

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (AVV: Auftragsverarbeitungsvertrag)

secrypt GmbH
Hohenzollerndamm 183
10713 Berlin
Deutschland

Inhalt

1	Präambel.....	2
2	Allgemeines.....	2
3	Dauer und Beendigung des Auftrags.....	2
4	Gegenstand des Auftrags.....	2
5	Rechte und Pflichten des Auftraggebers	3
6	Allgemeine Pflichten des Auftragnehmers	4
7	Kontrollbefugnisse	4
8	Unterauftragsverhältnisse.....	5
9	Vertraulichkeit und Geheimhaltung.....	6
10	Betroffenenrechte.....	6
11	Technische und organisatorische Maßnahmen zur Datensicherheit.....	7
12	Haftung	7
13	Beendigung	8
14	Schlussbestimmungen	8
	Anlage 1: Technische und organisatorische Maßnahmen (TOMs)	9
	Anlage 2: Genehmigte Unterauftragnehmer	12

1 Präambel

Dieser Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 Abs. 3 DSGVO ist Bestandteil des Vertragsverhältnisses über die Erbringung von Leistungen im Zusammenhang mit den Software-Produkten und Dienstleistungen der secrypt GmbH („Hauptvertrag“) zwischen der secrypt GmbH („Auftragnehmer“) und dem Kunden („Auftraggeber“).

Der vorliegende Vertrag über die Verarbeitung personenbezogener Daten im Auftrag („Vertrag“) wird als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Regelungen des Art. 28 der Datenschutz-Grundverordnung (DSGVO) zwischen den Parteien getroffen.

2 Allgemeines

Der Auftragnehmer erbringt im Auftrag des Auftraggebers Leistungen im Zusammenhang mit secrypt-Software (z.B. digiSeal reader, digiSeal office, digiSeal server, digiSeal archive, digiSeal web) und/oder weitere Dienstleistungen (z.B. Beratung) durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer personenbezogene Daten verarbeitet, um die vertragsgegenständlichen Leistungen erbringen zu können.

3 Dauer und Beendigung des Auftrags

- (1) Dieser Vertrag beginnt ab Abschluss des Hauptvertrages und gilt für die Dauer des Hauptvertrages.
- (2) Eine Kündigung des Hauptvertrages bewirkt automatisch auch eine Kündigung dieses Vertrages. Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

4 Gegenstand des Auftrags

(1) Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende produktspezifischen Arbeiten und/oder Leistungen:

- Erzeugung und Verifikation von Signaturen auf digitalen Daten und Dokumenten
- Zukünftiger Nachweis der Validität von Signaturen (Integrität und Authentizität)
- Nachvollziehbarkeit von Signaturprozessen
- Durchführung und Abrechnung von Online-Services von Vertrauensdiensteanbietern
- Installation, Registrierung (Freischaltung) und Konfiguration von secrypt-Software sowie etwaige Problembehandlung
- Anlegen, Ändern und Löschen von Benutzerkonten/Benutzerberechtigungen in secrypt-Software
- Verwendung des Rechthehaushaltes des Auftraggebers auf Betriebssystemebene (z.B. Microsoft Active Directory) in secrypt-Software zur Gewährleistung des Betriebes von secrypt-Software in spezifischen IT-Infrastrukturen (z.B. für ProxyAuthentifizierung)
- Fernwartung zur Installation, Registrierung (Freischaltung) und Konfiguration von secrypt-Software sowie etwaiger Problembehandlung

Im Einzelnen sind insbesondere folgende Daten Bestandteil der Datenverarbeitung:

Art der Daten	Zweck der Datenverarbeitung	Kreis der Betroffenen
Nutzer Profildaten	Erhebung und Verwaltung zur Bereitstellung der secrypt-Software	Beschäftigte/Mitarbeiter des Auftraggebers; andere berechtigte Nutzer
Kontaktinformationen	Erhebung und Verwaltung zur Bereitstellung der secrypt-Software	Beschäftigte/Mitarbeiter des Auftraggebers; andere berechtigte Nutzer
weitere Daten von Betroffenen, die im jeweiligen IT-System des Auftraggebers gespeichert sind	Erfüllung der Hauptleistungspflichten aus dem Hauptvertrag	Kunden des Auftraggebers, Dritte
Name und Kontaktdaten von Nutzern/Administratoren der IT-Systeme	Softwarepflege und Support	Beschäftigte/Mitarbeiter des Auftraggebers
weitere Daten von Betroffenen, die im jeweiligen IT-System des Auftraggebers gespeichert sind	Softwarepflege und Support	Kunden des Auftraggebers, Dritte

(2) Der Auftragnehmer verarbeitet die Auftraggeber-Daten ausschließlich im Auftrag und nach dokumentierter Weisung des Auftraggebers. Der Auftraggeber bleibt Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

5 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen aus den Art. 12 bis 22 DSGVO ist der Auftraggeber allein verantwortlich.

