

VERTRAGSBESTANDTEIL

Vereinbarung zur Auftragsverarbeitung (AVV)

nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) – Bestandteil der Verträge der 4develope UG (haftungsbeschränkt)

Stand: Oktober 2026

Inhalt

Präambel	§ 6 Nachweismöglichkeiten
§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung	§ 7 Subunternehmer (weitere Auftragsverarbeiter)
§ 2 Anwendungsbereich und Verantwortlichkeit	§ 8 Informationspflichten, Form, Vorrang, Rechtswahl
§ 3 Pflichten des Auftragnehmers	§ 9 Haftung und Schadensersatz
§ 4 Pflichten des Auftraggebers	Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO
§ 5 Anfragen betroffener Personen	

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag (Angebot, Leistungsbeschreibung und AGB von 4develope in der jeweils vereinbarten Fassung) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind für jedes Produkt in der Leistungsbeschreibung (Abschnitt „Datenschutz“) festgelegt. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

- Vom Auftraggeber gepflegte Inhalte, welche in der Leistungsbeschreibung definiert werden
- Zugangs- und Kontaktdaten der Mitarbeiter des Auftraggebers und sonstiger Nutzer, soweit sie für die bereitgestellten Zugänge verarbeitet werden (z. B. CMS- oder WordPress-Konten, E-Mail-Postfächer)

- Zugriffs- und Kommunikationsdaten, die bei der Nutzung der Leistungen anfallen (z. B. Zugriffsdaten in Server-Logs, über Formulare übermittelte Daten, Inhalte und Metadaten von E-Mails)

Zweck der Verarbeitung ist die Erbringung der vertraglich vereinbarten Leistungen (Funktion der Leistung) einschließlich der Verwaltung und Absicherung der Zugänge (Zugriffskontrolle).

Nicht Gegenstand dieser Vereinbarung sind Verarbeitungen, die der Auftragnehmer in eigener Verantwortung vornimmt, insbesondere die Verarbeitung der Kontakt- und Vertragsdaten des Auftraggebers und seiner Ansprechpartner zur Anbahnung, Durchführung und Abrechnung des Vertrags sowie der Angaben zum Domaininhaber. Hierüber informiert die Datenschutzerklärung des Auftragnehmers.

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Der konkrete Standort der Daten ist in der Leistungsbeschreibung festgelegt.

§ 2 Anwendungsbereich und Verantwortlichkeit

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
- (2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in Textform (§ 126b BGB) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, es sei denn, er ist durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

- (2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

- (3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Für Unterstützungsleistungen, die über die im Vertrag vereinbarten Leistungen hinausgehen, kann der Auftragnehmer eine angemessene Vergütung nach Aufwand verlangen; er weist den Auftraggeber vorab auf die zu erwartenden Kosten hin. Dies gilt nicht, soweit die Unterstützung durch einen Verstoß des Auftragnehmers gegen diese Vereinbarung oder gegen datenschutzrechtliche Vorschriften veranlasst ist.
- (4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
- (5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten des Auftraggebers bekannt geworden ist. Die Meldung enthält, soweit dem Auftragnehmer bekannt, die Angaben nach Art. 33 Abs. 3 DS-GVO, insbesondere
- a) eine Beschreibung der Art der Verletzung, soweit möglich mit den Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze,
 - b) den Namen und die Kontaktdaten des Ansprechpartners nach Abs. 6,
 - c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung,
 - d) eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Soweit die Angaben nicht zur selben Zeit bereitgestellt werden können, reicht der Auftragnehmer sie unverzüglich nach.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

- (6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
- (7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
- (8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

- (9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber. Liegt dem Auftragnehmer 30 Tage nach Auftragsende kein abweichendes Verlangen des Auftraggebers vor, löscht der Auftragnehmer die Daten. Daten in Datensicherungen (Backups) werden spätestens 90 Tage nach Auftragsende gelöscht; bis dahin sind sie vor Zugriff geschützt und werden nicht weiterverarbeitet. Gesetzliche Aufbewahrungspflichten des Auftragnehmers bleiben unberührt.
- (10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

- (1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (2) Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO verpflichtet sich der Auftraggeber, den Auftragnehmer bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
- (3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

- (1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der

Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

- (1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
- (2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für seinen Aufwand bei der Mitwirkung an Inspektionen kann der Auftragnehmer eine angemessene Vergütung verlangen; dies gilt nicht, soweit die Inspektion einen Verstoß des Auftragnehmers gegen diese Vereinbarung oder gegen datenschutzrechtliche Vorschriften ergibt.
- (3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

- (1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (»Subunternehmer«) nach Maßgabe der folgenden Absätze einzusetzen (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten Subunternehmer sind in der Leistungsbeschreibung des jeweiligen Produkts mit Firma, Anschrift, Teilleistung und Standort der Daten aufgeführt und gelten mit Vertragsschluss als genehmigt.
- (2) Ein Subunternehmerverhältnis im Sinne dieser Regelung liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt und dabei personenbezogene Daten des Auftraggebers verarbeitet werden. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer bei Dritten als reine Unterstützung in Anspruch nimmt, z. B. Telekommunikations-, Post- und Transportdienstleistungen.
- (3) Bei einer beabsichtigten Hinzuziehung oder Ersetzung von Subunternehmern informiert der Auftragnehmer den Auftraggeber mindestens 30 Tage vorher per E-Mail an den nach § 4 Abs. 3 benannten Ansprechpartner, ist kein Ansprechpartner benannt, an die im Vertrag angegebene E-Mail-

Adresse des Auftraggebers, sowie durch Veröffentlichung der Information unter <https://4develope.com/vertragsdokumente>.

