser Vereinbarung beschrieben.

Der Auftraggeber trägt die Verantwortung dafür, dass die vereinbarten Maßnahmen ein für die Risiken der zu verarbeitenden Daten angemessenes Schutzniveau bieten.

Der Auftragnehmer prüft, bewertet und evaluiert regelmäßig die internen Prozesse sowie die Wirksamkeit der technischen und organisatorischen Maßnahmen. Ihm ist es gestattet, Änderungen aufgrund organisatorischer und technischer Weiterentwicklungen umzusetzen. Dabei darf das Sicherheitsniveau der vereinbarten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind mit dem Auftraggeber abzustimmen und im Anhang 1 zu dokumentieren.

Soweit eine Prüfung oder ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

11 Genehmigte Verhaltensregeln, Zertifizierung

Zum Nachweis, dass der Auftragnehmer seinen Pflichten nach DS-GVO nachkommt, wird darauf verwiesen, dass:

- ☐ Für den Auftragnehmer die nachfolgend aufgeführten genehmigten Verhaltensregeln nach Art. 40 DS-GVO: [Klicken Sie hier, um Text einzugeben.](#) gelten. Die genehmigten Verhaltensregeln sind veröffentlicht im Verzeichnis der Aufsichtsbehörde [Klicken Sie hier, um Text einzugeben.](#)
- ☐ Der Auftragnehmer nach Art. 42 DS-GVO zertifiziert ist. Die Zertifizierung wurde von [Klicken Sie hier, um Text einzugeben.](#) erteilt und gilt bis zum [Klicken Sie hier, um ein Datum einzugeben.](#)

12 Unterstützung des Auftraggebers bezüglich seiner Pflichten gegenüber betroffenen Personen durch den Auftragnehmer

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen im Zusammenhang mit den Informationspflichten bei der Erhebung sowie den Rechten auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch. Wendet sich eine betroffene Person mit einem diesbezüglichen Ersuchen unmittelbar an den Auftragnehmer, leitet dieser es unverzüglich an den Auftraggeber weiter. Er bearbeitet den Antrag nicht selbst, sofern er vom Verantwortlichen nicht dazu ermächtigt wurde.

Der Auftragnehmer haftet dem Auftraggeber, wenn das Ersuchen der betroffenen Person wegen unzureichender oder verspäteter Weiterleitung vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet werden kann.

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind.

Der Auftragnehmer stellt sicher, dass von der Leistungsvereinbarung betroffene Daten berichtigt oder gelöscht werden können und berichtigt oder löscht Daten entsprechend der Anweisungen des Auftraggebers.

Hat der Auftragnehmer weitere Auftragsverarbeiter hinzugezogen, kommt er eigenständig den Mitteilungspflichten nach Art. 19 DS-GVO nach.

13 Unterstützung des Auftraggebers bei der Einhaltung der Pflichten gemäß den Artikeln 32 bis 36 DS-GVO durch den Auftragnehmer

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen der ihm zur Verfügung stehenden Informationen bei der

- Sicherstellung eines dem Risiko der Verarbeitung angemessenen Schutzniveaus durch geeignete technische und organisatorische Maßnahmen;
- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde;
- Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen
- Durchführung einer notwendigen Datenschutz-Folgenabschätzung
- Konsultation der Aufsichtsbehörde vor der Verarbeitung

14 Behandlung der personenbezogenen Daten bei Vertragsende

Ist in der Leistungsvereinbarung nichts anderes geregelt, hat der Auftragnehmer nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Der Auftraggeber kann vom Auftragnehmer verlangen, die Daten einem den Auftrag übernehmenden Dienstleister zu übermitteln.

Test- und Ausschussmaterial ist ohne gesonderte Beauftragung jeweils unverzüglich zu vernichten.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Ende der Laufzeit der Leistungsvereinbarung hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Ende der Laufzeit der Leistungsvereinbarung dem Auftraggeber übergeben.

