**Auftragsverarbeitung nach Art. 28 Datenschutz-Grundverordnung (DSGVO)**[1]

---

## Vereinbarung

zwischen

**Firma 1**

**Straße 1**

**PLZ Ort 1**

– verantwortliche Stelle, nachfolgend „Auftraggeber“ genannt –

und

**Firma 2**

**Straße 2**

**PLZ Ort 2**

– Auftragsdatenverarbeiter, nachfolgend „Auftragnehmer“ genannt –

Auftraggeber und Auftragnehmer jeweils einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet.

---

### 1. Vertragsgegenstand

Im Rahmen der Leistungserbringung nach dem Vertrag vom DATUM (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

### 2. Art und Zweck, Dauer der Auftragsverarbeitung

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nur nach Weisung des Auftraggebers. Der Auftraggeber bleibt gemäß Art. 5 Abs. 2 DSGVO im datenschutzrechtlichen Sinn Verantwortlicher („Herr der Daten“).

2.2 Die Verarbeitung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend den in **Anlage 1** zu diesem Vertrag enthaltenen Festlegungen zu Art und Zweck der Verarbeitung. Sie bezieht sich auf die in **Anlage 1** festgelegte Art der Auftraggeber-Daten und auf die dort bestimmten Kategorien betroffener Personen. Jede davon abweichende oder darüber hinausgehende Verarbeitung von Auftraggeber-Daten ist dem Auftragnehmer untersagt, insbesondere eine Verwendung der Auftraggeber-Daten zu eigenen Zwecken.

2.3 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1–88.

Mitgliedsstaat der Europäischen Union (EU) statt. Jede Verlagerung in ein Land außerhalb der EU („Drittland“) darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2.4 Der Auftragnehmer erwirbt an den Auftraggeber-Daten keine Rechte und ist auf Verlangen des Auftraggebers jederzeit auf erstes Anfordern zur Herausgabe der Auftraggeber-Daten in einer für den Auftraggeber lesbaren und weiter verarbeitbaren Form verpflichtet. Zurückbehaltungsrechte in Bezug auf Auftraggeber-Daten und die dazugehörigen Datenträger sind ausgeschlossen.

**3. Weisungsrechte des Auftraggebers**

3.1 Der Auftragnehmer verwendet die Auftraggeber-Daten ausschließlich in Übereinstimmung mit den in diesem Vertrag enthaltenen Bestimmungen und den sonstigen Weisungen des Auftraggebers. Der Auftraggeber besitzt insoweit gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht über Art, Zweck und Verfahren der Verarbeitung von Auftraggeber-Daten.

3.2 Die Weisungen des Auftraggebers sollen grundsätzlich in Schrift- oder Textform (z.B. E-Mail) erfolgen. Bei Bedarf kann der Auftraggeber Weisungen auch mündlich oder telefonisch erteilen. Mündlich oder telefonisch erteilte Weisungen bedürfen einer Bestätigung durch den Auftraggeber in Schrift- oder Textform (z.B. E-Mail).

3.3 Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich auszuführen. Der Auftraggeber ist berechtigt, dem Auftragnehmer hierfür im Einzelfall eine jeweils angemessene Frist zu setzen, die der Auftragnehmer einzuhalten hat.

3.4 Ist der Auftragnehmer der begründeten Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag, gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber (mindestens 14 Tage vorher) berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen. Bestätigt der Auftraggeber die Weisung, ist der Auftragnehmer verpflichtet, sie zu befolgen.

3.5 Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die Auftraggeber-Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber die entsprechenden rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.6 Sofern gegen den Auftraggeber wegen eines Verstoßes gegen die DSGVO Ansprüche auf Zahlung von Schadenersatz gemäß Art. 82 DSGVO geltend gemacht werden, weil der Auftragnehmer gegen eine vom Auftraggeber erlassene Weisung verstoßen hat, stellt der Auftragnehmer den Auftraggeber auf erstes Anfordern von allen Ansprüchen frei. Der Auftragnehmer übernimmt hierbei auch die Kosten der notwendigen Rechtsverteidigung des Auftraggebers einschließlich sämtlicher Gerichts- und Anwaltskosten. Die Freistellungspflicht gilt auch, soweit eine Weisung rechtswidrig und dies für den Auftragnehmer offensichtlich war oder der Schadenersatzanspruch auf die Verletzung einer speziell den Auftragsverarbeitern auferlegten Pflicht aus der DSGVO gestützt wird.