Der Auftraggeber kann der Änderung innerhalb von 14 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Änderung als genehmigt. Widerspricht der Auftraggeber und ist eine einvernehmliche Lösung zwischen den Parteien nicht möglich, kann jede Partei den Vertrag über die von der Änderung betroffenen Leistungen außerordentlich zu dem Zeitpunkt kündigen, zu dem der Auftragnehmer den neuen Subunternehmer einsetzen will. Die Kündigung ist bis zu diesem Zeitpunkt in Textform zu erklären. Bis zum Wirksamwerden der Kündigung setzt der Auftragnehmer den neuen Subunternehmer für die Verarbeitung der Daten des Auftraggebers nicht ein.

- (4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Der Auftragnehmer wird mit diesen Dritten Vereinbarungen treffen, die mindestens das Schutzniveau dieser Vereinbarung gewährleisten (Art. 28 Abs. 4 DS-GVO). Kommt ein Subunternehmer seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Subunternehmers.

§ 8 Informationspflichten, Form, Vorrang, Rechtswahl

- (1) 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.
- (2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen der Textform (§ 126b BGB) und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Änderungen nach § 13 der AGB (Änderungen der Vertragsdokumente) bleiben unberührt.
- (3) In allen Fragen der Verarbeitung personenbezogener Daten gehen die Regelungen dieser Vereinbarung der Leistungsbeschreibung und den AGB vor. Individuelle Vereinbarungen im Angebot bzw. in der Auftragsbestätigung gehen auch dieser Vereinbarung vor (§ 305b BGB). Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
- (4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart. Die Haftung der Parteien gegenüber betroffenen Personen nach Art. 82 DS-GVO bleibt unberührt.

Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Der Auftragnehmer trifft die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen für alle Leistungen, bei denen er personenbezogene Daten im Auftrag verarbeitet. Ein höheres Schutzniveau für einzelne Auftraggeber kann im Angebot vereinbart werden. Die Gliederung folgt Art. 32 Abs. 1 DS-GVO.

Die Server werden ausschließlich bei den in der jeweiligen Leistungsbeschreibung genannten Subunternehmern (Hosting-Anbietern) betrieben. Deren physische und infrastrukturelle Sicherheitsmaßnahmen sind Bestandteil der nachfolgend beschriebenen Maßnahmen.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Anforderung:

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Maßnahmen:

- Betrieb der Server ausschließlich in Rechenzentren der Hosting-Anbieter mit Zutrittskontrollsystemen, Videoüberwachung und Sicherheitspersonal.
- Es werden ausschließlich Hosting-Anbieter eingesetzt, deren Rechenzentren mindestens nach ISO/IEC 27001 zertifiziert sind. Die Zertifizierungen der einzelnen Anbieter sind in der Leistungsbeschreibung beim jeweiligen Subunternehmer angegeben.

1.2 Zugangskontrolle

Anforderung:

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen:

- Zugriff auf Server nur mit autorisierten SSH-Schlüsseln.
- Arbeitsplatzrechner im Büro und im Homeoffice sind mit Passwort gesichert, sperren sich bei Inaktivität automatisch (Bildschirmsperre) und ihre Festplatten sind vollständig verschlüsselt.
- Protokollierung der Zugriffe auf die Server und Verwaltungsoberflächen, mit denen die Leistungen erbracht werden.
- Benutzerverwaltung inklusive Rechtezuweisung nach dem dokumentierten Rollen- und Berechtigungskonzept des Auftragnehmers. Kennwörter, die in vom Auftragnehmer betriebenen Systemen gespeichert werden, werden ausschließlich mit einem kryptografischen Hashverfahren nach dem Stand der Technik gespeichert (z. B. bcrypt oder Argon2), nicht im Klartext.
- Passwortvergabe nach einer schriftlichen Passwortrichtlinie; Zugangsdaten werden in einem Passwortmanager verwaltet.

- Für alle Verwaltungsoberflächen der Hosting-Anbieter ist eine Mehr-Faktor-Authentifizierung (MFA) erforderlich; sie wird durch die jeweiligen Anbieter erzwungen, insbesondere bei privilegierten Zugriffen.