15 Nachweis der Einhaltung der vereinbarten Pflichten

Auftraggeber und Auftragnehmer müssen die Einhaltung dieser Vereinbarung nachweisen können. Der Auftragnehmer beantwortet diesbezügliche Anfragen des Auftraggebers unverzüglich und in angemessener Weise und stellt ihm alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in dieser Vereinbarung festgelegten und unmittelbar aus DSGVO und BDSG hervorgehenden Pflichten erforderlich sind. U. A. stellt der Auftragnehmer dem Auftraggeber folgende Informationen zur Verfügung:

- ☐ Ergebnisse eines Selbstaudits
- ☐ unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung

- ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Datenschutzauditoren, Qualitätsauditoren)
- ☐ Zertifikat zu Datenschutz und/oder Informationssicherheit (z. B. ISO 27001, BSI-Grundschutz)
- ☐ genehmigte Verhaltensregeln nach Art. 40 DS-GVO
- ☐ ein Zertifikat nach Art. 42 DS-GVO
- ☐ sonstige Unterlagen oder/und Zertifikate: [Klicken Sie hier, um Text einzugeben.](#)

16 Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer in angemessenen Abständen Kontrollen durchzuführen oder durch einen von ihm beauftragten, unabhängigen Prüfer durchführen zu lassen. Diesem Zweck dienende Inspektionen werden zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber oder der von diesem beauftragte Prüfer von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, zur Prüfung beizutragen und insbesondere dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Dabei kann der Prüfende einschlägige Zertifizierungen des Auftragnehmers berücksichtigen.

Der Auftraggeber und der von ihm beauftragte Prüfer sind hinsichtlich der Daten anderer Kunden und der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Verschwiegenheit verpflichtet.

Der Auftragnehmer kann die Inspektion von der Unterzeichnung einer entsprechenden Verpflichtungserklärung durch den Auftraggeber oder den von diesem beauftragten Prüfer abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Bei begründetem, dokumentiertem Verdacht auf Datenschutzverletzungen hat der Auftraggeber das Recht, unangekündigte Inspektionen durchzuführen.

17 Weitere Auftragsverhältnisse

Weitere Auftragsverhältnisse sind Dienstleistungen, die sich unmittelbar auf die Erbringung der in der Leistungsvereinbarung beschriebenen Aufgabe beziehen. Dazu zählt auch der Support von IT-Systemen, sofern ein unmittelbarer Zugriff auf Daten des Auftraggebers nicht ausgeschlossen werden kann.

Nicht zu den weiteren Auftragsverhältnissen gehören Nebenleistungen, die der Auftragnehmer zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikations-, Post-, Transport-, Reinigung- oder Bewachungsdienstleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen abzuschließen sowie Kontrollmaßnahmen durchzuführen.

Der Auftragnehmer ist nicht berechtigt, weitere Auftragsverarbeiter (Unterauftragnehmer) hinzuzuziehen.

- ☐ Der Auftraggeber stimmt zu, dass der Auftragnehmer zur Durchführung des vereinbarten Auftrages die in der Tabelle angeführten Unterauftragnehmer einsetzt, unter der Bedingung, dass der Auftragnehmer mit diesen eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4

DS-GVO abschließt und sicherstellt, dass der Unterauftragnehmer die Pflichten erfüllt, denen er selbst unterliegt.

Auftragsgegenstand	Auftragsverarbeiter (Firma, Anschrift)

Weitere Unterauftragnehmer dürfen nur dann hinzugezogen werden, wenn der Auftraggeber unter genauer Bezeichnung des Unterauftragnehmers und des Auftragsgegenstandes schriftlich zugestimmt hat. Sie sind dem Vertrag als Anlage anzufügen.

Das Gleiche gilt, wenn der Auftragnehmer einen Unterauftragnehmer durch einen anderen Unterauftragnehmer ersetzen will.

In beiden Fällen informiert der Auftragnehmer den Auftraggeber mindestens 15 Arbeitstage vor der geplanten Veränderung.

Der Auftraggeber darf seine Zustimmung nur aus wichtigen datenschutzrechtlichen Gründen verweigern. Ein wichtiger Grund kann die Verlagerung in ein Drittland ohne ausreichende Datenschutzgarantien sein.

Die Offenlegung (Übermittlung) von Daten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen der Zustimmung des Auftraggebers und nach Abschluss des Vertrags oder anderen Rechtsinstruments nach Art. 28 Abs. 2 bis 4 DSGVO zwischen Auftragnehmer und Unterauftragnehmer gestattet. Der Auftragnehmer kontrolliert regelmäßig die Einhaltung und Umsetzung der technischen und organisatorischen Maßnahmen beim Unterauftragnehmer. Er stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung.

Erbringt der Unterauftragnehmer die vereinbarte Leistung in einem Drittland, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch Vereinbarung von Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus nach Art. 44 ff. DS-GVO sicher (siehe auch Ziff. 6 dieser Vereinbarung).