3.7 Weisungsberechtigte Personen des Auftraggebers sind:

*Herr X, Firma 1, Datenschutzbeauftragter, Telefon 1, E-Mail 1*

Weisungsempfänger beim Auftragnehmer sind:

*Herr Y, Firma 2, Datenschutzbeauftragter, Telefon 2, E-Mail 2*

Bei einem Wechsel oder einer längerfristigen Verhinderung der weisungsberechtigten Person bzw. des Weisungsempfängers ist der jeweils anderen Partei unverzüglich schriftlich oder in Textform (z.B. E-Mail) eine Person mit Kontaktdaten (E-Mail-Adresse und Telefonnummer) zu benennen,

welche diese Funktion übernimmt.

**4. Pflichten des Auftraggebers**

4.1 Der Auftraggeber ist nach außen, also gegenüber Dritten und den Betroffenen, für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

4.2 Der Auftraggeber ist Eigentümer der Auftraggeber-Daten und Inhaber aller etwaigen Rechte, die die Auftraggeber-Daten betreffen.

**5. Pflichten des Auftragnehmers**

5.1 Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Bestimmungen dieses Vertrages und den Weisungen des Auftraggebers gemäß Ziffer 3.1 verarbeitet. Der Auftragnehmer bestätigt, dass ihm und seinen Mitarbeitern, die mit Auftraggeber-Daten umgehen, die Vorschriften der DSGVO und des BDSG und die sonstigen einschlägigen Datenschutzvorschriften bekannt sind.

5.2 Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung der Auftraggeber-Daten in Übereinstimmung mit diesem Vertrag und den Weisungen des Auftraggebers erfolgt und die technischen und organisatorischen Maßnahmen gemäß Ziffer 6 dieses Vertrages eingehalten werden.

5.3 Der Auftragnehmer darf ohne vorherige schriftliche Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

5.4 Sämtliche Datenträger, die vom Auftraggeber stammen oder für den Auftraggeber genutzt werden, werden vom Auftragnehmer besonders gekennzeichnet und unterliegen seiner laufenden Verwaltung.

5.5 Der Auftragnehmer hat den Auftraggeber unverzüglich darüber zu informieren, wenn das Eigentum des Auftraggebers oder seine sonstigen Rechte an den Auftraggeber-Daten beim Auftragnehmer durch Maßnahmen Dritter, z.B. durch Pfändung, Beschlagnahme, Insolvenz oder Vergleichsverfahren, oder durch sonstige Ereignisse gefährdet wird. Ferner wird der Auftragnehmer alle in diesem Zusammenhang Verantwortlichen darüber informieren, dass die Auftraggeber-Daten und die Datenträger, die vom Auftraggeber stammen, im Eigentum des Auftraggebers stehen.

5.6 Ist der Auftraggeber gegenüber einer staatlichen Stelle, einem Betroffenen oder einer anderen Person verpflichtet, Auskünfte über die Auftraggeber-Daten oder deren Verarbeitung zu erteilen, so ist der Auftragnehmer verpflichtet, den Auftraggeber bei der Erteilung solcher Auskünfte auf erstes Anfordern zu unterstützen, insbesondere durch unverzügliches Zurverfügungstellen sämtlicher Informationen und Dokumente über die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten einschließlich den vom Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen gemäß Ziffer 6, über den technischen Ablauf der Verwendung von Auftraggeber-Daten, die Orte, an denen Auftraggeber-Daten verwendet werden, und über die an der Verarbeitung beteiligten Mitarbeiter.

5.7 Der Auftragnehmer hat die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen gemäß Art. 28 Abs. 3 Satz 2 lit. b) DSGVO schriftlich auf die Vertraulichkeit zu verpflichten und sie zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen. Dies ist nicht erforderlich, wenn die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer wird die in dieser Ziffer niedergelegte Verpflichtung schriftlich dokumentieren und sie auf Verlangen des Auftraggebers diesem vorlegen.