1.3 Zugriffskontrolle

Anforderung:

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen:

- Vergabe von Berechtigungen nach dem Erforderlichkeitsprinzip (Need-to-know) auf Basis eines Rollen- und Rechtekonzepts
- Regelmäßige Überprüfung der Berechtigungen und unverzüglicher Entzug nicht mehr benötigter Zugänge, insbesondere beim Ausscheiden von Mitarbeitern
- Protokollierung von Zugriffen, sowie Änderungen.

1.4 Trennungskontrolle

Anforderung:

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können.

Maßnahmen:

- Trennung der Daten des Auftraggebers von den Daten des Auftragnehmers und anderen Mandanten
- Strikte Trennung von Test- und Livesystem

1.5 Pseudonymisierung und Verschlüsselung

Anforderung:

Personenbezogene Daten sind, soweit dies für den jeweiligen Zweck möglich ist, zu pseudonymisieren und nach dem Stand der Technik zu verschlüsseln.

Maßnahmen:

- Vollständige Verschlüsselung der Festplatten der Arbeitsplatzrechner (siehe Ziffer 1.2)
- Verschlüsselung der Daten bei der Übertragung und Speicherung (siehe Ziffer 2.1)
- In Test- und Entwicklungsumgebungen werden keine Echtdateien verwendet oder diese werden zuvor pseudonymisiert.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Anforderung:

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes 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.

Personenbezogene Daten dürfen nicht ohne Zustimmung an Dritte weitergegeben werden. Eine zufällige Weitergabe an unbefugte Dritte ist auszuschließen.

Maßnahmen:

- Die Übertragung von Daten zwischen Endgerät und Servern erfolgt verschlüsselt (TLS, z. B. HTTPS, IMAPS, SMTPS) mit Algorithmen nach dem Stand der Technik.
- Bei der Speicherung werden Daten verschlüsselt, soweit der jeweilige Hosting-Anbieter dies vorsieht; in der Google Cloud erfolgt die Verschlüsselung gespeicherter Daten standardmäßig.
- Auf Wunsch des Auftraggebers kann ein kundenspezifischer Schlüssel eingesetzt werden, der ausschließlich für die Daten dieses Auftraggebers verwendet wird. Der Schlüssel wird auf eigener Hardware erstellt und gespeichert und dem Hosting-Anbieter nur zur Verschlüsselung und Entschlüsselung der Daten zur Verfügung gestellt. Er kann jederzeit entzogen werden, sodass die Daten selbst im Fall eines Angriffs oder einer behördlichen Datenabfrage beim Hosting-Anbieter nicht lesbar sind. Die Einzelheiten werden im Angebot vereinbart.
- Datenschutzkonformes Löschen
- Protokollierung von Datenverbindungen

2.2 Eingabekontrolle**Anforderung:**

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- Identifizierung und Authentifizierung der Berechtigten
- Protokollierung von Zugriffen, sowie Änderungen.
- Regelmäßige Auswertung der Protokolle (Stichprobenartig)

3. Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO)**3.1 Verfügbarkeitskontrolle****Anforderung:**

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:

- Tägliches Backup der Datenbanken; Umfang und Aufbewahrungsdauer der Backups regelt die jeweilige Leistungsbeschreibung.
- Nutzung von Cloud-Infrastruktur um einen reibungslosen Betrieb zu gewährleisten und schnell auf mögliche Ausfälle reagieren zu können.

- Redundante Infrastruktur in den Rechenzentren der Hosting-Anbieter (unterbrechungsfreie Stromversorgung, Klimatisierung, Brandschutz) sowie Absicherung der Server durch Firewalls

3.2 Wiederherstellbarkeit

Anforderung:

Die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen sind bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Maßnahmen:

- Wiederherstellung der Daten aus den Backups nach Ziffer 3.1; Umfang und Aufbewahrungsdauer der Backups regelt die jeweilige Leistungsbeschreibung.
- Nutzung der Redundanz- und Wiederherstellungsmechanismen der Hosting-Anbieter.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO)

4.1 Auftragskontrolle

Anforderung:

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen:

- Identifizierung und Authentifizierung der Berechtigten
- Protokollierung der Aktionen
- Überprüfung anhand von Audits
- Regelmäßige Auswertung der Protokolle (Stichprobenartig)
- Sorgfältige Auswahl der Subunternehmer und vertragliche Verpflichtung nach Art. 28 Abs. 4 DS-GVO (§ 7)

4.2 Datenschutz-Management und Umgang mit Sicherheitsvorfällen

Anforderung:

Die Wirksamkeit der technischen und organisatorischen Maßnahmen ist regelmäßig zu überprüfen, Sicherheitsvorfälle sind zu erkennen, zu bewerten und zu melden.

Maßnahmen:

- Überprüfung und Aktualisierung dieser Maßnahmen mindestens einmal jährlich sowie bei wesentlichen Änderungen der Infrastruktur
- Verpflichtung aller Mitarbeiter auf die Vertraulichkeit und regelmäßige Sensibilisierung zum Datenschutz
- Festgelegter Ablauf zur Erkennung, Bewertung und Meldung von Verletzungen des Schutzes personenbezogener Daten an den Auftraggeber (§ 3 Abs. 5)