Der Auftraggeber erklärt sich damit einverstanden, dass in den Fällen, in denen der Auftragnehmer einem Unterauftragnehmer in einem Drittland personenbezogene Daten des Auftraggebers übermittelt, der Auftragnehmer und der Unterauftragnehmer zur Einhaltung von Kapitel V der DSGVO EU-Standardvertragsklauseln verwenden können, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Die Vereinbarung zur Auftragsverarbeitung zwischen Auftragnehmer und Unterauftragnehmer wird dem Auftraggeber auf dessen Verlangen vorgelegt,

Kommt der Unterauftragnehmer seinen Pflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber in vollem Umfang. Der Auftragnehmer benachrichtigt den Auftraggeber, wenn der Unterauftragnehmer seine vertraglichen Pflichten nicht erfüllt.

Die Hinzuziehung weiterer Unterauftragnehmer durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers.

Die vertraglichen und sonstigen Regelungen zwischen den Unterauftragnehmern sind entsprechend dieses Absatzes zu gestalten. Zusätzlich vereinbart der Auftragnehmer mit dem Unterauftragnehmer eine Drittbegünstigtenklausel, wonach der Auftraggeber – im Falle, dass der Auftragnehmer faktisch oder

rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und dem Unterauftragnehmer Anweisungen bezüglich der von ihm verarbeiteten Daten des Auftraggebers, insbesondere zur Löschung oder Rückgabe der Daten, zu erteilen.

18 Ansprechpartner des Auftragnehmers

Der Auftragnehmer benennt als Ansprechpartner zu allen Fragen des Datenschutzes:

Bitte eintragen: Vorname, Name, Organisationseinheit, Stellenbezeichnung, Kontaktdaten.

19 Zusammenarbeit mit der und Kontrollen durch die Aufsichtsbehörde

Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Der Auftragnehmer informiert unverzüglich den Auftraggeber über Kontrollhandlungen, Maßnahmen und Ermittlungen der Aufsichtsbehörde oder einer sonstigen zuständigen Behörde, soweit davon Inhalte der Leistungsvereinbarung betroffen sind.

Der Auftragnehmer unterstützt im Rahmen seiner Möglichkeiten den Auftraggeber, soweit dieser einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung ausgesetzt ist.

20 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der Regelungen des Art. 82 DS-GVO.

21 Informationspflichten, Schriftformklausel, Rechtswahl

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Der Verzicht auf dieses Formerfordernis ist nicht möglich.

Bei etwaigen, den Datenschutz betreffenden, Widersprüchen gehen die Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen der Leistungsvereinbarung vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Es gilt deutsches Recht.

22 Aussetzen und Beendigung der Leistungsvereinbarung

Falls der Auftragnehmer seinen Pflichten nach dieser Vereinbarung nicht nachkommt, kann der Auftraggeber ihn anweisen, die Verarbeitung gemäß Leistungsvereinbarung auszusetzen, bis er diese Vereinbarung einhält oder die Leistungsvereinbarung beendet ist. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn er nicht in der Lage ist, diese Vereinbarung einzuhalten.

Der Auftraggeber ist berechtigt, die Leistungsvereinbarung zu kündigen, soweit sie die Verarbeitung von unter diese Vereinbarung fallenden personenbezogenen Daten betrifft, wenn

- der Auftraggeber die Verarbeitung gemäß erstem Absatz ausgesetzt hat und die Einhaltung dieser Vereinbarung nicht spätestens innerhalb eines Monats nach der Aussetzung wiederhergestellt wird
- der Auftragnehmer in erheblichem Umfang oder fortdauernd gegen diese Vereinbarung verstößt oder seinen gesetzlichen Verpflichtungen nicht nachkommt
- der Auftragnehmer einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde nicht nachkommt., die seine vertraglichen und/oder gesetzlichen Pflichten zum Gegenstand hat

Der Auftragnehmer ist berechtigt, die Leistungsvereinbarung zu kündigen, soweit sie die Verarbeitung von unter diese Vereinbarung fallenden personenbezogenen Daten betrifft, wenn er den Auftraggeber gemäß Ziff. 8 darüber in Kenntnis gesetzt hat, dass seine Anweisungen gegen die DS-GVO oder andere Datenschutzbestimmungen verstoßen und der Auftraggeber auf der Erfüllung seiner Anweisungen besteht.