5.8 Sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind, ist der Auftragnehmer verpflichtet, einen auf dem Gebiet des Datenschutzrechts und der

Datenschutzpraxis fachkundigen, für die Aufgaben nach Art. 39 DSGVO fähigen und zuverlässigen betrieblichen Datenschutzbeauftragten schriftlich zu bestellen, der seine Tätigkeit gemäß Art. 38, 39 DSGVO und § 38 Abs. 2 BDSG ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mindestens in Textform (z.B. E-Mail) mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Sollte keine Bestellpflicht für einen betrieblichen Datenschutzbeauftragten bestehen, benennt der Auftragnehmer gegenüber dem Auftraggeber mindestens in Textform (z.B. E-Mail) einen Ansprechpartner für datenschutzrechtliche Belange und teilt dem Auftraggeber dessen Kontaktdaten mit. Sollte der Auftragnehmer seinen Sitz außerhalb der EU haben, benennt er gegenüber dem Auftraggeber einen Vertreter nach Art. 27 Abs. 1 DSGVO in der EU und teilt dem Auftraggeber dessen Kontaktdaten mindestens in Textform (z.B. E-Mail) mit.

5.9 Der Auftragnehmer unterliegt der behördlichen Aufsicht nach § 40 BDSG sowie den Bußgeld- und Strafvorschriften in § 42, 43 BDSG sowie in Art. 83 Abs. 4-6 DSGVO nach Maßgabe von § 41 BDSG.

5.10 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der nach **Anlage 2** zu treffenden technischen und organisatorischen Maßnahmen im Rahmen der Kontrollrechte nach Ziffer 8 dieses Vertrages nachzuweisen.

**6. Technische und organisatorische Maßnahmen**

6.1 Der Auftragnehmer garantiert, dass er vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c), Art. 32 DSGVO implementieren und während des Vertrags aufrechterhalten wird. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

6.2 Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer nach vorheriger schriftlicher Zustimmung des Auftraggebers gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 2** festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

6.3 Auf Weisung des Auftraggebers wird der Auftragnehmer darüber hinausgehende wirksame technische und organisatorische Maßnahmen umsetzen, wenn sich die in **Anlage 2** des Vertrages bestimmten Maßnahmen als nicht ausreichend erwiesen haben oder wenn der technische Fortschritt dies erfordert. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß **Anlage 2** nicht mehr ausreichend sind oder der technische Fortschritt weitere Maßnahmen erfordert.

6.4 Auf Verlangen stellt der Auftragnehmer dem Auftraggeber ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsdatenverarbeitung nach diesem Vertrag zur Verfügung.

**7. Mitteilungs- und Unterstützungspflichten bei Datensicherheitsvorfällen**

7.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er oder ein Mitarbeiter bei der Verarbeitung von Auftraggeber-Daten gegen datenschutzrechtliche Vorschriften, gegen Festlegungen aus diesem Vertrag oder gegen eine vom Auftraggeber erteilte Weisung verstoßen

hat, wenn Anhaltspunkte dafür bestehen, dass ein Dritter unrechtmäßig Kenntnis von Auftraggeber-Daten erlangt haben könnte, oder wenn in sonstiger Weise eine Gefährdung für die Integrität oder Vertraulichkeit der Auftraggeber-Daten eingetreten ist („Datensicherheitsvorfall“).

7.2 Die Information über den Datensicherheitsvorfall hat Angaben über den Zeitpunkt und die Art des Vorfalls (einschließlich einer Information, welche und wie Auftraggeber-Daten betroffen sind), das betroffene EDV-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, alle denkbaren nachteiligen Folgen des Datensicherheitsvorfalls sowie die von dem Auftragnehmer daraufhin ergriffenen Maßnahmen zu enthalten.

7.3 Eine erste Information des Auftraggebers hat unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung von dem Datensicherheitsvorfall, zu erfolgen. Eine weitere, detaillierte Unterrichtung des Auftraggebers, die sämtliche Informationen gemäß Ziffer 7.2 enthalten muss, hat innerhalb von sieben Tagen nach Kenntniserlangung von dem Datensicherheitsvorfall zu erfolgen.

7.4 Der Auftragnehmer ist verpflichtet, den Auftraggeber im Falle eines Datensicherheitsvorfalls bei seinen diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen auf erstes Anfordern auf angemessene Weise zu unterstützen.