(2) Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer im Rahmen dieses Vertrages erfolgt ausschließlich nach Weisung des Auftraggebers gemäß Art. 28 Abs. 3 S. 2 lit. a DSGVO, es sei denn, der Auftragnehmer ist nach dem Recht der Europäischen Union oder dem Recht des Mitgliedstaates, dem er unterliegt, zur weiteren Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Pflege- und Supportleistungen gegenüber dem Auftragnehmer zu erteilen. Solche Einzelweisungen nach Abschluss des Vertrages bedürfen der Textform (z.B. E-Mail) und sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit den Pflege- und Supportleistungen durch den Auftragnehmer feststellt.

6 Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Zusammenhang mit den Pflege- und Supportarbeiten im Auftrag verarbeitet, vor der unbefugten Kenntnisnahme Dritter geschützt sind. Dies schließt die Verpflichtung der entsprechenden Angestellten auf die Einhaltung der datenschutzrechtlichen Anforderungen und auf die Verschwiegenheit ein, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Den Auftragnehmer trifft keinerlei Verpflichtung, Weisungen des Auftraggebers (datenschutz-)rechtlich zu prüfen. Ist der Auftragnehmer jedoch der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, wird er den Auftraggeber darauf hinweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis die Weisung bestätigt oder geändert wird. Räumt der Auftraggeber auf die Information über eine nach Ansicht des Auftragnehmers rechtswidrige Weisung die Bedenken des Auftragnehmers nicht aus, kann dieser die Durchführung der betreffenden Weisung ablehnen, soweit sie seine Verantwortungssphäre betrifft.

(3) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(4) Der Auftragnehmer ist verpflichtet den Auftraggeber, im Rahmen des Zumutbaren und Erforderlichen sowie gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten, bei der Erfüllung von dessen Pflichten aus Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO zu unterstützen. Die Unterstützung erfolgt unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen sowie nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, insbesondere bei der Beantwortung von Anträgen auf Wahrnehmung der entsprechend in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen.

(5) Der Auftragnehmer wird seinen Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verarbeitungsverzeichnisses nachkommen. Diese Pflicht besteht nicht, wenn die Voraussetzungen von Art. 30 Abs. 5 DSGVO erfüllt sind.

(6) Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Der Auftragnehmer ist verpflichtet, einen fachkundigen und zuverlässigen Datenschutzbeauftragten schriftlich zu bestellen, der seine Tätigkeit gemäß der Art. 37, 38 und 39 DSGVO sowie § 38 BDSG ausüben kann, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind.

7 Kontrollbefugnisse

(1) Der Auftraggeber überzeugt sich auf eigene Kosten vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Anlage 1 und dokumentiert das Ergebnis. Dies

geschieht durch Einholung einer Selbstauskunft des Auftragnehmers, die dieser auch durch Vorlage eines geeigneten Zertifikats eines Sachverständigen erfüllen kann.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung alle erforderlichen Auskünfte und Informationen bezüglich seiner Pflichten aus dieser Vereinbarung zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen der Anlage 1 nachzuweisen. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 oder Zertifizierungen gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren), eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erfolgen.

(3) Der Auftraggeber oder ein entsprechend Beauftragter haben das Recht vorgenannte Kontrollen zu den üblichen Geschäftszeiten vorzunehmen. Diese Kontrollen sind rechtzeitig (in der Regel mindestens zwei Wochen vorher) anzukündigen und haben den Betriebsablauf beim Auftragnehmer so wenig wie möglich zu beeinträchtigen.

(4) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aus diesem Vertrag verpflichtet ist. Zudem hat er den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

8 Unterauftragsverhältnisse

(1) Der Auftraggeber stimmt der Beauftragung der in **Anlage 2** aufgeführten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 1 bis 4 DSGVO ausdrücklich zu.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragnehmer informieren. Gegen derartige Änderungen darf der Auftraggeber aus wichtigem, dem Auftragnehmer nachzuweisenden Grund, Einspruch erheben. Der Einspruch ist binnen einer Frist von einer Woche ab Zugang einer entsprechenden Mitteilung des Auftragnehmers schriftlich auszusprechen.