Anhang technische und organisatorische Maßnahmen

Hinweis: Alle zu treffenden Maßnahmen sind konkret zu bestimmen. Pauschale Aussagen und Wiederholungen der gesetzlichen Vorschriften genügen nicht. Die Reihenfolge der Regelungstatbestände ist am Art. 32 DS-GVO orientiert. Dabei handelt es sich um eine beispielhafte Liste möglicher Maßnahmen. Angeführt und umgesetzt werden müssen nur Maßnahmen, die erforderlich und angemessen sind.

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der entsprechend der Leistungsvereinbarung durchzuführenden Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der von der Verarbeitung betroffenen Personen hat der Auftragsverarbeiter die nachfolgend aufgeführten technischen und organisatorischen Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. Regelungen und Maßnahmen zur Pseudonymisierung und Verschlüsselung (z. B. Festlegung der Notwendigkeit, etwa für Testsysteme und Beschreibung der Umsetzung)
 - Die „Data-in-transit“-Daten bzw. die Übertragung von Daten und die Kommunikationsverbindungen erfolgen nur über eine verschlüsselte Verbindung und sind nach Möglichkeit zu signieren
 - Sind Datenübertragung nicht verschlüsselbar, sind die Datencontainer zu verschlüsseln und zu übertragen
2. Regelungen und Maßnahmen zur Sicherstellung der Vertraulichkeit (z. B. Zutrittsregelungen, Zugangsregelungen, Zugriffsregelungen, Speicherungsregelungen, Übermittlungsregelungen, Löschregeln, Vertragsgestaltung)
 - Es ist der DL/ Lieferanten Zugangs- und Zugriffsstandard einzuhalten.
 - Stand der Technik physische Sicherheit (z.B. angemessene RC-Klassen Türen/ Fenster und Videoüberwachte Zutritte)
 - Es existieren Zugangsregelungen für Wartung und Fernwartung
 - Erstellung und Anwendung eines Berechtigungskonzeptes.
 - Jährliche Berechtigungsprüfung und Beseitigung falscher Berechtigungen.
 - Es sind Stand der Technik Zutrittskontrolle und -steuerung einzuhalten.
 - Es existiert eine Schlüsselregelung und mindestens ein manuelles Schließsystem.
 - Bei elektronischen Schließungen besteht ein Berechtigungskonzept und dessen adäquate Umsetzung.
 - Reinigungs- und Wartungspersonal ist auf Vertraulichkeit (ZVB Vertraulichkeit) verpflichtet. Gesicherte und regelmäßige Schulung der Mitarbeiter in Bezug auf Informationssicherheitsmaßnahmen
 - Lokale Speicherung auf dem Client oder externen lokalen Speichermedien wird ausgeschlossen.
3. Regelungen und Maßnahmen zur Sicherstellung der Integrität (z. B. Protokollierung, Plausibilitätsprüfungen, Zugangsregelungen, Zugriffsregelungen, Übermittlungsregelungen, Revisionsfähigkeit, ggf. Unveränderbarkeit)
 - Protokollierung und Auswertung der Systembenutzung
 - Protokollierung von Dateizugriffen und -löschungen
 - Regelmäßige Auswertung von Protokollen (Logfiles)
 - Sollte Kenntnis erlangt werden, dass Zugangs- und Zugriffsdaten kompromittiert wurden sind, sind diese ohne schuldhaftes Zögern beim AG anzuzeigen.

4. Regelungen und Maßnahmen zur Sicherstellung der Verfügbarkeit (z. B. Kapazitätsplanung, business continuity management, Schutz vor unbefugtem Eindringen)
 - Backup & Recovery-Konzept
 - RAID System / Festplattenspiegelung
 - Überwachung (der Serverräumlichkeiten)
5. Regelungen und Maßnahmen zur Sicherstellung der Belastbarkeit (z. B. Monitoring, Systemdimensionierung, Kapazitätsplanung, Schutz vor unberechtigtem Eindringen, Automatische Systemmeldungen)
 - Schutz des lokalen Netzwerks durch Firewall-Systeme
 - Nutzung von Anti-Viren-Software
6. Regelungen und Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit und des Zugangs zu den Daten bei einem physischen oder technischen Zwischenfall (z. B. USV, Datensicherungen, business continuity management)
 - Notfallplan bei Kompromittierung
 - Notfallplan bei Datenverlust
7. Regelungen und Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen: (z. B. Datenschutz-Management, Incident-Response-Management, PDCA-Zyklus, organisatorische Regelungen)