7.5 Der Auftragnehmer ist verpflichtet, unverzüglich nach Kenntniserlangung von einem Datensicherheitsvorfall eine technische Analyse durchzuführen, diese zu dokumentieren und dem Auftraggeber die Dokumentation auf Verlangen auszuhändigen. Stellt der Auftraggeber hierbei fest, dass die bisherigen, vom Auftragnehmer realisierten technischen und organisatorischen Maßnahmen zum Schutz der Auftraggeber-Daten nicht ausreichend waren, ist der Auftragnehmer verpflichtet, ohne zusätzliche Kosten solche zusätzlichen technischen und organisatorischen Maßnahmen umzusetzen, die nach Ansicht des Auftraggebers erforderlich sind für einen angemessenen Schutz der Auftraggeber-Daten gegen Datensicherheitsvorfälle.

**8. Unterstützung des Auftragnehmers zur Einhaltung der Pflichten des Auftraggebers nach Art. 32 – 36 DSGVO**

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) die Unterstützung des Auftraggebers im Falle einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO,

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht nach Art. 34 DSGVO gegenüber einem Betroffenen zu unterstützen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzungen i. S. d. Art. 35 DSGVO,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde nach Art. 36 DSGVO.

**9. Kontrollrechte des Auftraggebers**

9.1 Der Auftraggeber ist dazu berechtigt, jederzeit die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer einschließlich der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen und die Ordnungsmäßigkeit der Datenverarbeitungsprozesse und -programme des Auftragnehmers zu prüfen, um sich von der Einhaltung der Bestimmungen dieses Vertrags, der vom

Auftraggeber erteilten Weisungen sowie der einschlägigen gesetzlichen Datenschutzbestimmungen zu überzeugen.

9.2 Zur Durchführung von Kontrollen nach Ziffer 9.1 ist der Auftraggeber berechtigt, jederzeit sämtliche Geschäftsräume des Auftragnehmers zu betreten und dort Vor-Ort-Kontrollen durchzuführen. Soweit möglich, wird der Auftraggeber dem Auftragnehmer solche Vor-Ort-Kontrollen rechtzeitig vorher ankündigen. Der Auftragnehmer gewährt dem Auftraggeber sämtliche für die Durchführung der Kontrolle vom Auftragnehmer benötigten Zugangs-, Auskunfts- und Einsichtsrechte. Der Auftragnehmer verpflichtet sich insbesondere, dem Auftraggeber Zugang zu den Datenverarbeitungseinrichtungen, Dateien und anderen Dokumenten zu gewähren, um die Kontrolle und Überprüfung der relevanten Datenverarbeitungseinrichtungen, Dateien und anderer Dokumentationen zu ermöglichen, die mit der Verarbeitung von Auftraggeber-Daten im Zusammenhang stehen. Der Auftragnehmer stellt dem Auftraggeber alle von ihm für die Kontrolle benötigten Informationen zur Verfügung. Der Auftraggeber nimmt hierbei angemessene Rücksicht auf die Betriebsabläufe und berechtigte Geheimhaltungsinteressen des Auftragnehmers.

9.3 Zur Ermöglichung von Kontrollen nach Ziffer 9.1 ist der Auftragnehmer außerdem verpflichtet, dem Auftraggeber unverzüglich sämtliche Zertifikate, Auditberichte und sonstige Ergebnisse von Überprüfungen im Hinblick auf die Verarbeitung von Auftraggeber-Daten ungekürzt vorzulegen.

9.4 Der Auftraggeber ist berechtigt, von dem betrieblichen Datenschutzbeauftragten des Auftragnehmers Auskunft über sämtliche Aspekte der Verarbeitung von Auftraggeber-Daten, einschließlich der getroffenen technischen und organisatorischen Maßnahmen, zu erhalten und insbesondere von dem betrieblichen Datenschutzbeauftragten des Auftragnehmers regelmäßig eine Bestätigung der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu verlangen. Der Auftragnehmer wird unter Beachtung der Weisungsfreiheit des Datenschutzbeauftragten dafür sorgen, dass der betriebliche Datenschutzbeauftragte auf Verlangen des Auftraggebers Auskünfte und Bestätigungen zeitnah erteilt.

9.5 Der Auftraggeber ist berechtigt, die Kontrollhandlungen nach dieser Ziffer 9 selbst oder durch einen zur Geheimhaltung verpflichteten Bevollmächtigten vorzunehmen. Der Auftragnehmer ist verpflichtet, die Kontrollhandlungen eines solchen Bevollmächtigten in derselben Weise zu dulden und zu unterstützen wie Kontrollen durch den Auftraggeber.