(3) Keiner Mitteilung bedarf die Einschaltung von Unterauftragnehmern, bei denen der Unterauftragnehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung nach dem Hauptvertrag in Anspruch nimmt, z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder zur Entsorgung von Datenträgern sowie für sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann. Der Auftragnehmer wird auch diese mit der gebotenen Sorgfalt auswählen und im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Schutz der Auftraggeber Daten zu gewährleisten.

(4) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und

regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten benannt hat, sofern dies nach Art. 37 DSGVO i.V.m. § 38 BDSG erforderlich ist.

(5) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(6) Die Verpflichtung des Unterauftragnehmers muss den Anforderungen von Art. 28 Abs. 4 DSGVO entsprechen.

(7) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

9 Vertraulichkeit und Geheimhaltung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Dies gilt insbesondere in den Fällen, in denen der Auftraggeber zur Einhaltung der Schweigepflicht aus § 203 StGB verpflichtet ist. Der Auftraggeber wird dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist.

10 Betroffenenrechte

(1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei dessen gesetzlichen Pflichten zur Umsetzung der Rechte betroffener Personen.

(2) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zur Wahrnehmung ihrer Rechte gemäß der Art. 12 bis 22 DSGVO der sie betreffenden Daten wenden sollte, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen.

(3) Der Auftragnehmer löscht auf Anforderung des Auftraggebers von der Verarbeitung umfasste personenbezogene Daten. Darüber hinaus hat der Auftragnehmer die zu verarbeitenden Daten nur nach dokumentierter Weisung des Auftraggebers zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken (sperrern).

11 Technische und organisatorische Maßnahmen zur Datensicherheit

- (1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen.
- (2) Für den Fall, dass der Auftragnehmer die Pflege- und Supportarbeiten für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt (z.B. im Falle der Fernwartung), sind vom Auftragnehmer die in der Anlage zu diesem Vertrag genannten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten einzuhalten.
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in Anlage 1 TOM zu diesem Vertrag.

12 Haftung

- (1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.
- (2) Für den Ersatz von Schäden, die eine betroffene Person wegen einer nach dem geltenden Datenschutzrecht unzulässigen oder unrichtigen Verarbeitung von Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber verantwortlich.
- (3) Der Auftraggeber verpflichtet sich, den Auftragnehmer im Innenverhältnis von allen Ansprüchen Dritter frei zu stellen, solange und soweit er nicht nachweist, dass der Auftragnehmer seinen speziell den Auftragnehmer treffenden Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung einer rechtmäßig erteilten Weisung des Auftraggebers oder gegen eine rechtmäßig erteilte Weisung gehandelt hat.
- (4) Sollte eine Datenschutzbehörde oder ein Gericht gegen den Auftragnehmer eine Geldbuße auf Grund einer Datenverarbeitung des Auftragnehmers verhängen, die auf einer Weisung des Auftraggebers beruht, hat der Auftraggeber dem Auftragnehmer den entsprechenden Betrag auf schriftliche Mitteilung hin in voller Höhe innerhalb von 30 Tagen ab der schriftlichen Mitteilung zu erstatten.
- (5) Der Auftraggeber hat dem Auftragnehmer sämtliche sich aus der von ihm zu vertretenden Rechtsverletzung gemäß Absatz 3 und 4 ergebenden Kosten zu erstatten, einschließlich der Kosten der Rechtsverfolgung.
- (6) Unbeschränkte Haftung: Der Auftragnehmer haftet unbeschränkt für Vorsatz und grobe Fahrlässigkeit, bei Verletzung einer vertraglich gewährten Garantie sowie nach Maßgabe des Produkthaftungsgesetzes. Für leichte Fahrlässigkeit haftet der Auftragnehmer bei Schäden aus der Verletzung des Lebens, des Körpers und der Gesundheit von Personen. Im Übrigen gilt folgende beschränkte Haftung: Bei leichter Fahrlässigkeit haftet der Auftragnehmer nur im Falle der Verletzung einer wesentlichen Vertragspflicht des Hauptvertrages, deren Erfüllung die ordnungsgemäße Durchführung des Hauptvertrages überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf (Kardinalpflicht). Die Haftung für leichte Fahrlässigkeit ist der Höhe nach beschränkt auf die bei Vertragsschluss vorhersehbaren Schäden, mit deren Entstehung typischerweise gerechnet werden muss.

13 Beendigung

- (1) Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags), nach Wahl des Auftraggebers, zurückzugeben oder zu löschen und bestehende Kopien zu vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der Daten besteht.
- (2) Der Auftragnehmer hat die Löschung bzw. Vernichtung von Auftraggeber-Daten zu dokumentieren und den Nachweis dem Auftraggeber auf Anforderung nachzuweisen.
- (3) 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 Schlussbestimmungen

- (1) Es gilt das Recht der Bundesrepublik Deutschland.
- (2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.
- (3) Gerichtsstand für Streitigkeiten im Zusammenhang mit dieser Vereinbarung ist Berlin.