Management Prozess zum Management von IT-Störungen und Ausfällen

8. Regelungen und Maßnahmen zur Herstellung von Transparenz (z. B. Dokumentationen)
 - differenzierte Festlegung, Kontrolle und ständige Aktualisierung der Zugriffsberechtigungen entsprechend eines Konzeptes
 - Regelmäßige Überprüfung von Berechtigungen
9. Regelungen und Maßnahmen zur Identifizierung und Autorisierung der Nutzer
 - Individuelles, personalisiertes Benutzerkonto für jeden Mitarbeiter
 - Implementierung eines Rollen- und Berechtigungskonzept
 - Authentifikation mit individuellem Passwort
 - Komplexitätsanforderungen an Kennwörter für Nutzer (Mindestlänge: 8 Zeichen, Zeichenmix: Groß-, Kleinbuchstabe, Ziffer, Sonderzeichen, 3 aus 4)
 - Komplexitätsanforderungen an Kennwörter für Administratoren (Mindestlänge: 12 Zeichen, Zeichenmix: Groß-, Kleinbuchstabe, Ziffer, Sonderzeichen, 4 aus 4)
 - Verschlüsselte Speicherung der Kennwörter
 - Automatisierte Kontensperrung nach mehrmaliger Falscheingabe des Passworts
 - Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
 - Prozess zum Rechtewechsel/-entzug bei Abteilungswechsel von Mitarbeitern
 - Prozess zum Rechteentzug bei Austritt von Mitarbeitern
 - Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität
 - Prüfung der Berechtigung bei jeder Anmeldung an der Anwendung
 - Vergabe von Administratorrechten an minimale Anzahl Personen

- Anstreben von Multi-Faktor-Authentifizierungstechnologien
10. Regelungen und Maßnahmen zum Schutz der Daten während der Übermittlung
- Ausschließlich verschlüsselte Übermittlung von Daten (s.o. ggf. und signierte Datenübermittlung)
 - Es sind die von der KWL GmbH angebotenen Lösungen zu verwenden bzw. vorzuziehen.
11. Regelungen und Maßnahmen zum Schutz der Daten während der Speicherung
- Backup & Recovery-Konzept
 - RAID System / Festplattenspiegelung
 - Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)
 - Regelmäßige Tests zur Datenwiederherstellung
 - Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft
12. Regelungen und Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden
- Mindestens mechanisches Schließsystem
 - Einbruchmeldeanlage
 - Brandmeldeanlage
 - Stand der Technik physische Sicherheit (z.B. angemessene RC-Klassen Türen/ Fenster und Videoüberwachte Zutritte)
 - Bei elektronischen Schließungen besteht ein Berechtigungskonzept und dessen adäquate Umsetzung
 - Es sind Stand der Technik Zutrittskontrolle und -steuerung einzuhalten.
13. Regelungen und Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen
- Monitoring und automatische Benachrichtigung bei Systemausfall
 - Monitoring und automatische Benachrichtigung bei kritischem Ereignis
 - Kapazitätsüberwachung technischer Infrastrukturen
 - Protokollierung und Detektierung der Infrastrukturen muss aktiviert und überwacht werden
14. Regelungen und Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration
- Es ist security by default anzustreben
 - Standard Passwörter sind gemäß Passwort-Richtlinie zu ändern.
15. Regelungen und Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit
-
16. Regelungen und Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten
-
17. Regelungen und Maßnahmen zur Gewährleistung der Datenminimierung

Die Daten dürfen nicht vervielfältigt oder zweckentfremdet werden.

18. Regelungen und Maßnahmen zur Gewährleistung der Datenqualität

- Vollständigkeits- und Richtigkeitsprüfung
- Nachvollziehbarkeit der Bearbeitung von Daten durch individuelle Benutzernamen
- Protokollauswertungsregelung und -system

19. Regelungen und Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

-

20. Regelungen und Maßnahmen zur Gewährleistung der Rechenschaftspflicht

-

21. Regelungen und Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Die Daten sind nach Erfüllung des Vertrags zu löschen.

22. Regelungen und Maßnahmen zum Schutz der Daten bei Heim- und mobiler Arbeit

- Mobile Arbeit ist nur über einen geschützten Kanal (VPN) gestattet
- Eine lokale Speicherung der Daten in der mobilen Arbeit ist ausgeschlossen
- Die Einsichtnahme der Daten in der mobilen Arbeit ist auf den Bearbeiter durch entsprechende Maßnahmen einzuschränken

23. Spezifische technische und organisatorische Regelungen und Maßnahmen, die der Auftragnehmer zur Unterstützung des Auftraggebers ergreifen muss

-