9.6 Gemäß den anwendbaren Datenschutzvorschriften unterliegen der Auftraggeber und der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Verlangen des Auftraggebers wird der Auftragnehmer den Auftraggeber im Rahmen von behördlichen Aufsichtsverfahren nach Kräften unterstützen, wenn und soweit die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten Gegenstand des Aufsichtsverfahrens ist. Der Auftragnehmer wird insbesondere auf Verlangen des Auftraggebers ihm selbst oder der Aufsichtsbehörde unmittelbar alle Informationen im Zusammenhang mit diesem Vertrag geben und der Aufsichtsbehörde die Möglichkeit einräumen, Prüfungen in demselben Umfang durchzuführen wie sie die Aufsichtsbehörde beim Auftraggeber durchführen darf. Der Auftragnehmer gewährt der zuständigen Aufsichtsbehörde auch in diesem Rahmen alle erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte. Falls die Aufsichtsbehörde beim Auftragnehmer Kontrollhandlungen, Ermittlungen oder Maßnahmen durchführt, die Auftraggeber-Daten betreffen, hat der Auftragnehmer den Auftraggeber darüber so früh wie möglich und in der Regel unverzüglich nach Erhalt der Ankündigung der Aufsichtsmaßnahme durch die Behörde zu informieren.

**10. Unterauftragsverhältnisse**

10.1 Der Auftragnehmer darf Unterauftragsverhältnisse (Unterauftragnehmer) hinsichtlich der Verarbeitung von Auftraggeber-Daten nur nach vorheriger schriftlicher Zustimmung des Auftraggebers begründen. Zurzeit sind für den Auftragnehmer die in **Anlage 3** mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer informiert den Auftraggeber immer über

jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragnehmers.

10.2 Nicht als Unterauftragsverhältnis im Sinne der Ziffer 10.1 sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

10.3 Zur Prüfung einer Zustimmung nach Ziffer 10.1 hat der Auftragnehmer dem Auftraggeber den Entwurf des Unterauftragsdatenverarbeitungsvertrags zwischen ihm und dem Unterauftragnehmer ungekürzt in Kopie zur Verfügung zu stellen. Ein Anspruch auf Erteilung der Zustimmung durch den Auftraggeber besteht nicht.

10.4 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer stellt bei jeder Unterbeauftragung sicher, dass die in Art. 28 Abs. 2 und Abs. 4 DSGVO genannten Bedingungen eingehalten werden. Die Ausübung der Kontrollrechte des Auftraggebers nach Ziffer 9 muss gegenüber dem Unterauftragnehmer möglich sein. In dem Unterauftragsdatenverarbeitungsvertrag sind die Verantwortlichkeitssphären des Auftragnehmers und des Unterauftragnehmers klar voneinander abzugrenzen. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen den einzelnen Unterauftragnehmern. Der Auftragnehmer haftet für ein Verschulden seiner Unterauftragnehmer wie für eigenes Verschulden. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, von dem Auftragnehmer Auskunft über den datenschutzwesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

10.5 Der Auftragnehmer hat den Unterauftragnehmer schriftlich zu verpflichten, was auch in einem elektronischen Format erfolgen kann (z.B. E-Mail).

10.6 Die Regelungen in dieser Ziffer 10 gelten auch, wenn ein Unterauftragnehmer in einem Drittstaat eingeschaltet wird. Der Auftragnehmer stellt in einem solchen Fall die datenschutzrechtliche Zulässigkeit durch geeignete Rechtsinstrumente, beispielsweise EU-Standardvertragsklauseln, sicher.

10.7 Der Auftragnehmer hat abgeleitete Kontrollpflichten gegenüber den Unterauftragnehmern und kann und muss hierfür die in diesem Vertrag beschriebenen, und in dem Unterauftragsdatenverarbeitungsvertrag zu spiegelnden Kontrollbefugnisse des Auftraggebers wahrnehmen. Der Auftraggeber bleibt berechtigt, die Ausübung der Kontrollbefugnisse durch den Auftragnehmer uneingeschränkt zu überwachen und kann jederzeit auch selbst diese Kontrolle gegenüber dem Unterauftragnehmer ausüben.