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

Der Auftragnehmer ist verpflichtet, nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO einzuhalten:

1. VertraulichkeitZutrittskontrolle

Der Auftragnehmer trägt Sorge dafür, dass seine Büro- und Geschäftsräume grundsätzlich außerhalb der Büro- und Geschäftszeiten geschlossen sind.

Während der Büro- und Geschäftszeiten ist sichergestellt, dass Besucher oder sonstige Dritte sich nicht alleine in Räumen bewegen können, in denen sie Zugang zu personenbezogenen Daten erhalten könnten.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zugangskontrolle

Um Zugang zu IT-Systemen zu erhalten, müssen der Auftragnehmer und seine Beschäftigten über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von einem oder mehreren Administratoren vergeben.

Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Passwörter werden nach einem vorgegebenen Turnus gewechselt. Eine Passworthistorie ist hinterlegt. Fehlerhafte Anmeldeversuche werden protokolliert. Bei mehrmaliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte Verbindungen.

Alle Server und Client-Systeme, die bei der Erbringung von Leistungen für den Auftraggeber im Einsatz sind, sind durch Firewalls geschützt, die gewartet und mit aktuellen Updates und Patches versorgt werden.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter, die der Auftragnehmer vom Auftraggeber erhält oder für dessen IT-Systeme verwendet, werden grundsätzlich verschlüsselt gespeichert und sind nur den Beschäftigten zugänglich zu machen, die konkret mit der Erbringung von Leistungen für den Auftraggeber betraut sind.

Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.

Trennung

Soweit der Auftragnehmer personenbezogene Daten vom Auftraggeber im Zusammenhang mit der Auftragsverarbeitung erhält, wird er diese getrennt von Daten anderer Kunden verarbeiten.

Verschlüsselung

Ein administrativer Zugriff auf IT-Systeme des Auftraggebers erfolgt grundsätzlich über verschlüsselte Verbindungen, soweit dieser nicht innerhalb der Räumlichkeiten des Auftraggebers erfolgt.

2. Integrität

Eingabekontrolle

Der Auftragnehmer wird Eingaben, Änderungen oder Löschungen von personenbezogenen Daten, die er im Auftrag des Auftraggebers durchführt, in geeigneter Weise dokumentieren, sofern nicht sichergestellt ist, dass das jeweilige IT-System selbst eine Protokollierung entsprechender Aktivitäten durchführt.

Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf jeweils nur in dem Umfang erfolgen, wie und soweit dies mit dem Auftraggeber abgestimmt ist.

Die Nutzung von privaten Datenträgern ist dem Auftragnehmer im Zusammenhang mit der Auftragsverarbeitung für den Auftraggeber untersagt.

3. Verfügbarkeit und Belastbarkeit

Soweit der Auftragnehmer personenbezogene Daten oder Zugangsdaten für den Auftraggeber speichert oder verwaltet, trägt er Sorge dafür, dass diese Daten mindestens täglich inkrementell und wöchentlich „voll“ gesichert werden. Es gibt ein Datensicherungskonzept, das auch das erfolgreiche Testen der Wiederherstellung von Daten beinhaltet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Auftragnehmer trägt durch Richtlinien und/oder Anweisungen an die Beschäftigten dazu bei, dass eine Verarbeitung personenbezogener Daten in einer Weise gewährleistet ist, die den Anforderungen der DSGVO entspricht.

Dies beinhaltet insbesondere Überprüfungen der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten und ggf. der Anpassung. Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich

dem Auftraggeber gemeldet werden, wenn dies Daten betrifft, die im Rahmen der Auftragsverarbeitung für den Auftraggeber verarbeitet werden.

Auftragskontrolle

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Etwaige nach Art. 25 DSGVO erforderliche Maßnahmen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten durch den Auftraggeber sind vom Auftraggeber zu treffen bzw. durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer festzulegen.

Anlage 2: Genehmigte Unterauftragnehmer

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Deutschland	Datenspeicherung
Mittwald CM Service GmbH & Co. KG	Königsberger Straße 4-6 32339 Espelkamp Deutschland	Datenspeicherung
Staufenberg Advisory GmbH	Am Räschen 10 35279 Neustadt (Hessen) Deutschland	Datenspeicherung
weclapp GmbH	Friedrich-Ebert-Straße 28 97318 Kitzingen Deutschland	Datenspeicherung