10.8 Die Mitteilungspflichten des Auftragnehmers gemäß Ziffer 7 gelten entsprechend für Datensicherheitsvorfälle, die sich bei seinen Unterauftragnehmer ereignen.

10.9 Die Weitergabe von Auftraggeber-Daten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

**11. Rechte der Betroffenen**

11.1 Die Rechte der durch die Datenverarbeitung betroffenen Personen nach Kapitel 3 DSGVO (Art. 12-23 DSGVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32-37 BDSG), insbesondere auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch der gespeicherten Auftraggeber-Daten, sind gegenüber dem Auftraggeber geltend zu machen.

11.2 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks der unter Ziffer 10.1 aufgeführten Rechte wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und ohne entsprechende Einzelweisung des Auftraggebers nicht mit dem Betroffenen in Kontakt treten. Der Auftragnehmer darf Auskünfte an Betroffene nur nach vorheriger Weisung durch den Auftraggeber erteilen.

11.3 Für den Fall, dass eine betroffene Person ihre Rechte im Sinne von Ziffer 11.1 geltend macht, hat der Auftragnehmer den Auftraggeber auf erstes Anfordern bei der Erfüllung dieser Ansprüche angesichts der Art der Verarbeitung auf zumutbare Weise mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen. Insbesondere wird der Auftragnehmer dem Auftraggeber unverzüglich, längstens aber innerhalb von fünf Werktagen, Informationen über die gespeicherten Auftraggeber-Daten (auch soweit sie sich auf den Speicherungszweck beziehen), die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen.

11.4 Der Auftragnehmer ist verpflichtet, Auftraggeber-Daten auf Weisung des Auftraggebers unverzüglich, spätestens aber innerhalb einer Frist von fünf Werktagen, zu berichtigen, zu löschen oder zu sperren. Der Auftragnehmer wird dem Auftraggeber die weisungsgemäße Berichtigung, Sperrung und Löschung jeweils auf Verlangen schriftlich bestätigen.

**12. Auskunft an Dritte**

Soweit der Auftragnehmer aufgrund gesetzlicher Bestimmungen Dritten Auskunft über Auftraggeber-Daten erteilen muss, ist der Auftragnehmer verpflichtet, den Auftraggeber rechtzeitig vor Auskunftserteilung über Empfänger, Zeitpunkt und Inhalt der zu erteilenden Auskunft und deren Rechtsgrundlage schriftlich zu informieren.

**13. Rückgabe und Löschung überlassener Daten und Datenträger**

13.1 Dem Auftragnehmer ist es untersagt, nach Beendigung dieses Vertrags Auftraggeber-Daten aktiv zu verarbeiten; nur eine weitere Speicherung der Auftraggeber-Daten bleibt zugelassen, bis der Auftragnehmer diese Auftraggeber-Daten bestimmungsgemäß an den Auftraggeber herausgegeben oder sie gelöscht oder vernichtet hat; in diesem Fall gelten die Bestimmungen dieses Vertrags auch nach Beendigung des Vertrags bis zu dem Zeitpunkt weiter, in dem der Auftragnehmer über keinerlei Auftraggeber-Daten mehr verfügt.

13.2 Der Auftragnehmer hat sämtliche ihm vom Auftraggeber überlassenen sowie sämtliche im Zuge der Vertragsdurchführung hinzugewonnenen Auftraggeber-Daten und alle Verarbeitungsergebnisse hieraus vollständig und unwiederbringlich zu löschen bzw. zu vernichten, sobald ihre Kenntnis für die Erfüllung des Zwecks der jeweiligen Verarbeitung nicht mehr erforderlich ist, spätestens jedoch nach Beendigung der vertragsgegenständlichen Leistungserbringung.

13.3 Mindestens 18 Werktage vor jeder Löschung oder Vernichtung nach Ziffer 13.2 hat der Auftragnehmer den Auftraggeber unter detaillierter Angabe der betroffenen Auftraggeber-Daten und Ergebnisse schriftlich über die bevorstehende Löschung bzw. Vernichtung zu informieren. Der Auftraggeber kann innerhalb dieser Frist vom Auftragnehmer die Herausgabe der von der Löschung bzw. Vernichtung betroffenen Auftraggeber-Daten und Ergebnisse verlangen oder ihn anweisen, die Löschung/Vernichtung nicht vorzunehmen.

13.4 Soweit Auftraggeber-Daten auf Datenträgern enthalten sind, sind diese unter Einhaltung einer angemessenen Sicherheitsstufe zu vernichten.

13.5 Die Bestimmungen der Ziffern 13.2–13.4 gelten auch für Vervielfältigungen der Auftraggeber-Daten (insbesondere Archivierungs- und Sicherungsdateien) in allen Systemen des Auftragnehmers sowie für Test- und Ausschussdaten.

13.6 Über eine Löschung bzw. Vernichtung von Auftraggeber-Daten hat der Auftragnehmer ein Protokoll zu erstellen, das dem Auftraggeber auf Anforderung unverzüglich vorzulegen ist.

13.7 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch den Auftragnehmer entsprechend der

jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

**14. Vertragsdauer und Kündigung**

14.1 Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

14.2 Ergänzend zu Ziffer 14.1 steht dem Auftraggeber ein jederzeitiges außerordentliches Kündigungsrecht bezüglich dieses Vertrags sowie des Hauptvertrags aus wichtigem Grund zu. Ein wichtiger Grund liegt für den Auftraggeber insbesondere vor, wenn

- der Auftragnehmer gegen eine wesentliche Pflicht aus diesem Vertrag verstößt,
- der Auftragnehmer die Auftraggeber-Daten für andere als nach Ziffer 2.2 zugelassene Zwecke verwendet,
- eine Weisung des Auftraggebers nach Ziffer 3 dieses Vertrags nicht oder nur teilweise ausführt,
- der Auftragnehmer die Ausübung der Kontrollrechte des Auftraggebers nach Ziffer 9 dieses Vertrags verweigert oder nicht nur unerheblich behindert oder
- der Auftragnehmer Unterauftragnehmer entgegen Ziffer 10 ohne vorherige schriftliche Zustimmung des Auftragnehmers einschaltet.

14.3 Der Hauptvertrag darf im Falle einer Beendigung dieses Vertrags nur fortgeführt werden, wenn ausgeschlossen ist, dass der Auftragnehmer Auftraggeber-Daten verwendet oder darauf zugreift.

**15. Verhältnis zum Hauptvertrag**

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

**16. Geltungszeitraum**

Die Bestimmungen aus dieser Vereinbarung zur „Auftragsverarbeitung nach Art. 28 DSGVO“ gelten ab dem 25. Mai 2018. Bis zum Ablauf des 24. Mai 2018 gilt nur die zugehörige Vereinbarung zur „Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz (BDSG)“.

| | |
|---|---|
| _____ | _____ |
| Ort, Datum | Ort, Datum |
| _____ | _____ |
| Unterschrift Auftraggeber | Unterschrift Auftragnehmer |

**Hinweis:**

Diese Vereinbarung ist bei gleichzeitigem Abschluss der „Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz (BDSG)“ ohne eigene Unterschrift wirksam.

**Anlagen:**

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Unterauftragnehmer

**Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen**

**Art und Zweck der Datenverarbeitung:**

| |
|---|
| |

**Art der personenbezogenen Daten:**

| |
|---|
| |

**Kategorien betroffener Personen:**

| |
|---|
| |

**Anlage 2: Technische und organisatorische Maßnahmen**

**1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)**

**Zutrittskontrolle**
Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

**Beispiele für mögliche Vorkehrungen**

- Eingangstüren werden stets verschlossen gehalten
- Individuelle Zutrittsberechtigung über RFID-Chip mit Dokumentation der Zutrittsrechte
- Anwesenheitsaufzeichnungen für Mitarbeiter (Zeiterfassungseinrichtungen)
- Besucher/Externe werden begleitet bzw. abgeholt und stets beaufsichtigt
- Videoüberwachung mit Aufzeichnung an der Eingangstür
- Magnetische oder Chipkarten
- Schlüssel
- Elektronische Türöffner
- Sicherheitsdienst und/oder Sicherheitspersonal am Eingang
- Alarmsystem

**Zugangskontrolle/Verschlüsselung**
Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

**Beispiele für mögliche Vorkehrungen**

- Alle IT-Programme laufen auf dem eigenen Server im Rechenzentrum (Housing)
- Zugang ist besonders gesichert (Verschlüsselung, VPN)
- Abschottung des Netzwerkes gegen ungewollte Zugriffe von außen (Firewall).
- Zugang zu EDV-Systemen nur mit Benutzerkennung und individuellem Passwort möglich.
- Zugangsberechtigungen werden dokumentiert
- Passwortrichtlinie wird über Active Directory durchgesetzt.
- IT-Systeme werden bei wiederholt erfolglosem Anmeldeversuch automatisch gesperrt
- Funktionale Zuordnung einzelner Endgeräte und Protokollierung der Systemnutzung.
- Mobile Datenträger sind verschlüsselt (Hardwareverschlüsselung)
- Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit
- Zwei-Faktor-Identifizierung

**Zugriffskontrolle**
Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

**Beispiele für mögliche Vorkehrungen**

- Individuelle Zugriffsrechte für jeden einzelnen Benutzer (in einem schriftlichen Berechtigungskonzept dokumentiert), zentrale Verwaltung und Steuerung.
- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt.
- Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen.
- Es ist technisch unterbunden, dass Daten auf lokale IT-Systeme kopiert werden
- Daten auf mobilen IT-Systemen sind verschlüsselt (komplettes System, Hardwareverschlüsselung)
- Aufzeichnung von Zugriffen auf das IT-System

**Trennungskontrolle/Zweckbindungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

| **Beispiele für mögliche Vorkehrungen** |
| --- |
| - Trennung der Zugriffsregelungen über Datenbankprinzip.<br>- Softwareseitige Mandantentrennung<br>- Trennung von Produktiv- und Testsystemen (in getrennten Datenbanken) |

**2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)**

**Weitergabekontrolle**
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

**Beispiele für mögliche Vorkehrungen**

- Übermittlungen personenbezogener Daten sind in Verfahrensübersicht dokumentiert.
- Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Verbindung zwischen Clients und Server ist besonders gesichert (Verschlüsselung, VPN).
- Mitbringen und verwenden privater Datenträger ist untersagt. Es dürfen nur verschlüsselte betriebliche Datenträger genutzt werden.
- Wiederbeschreibbare Datenträger werden vor der Wiederverwendung nach Standard DOD 5220-220.M gelöscht.
- Bei Hardwaretausch werden Festplatten vorher ausgebaut.
- Kontrollierte Vernichtung von Datenträgern mit Protokollierung (physische Vernichtung, zertifizierter Entsorger).
- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN.
- Elektronische Unterzeichnung

**Eingabekontrolle**
Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

**Beispiele für mögliche Vorkehrungen**

- automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung
- Protokollierung gescheiterter Zugriffsversuche
- Protokollierung der Aktivitäten des Systemverwalters und sämtlicher Benutzer
- Protokollierung aller Aktivitäten auf dem Server
- Sicherung der Protokolldaten gegen Verlust oder Veränderung
- Dokumentation der Eingabeprogramme

**3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO**

**Verfügbarkeitskontrolle**
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

**Beispiele für mögliche Vorkehrungen**

- Datensicherheitskonzept.
- Versionierte Daten- und Systembackups nach Backup-Plan (täglich/wöchentlich)
- Festplattenspiegelung (RAID), Backup-Rechenzentrum.
- Schadsoftwareschutz. Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt
- Erhaltene und auszuliefernde Datenträger werden Schadsoftwarecheck unterzogen
- Berichtsverfahren und Notfallplan
- Unterbrechungsfreie Stromversorgung

**4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO, Art. 25 Abs. 1 DSGVO)**

**Auftragskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können:

**Beispiele für mögliche Vorkehrungen**

- Auftragnehmer werden sorgfältig ausgesucht.
- Klare und unzweifelhafte vertragliche Regelungen zur Datenverarbeitung
- Formalisiertes Weisungsmanagement
- Weisungen werden grundsätzlich schriftlich erteilt.
- Kontrolle des Auftragnehmers durch die Geschäftsführung oder den Datenschutzbeauftragten
- Pflicht zur Vorbewertung

**5. Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO, Art. 25 Abs. 1 DSGVO)**

Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

**Beispiele für mögliche Vorkehrungen**

- Abgestufte Löschvorgänge in Petentenakten

**Anlage 3: Unterauftragnehmer**

| Name | Anschrift/Land |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |