

Auftragsverarbeitungsvertrag - Addendum

Im Rahmen der Erbringung der vertraglich vereinbarten Software-as-a-Service-Leistungen („SaaS-Leistungen“) verarbeitet die Xentral ERP Software GmbH personenbezogene Daten im Auftrag des Kunden. Dabei handelt der Kunde als Verantwortlicher („Auftraggeber“) und Xentral als Auftragsverarbeiter („Auftragnehmer“) im Sinne der DSGVO.

Dieser Vertrag zur Auftragsverarbeitung („AV-Vertrag“) regelt die Rechte und Pflichten der Parteien im Zusammenhang mit dieser Verarbeitung gemäß Art. 28 DSGVO. Er wird mit Annahme des Angebots durch den Kunden Bestandteil des zwischen den Parteien geschlossenen Vertrags über die SaaS-Leistungen auf Grundlage der Xentral Allgemeinen Geschäftsbedingungen für Software-as-a-Service-Leistungen („SaaS AGB“).

Im Falle eines Widerspruchs zwischen den Bestimmungen dieses AV-Vertrags und den SaaS AGB haben die Bestimmungen dieses AV-Vertrags Vorrang.

§ 1 Gegenstand und Dauer der Datenverarbeitung

1. Gegenstand der Datenverarbeitung

a. Inhaltlicher Geltungsbereich

Gegenstand dieses AV-Vertrags ist die Erbringung der im Angebot beschriebenen Software as a Service (SaaS) für den Auftraggeber.

Dieser AV-Vertrag gilt für sämtliche Tätigkeiten, bei denen Mitarbeiter und/oder - soweit gem. nachstehendem § 6 zulässig - Subunternehmer des Auftragnehmers personenbezogene Daten des Auftraggebers erheben, verarbeiten oder nutzen.

b. Räumlicher Geltungsbereich

Nach diesem AV-Vertrag ist die Datenverarbeitung weltweit zulässig, d.h. im Gebiet der Europäischen Union und des Europäischen Wirtschaftsraumes (EWG), sicherer Drittstaaten (Art. 45 DSGVO) und weiterer Staaten (Art. 46 DSGVO).

2. Dauer der Datenverarbeitung

Dieser AV-Vertrag tritt mit Annahme des Angebots in Kraft, welches auf diesen AV-Vertrag referenziert. Die Laufzeit des AV-Vertrages richtet sich nach der Laufzeit bzw. Wirksamkeit des Hauptvertrages (SaaS AGB) zwischen den Parteien. Das Recht zur

außerordentlichen Kündigung aus wichtigem Grund bleibt davon unberührt.

§ 2 Umfang, Art und Zweck der Datenverarbeitung und Betroffene

1. Umfang und Zweck der Datenverarbeitung

Im Rahmen der Bestellung des Auftraggebers gestaltet sich Umfang und Zweck der Datenverarbeitung

- SaaS-Betrieb gemäß Angebot und SaaS-AGB
- Betrieb eines Ticket-Systems bzw. Support-Kanäle.

2. Art der Daten der Datenverarbeitung

Im Rahmen des AV-Vertrags erhebt, verarbeitet und nutzt der Auftragnehmer folgende Arten von Daten und hat hierauf die Möglichkeit eines Zugriffs:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkte- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

3. Kreis der Betroffenen

Der Kreis der durch den Umgang mit personenbezogenen Daten im Rahmen dieses AV-Vertrags Betroffenen umfasst:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten

§ 3 Verantwortung, einschließlich Weisungen

3.1 Verantwortung des Auftraggebers

1. Der Auftraggeber ist im Hinblick auf die Datenverarbeitung für die Einhaltung sämtlicher einschlägiger Datenschutzvorschriften, insb. der DSGVO und des Bundesdatenschutzgesetzes („BDSG“), verantwortlich soweit darin keine Aufgaben explizit dem Auftragnehmer zugewiesen sind (vgl. Art. 28 DSGVO)

Der Auftraggeber ist insb. dafür verantwortlich,

dass

- a. er die Zulässigkeit der Verarbeitung gem. Art. 6 Abs. 1 DSGVO beurteilt, insbes. etwaige Einwilligungserklärungen und/oder Betriebsvereinbarungen, die für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten erforderlich sind, eingeholt wurden und die gesetzlichen Erlaubnistatbestände dazu vorliegen.
 - b. die Rechte der Betroffenen (Art. 12 – 23 DSGVO) gewährt werden.
 - c. der Auftragnehmer bei der Durchführung der Pflegeleistungen nach diesem AV-Vertrag mit möglichst wenig personenbezogenen Daten in Kontakt kommt gemäß Art. 25 DSGVO.
 - d. er angemessene Vorkehrungen für den Fall trifft, dass Xentral ganz oder teilweise nicht ordnungsgemäß arbeitet (z.B. durch tägliche Datensicherung, Störungsdiagnose, regelmäßige Überprüfung der Datenverarbeitungsergebnisse).
 - e. er den Auftragnehmer vor einem Datenzugriff im Wege der Fernwartung rechtzeitig vorab darauf hinweist, inwieweit seine Daten nicht gegen Datenverlust gesichert sind. Ohne einen solchen Hinweis darf der Auftragnehmer davon ausgehen, dass alle Daten des Auftraggebers gegen Datenverlust gesichert sind, auf die der Auftragnehmer Zugriff erhält.
2. Der Auftraggeber ist „Verantwortlicher“ i.S.d. Art. 4 Abs. 7 DSGVO. Der Auftragnehmer verarbeitet die Daten ausschließlich zur Durchführung nach Weisung des Auftraggebers gemäß diesem AV-Vertrag. Darüber hinaus gilt:
- a. Sämtliche Weisungen des Auftraggebers zum Zeitpunkt des Abschlusses dieses AV-Vertrags finden sich abschließend in den Regelungen dieses AV-Vertrags und seinen Anhängen. Weitere Weisungen erteilt der Auftraggeber nur, soweit diese zur Durchführung der Datenverarbeitung erforderlich sind. Der Auftraggeber erteilt seine Weisungen nur in Schrift- oder Textform und in dokumentierter Art und Weise.
 - b. Der Auftraggeber wird gegenüber dem Auftragnehmer weisungsberechtigte Personen und ihre Vertreter wenigstens in Textform benennen. Ohne Benennung gelten nur die Support-berechtigten Personen (9.2 Customer Care-AGB) als weisungsberechtigt im Sinne dieses

AV-Vertrags.

3. Der Auftraggeber weist den Auftragnehmer darauf hin, wenn und soweit die technischen und organisatorischen Maßnahmen (Anhang 1) und/oder die übrigen Vorgaben dieses AV-Vertrags nicht mehr den gültigen Datenschutzvorschriften entsprechen, die auf den Auftraggeber Anwendung finden (inkl. gesetzlicher Neuerungen). Der Auftraggeber ist sich insbesondere im Klaren darüber, dass der Auftragnehmer grundsätzlich nur eine unverschlüsselte Kommunikation per E-Mail anbietet und dass durch einen unverschlüsselten E-Mail-Verkehr keine ausreichende Geheimhaltung gegenüber Dritten gewährleistet werden kann. Wünscht der Auftraggeber eine Verschlüsselung der E-Mail-Kommunikation, wird er hierzu das Ticket-System (gemäß 2.5 Customer Care-AGB) verwenden und/oder sich mit dem Auftragnehmer abstimmen.
4. Der Auftraggeber informiert den Auftragnehmer über jeden aktuellen Informationsaustausch mit den Datenschutzbehörden, soweit dieser Austausch die Datenverarbeitung nach diesem AV-Vertrag betrifft oder betreffen könnte.

3.2 Verantwortung des Auftragnehmers

1. Der Auftragnehmer wird personenbezogene Daten, die er im Rahmen dieses AV-Vertrags im Auftrag für den Auftraggeber verarbeitet, ausschließlich zur Erfüllung dieses AV-Vertrags verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch EU-Recht oder dem anwendbaren Recht eines Mitgliedstaates verpflichtet ist (z.B. Ermittlungen von Strafverfolgungsbehörden); 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 (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).
2. Wenn und soweit der Auftragnehmer der Auffassung ist, dass die Ausführung von Weisungen des Auftraggebers im Sinne des vorstehenden Absatzes zu einer Verletzung von Datenschutzbestimmungen führt, ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich hierauf hinzuweisen (Art. 28 Abs. 3 S. 3 DSGVO). In diesem Fall ist er berechtigt, die Durchführung der entsprechenden Weisung des Auftraggebers so lange auszusetzen, bis sie durch den Ansprechpartner des Auftraggebers bestätigt oder geändert wird.

3. Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich zu informieren, wenn und soweit er oder die bei ihm beschäftigten Personen gegen Datenschutz- oder gegen Bestimmungen dieses AV-Vertrags verstoßen haben.
4. Der Auftragnehmer wird den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 30, 32 - 36 DSGVO angemessen unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.
5. Der Auftragnehmer unterstützt den Auftraggeber bei Erfüllung der Rechte der Betroffenen (Art. 12 – 23 DSGVO), wenn der Auftraggeber hierzu eine dokumentierte Aufforderung (schriftlich oder in Textform) an den Auftragnehmer abgegeben hat.

§ 4 Kontrollen

1. Der Auftragnehmer wird seine zur Datenverarbeitung befugten Mitarbeiter zur Vertraulichkeit verpflichten und dies kontrollieren. Der Auftragnehmer weist dem Auftraggeber diese Verpflichtung auf das Datengeheimnis auf Anfrage nach.
2. Der Auftragnehmer ist berechtigt, den Nachweis über die Einhaltung des Datenschutzes und der Datensicherheit, insbesondere nach Art. 28 (3) lit. h. DSGVO bei sich und/oder Subunternehmern durch die Vorlage von Testaten oder Berichten unabhängiger Instanzen, ein schlüssiges Datensicherheitskonzept oder eine geeignete Zertifizierung durch ein IT-Sicherheits- und Datenschutzaudit ("Nachweise") zu erbringen. Eine Kontrolle vor Ort entfällt dadurch, sofern keine außergewöhnlichen Anlässe bestehen (§ 4 (3) Abs. 2). Die Testate sind vom Auftragnehmer maximal einmal jährlich zu aktualisieren.
3. Falls der Auftragnehmer nach § 4 (2) keine aktuellen Nachweise vorlegen kann, kann der Auftraggeber die Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit beim Auftragnehmer zu dessen üblichen Geschäftszeiten einmal jährlich stichprobenartig kontrollieren, soweit

keine Anhaltspunkte für einen Verstoß des Auftragnehmers gegen die Weisungen des Auftraggebers oder gegen diesen AV-Vertrag vorliegen.

Im Übrigen kann der Auftraggeber die vorgenannten Kontrollen jederzeit durchführen, wenn bestimmte Anhaltspunkte für einen Verstoß des Auftragnehmers gegen die Weisungen des Auftraggebers bestehen oder dafür, dass der Auftraggeber gegen diesen AV-Vertrag verstoßen hat.

4. Die Kontrollen nach § 4 (2) und (3) werden vom Auftraggeber – sofern keine Anhaltspunkte eine frühere Kontrolle notwendig machen - mindestens 21 Tage im Voraus angekündigt und hinsichtlich des Gegenstands und des Umfangs mit dem Auftragnehmer abgestimmt.
5. Zur Ausführung der Kontrollen nach § 4 (3) wird der Auftragnehmer dem Auftraggeber insbesondere Zugang zu den Datenverarbeitungsanlagen gewähren, die für die Datenverarbeitung nach diesem AV-Vertrag bestimmt sind.
6. Zur Kontrolle nach § 4 (3) seitens des Auftraggebers sind – soweit vorhanden - dessen Datenschutzbeauftragter oder vom Auftraggeber bestellte neutrale IT-Sachverständige befugt, soweit diese strafbewehrt erklären, die berechtigten Geheimhaltungs- und Datenschutzinteressen des Auftragnehmers und dessen weitere Kunden zu wahren.
7. Der Auftragnehmer ist verpflichtet, der für den Auftraggeber zuständigen Datenschutzbehörde im gesetzlich erforderlichen Umfang Zugang zu seinen Geschäftsräumen und Aufzeichnungen über die Datenverarbeitung für den Auftraggeber zu gewähren. Für den Fall, dass behördliche Kontrollen durch den Auftraggeber veranlasst sind, wird dieser dem Auftragnehmer den durch die Kontrollen entstehenden Aufwand ersetzen.

§ 5 Grundsätze der technisch-organisatorische Maßnahmen

1. Die technischen und organisatorischen Maßnahmen gemäß § 32 DSGVO werden in Abstimmung mit dem Auftraggeber ergriffen (Anhang 1).
2. Diese Maßnahmen (Anhang 1) unterliegen dem technischen Fortschritt und dürfen vom Auftragnehmer durch andere adäquate Maßnahmen ersetzt werden, soweit damit das ursprüngliche Sicherheitsniveau nicht unterschritten wird. Der Auftragnehmer wird

solche Ersetzungen dokumentieren und dem Auftraggeber auf schriftliche Anfrage zur Verfügung stellen.

3. Der Datenschutzbeauftragte des Auftragnehmers ist in Anhang 1 hinterlegt. Er kann einseitig durch den Auftragnehmer geändert werden. Sollten sich dadurch die Kontaktdaten des Datenschutzbeauftragten ändern, wird der Auftragnehmer dies dem Auftraggeber mitteilen.

§ 6 Einschaltung von Subunternehmern

1. Allgemeine Genehmigung

Der Auftragnehmer ist allgemein berechtigt, in seinem Ermessen Subunternehmern zur Leistungserbringung für diesen AV-Vertrag einzuschalten, soweit diese über geeignete technische und organisatorische Maßnahmen verfügen, sowie den Anforderungen von Art. 28 Abs. 4 S. 1, Abs. 3 DSGVO genügen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Subunternehmer sind in Anhang 2 aufgeführt und gelten als genehmigt.

2. Beauftragung von Subunternehmern

Der Auftragnehmer stellt sicher, dass jeder eingesetzte Subunternehmer durch Vertrag oder ein anderes Rechtsinstrument mindestens denselben Datenschutzpflichten unterliegt, die dem Auftragnehmer nach diesem AV-Vertrag obliegen, soweit diese für die vom Subunternehmer erbrachten Leistungen relevant sind. Insbesondere stellt der Auftragnehmer sicher, dass der Subunternehmer geeignete technische und organisatorische Maßnahmen gemäß den Anforderungen der DSGVO trifft. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Subunternehmers nach Maßgabe von Art. 28 Abs. 4 DSGVO verantwortlich.

3. Änderungen und Widerspruchsrecht

Der Auftragnehmer informiert den Auftraggeber rechtzeitig im Voraus über die beabsichtigte Hinzuziehung neuer oder die Ersetzung bestehender Subunternehmer. Der Auftraggeber kann einer solchen Änderung innerhalb von vier (4) Wochen nach Zugang der Information in Textform aus berechtigten datenschutzrechtlichen Gründen im Sinne des Art. 28 Abs. 2 S. 2 DSGVO widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Änderung als genehmigt.

4. Drittlandsübermittlungen

Soweit der Einsatz eines Subunternehmers mit einer Übermittlung personenbezogener Daten

in ein Drittland im Sinne von Kapitel V DSGVO verbunden ist, stellt der Auftragnehmer sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden. Soweit erforderlich, können hierzu insbesondere die von der Europäischen Kommission gemäß Art. 46 Abs. 2 DSGVO erlassenen Standardvertragsklauseln abgeschlossen werden.

4. Kontrollrechte des Auftraggebers

Der Auftragnehmer stellt dem Auftraggeber auf begründete Anfrage die zur Überprüfung der Einhaltung der vorstehenden Verpflichtungen erforderlichen Informationen über die eingesetzten Subunternehmer gem. Art. 28 Abs. 3 h) DSGVO zur Verfügung.

§ 7 Berichtigung, Löschung und Sperrung von Daten

1. Die im Auftrag des Auftraggebers erhobenen, verarbeiteten und genutzten Daten wird der Auftragnehmer nur nach Weisung des Auftraggebers berichtigen, löschen oder sperren, wenn berechnete Interessen des Auftragnehmers dem nicht entgegenstehen. Wenn sich ein Betroffener zu diesem Zweck direkt an den Auftragnehmer wendet, hat dieser ein solches Ersuchen unverzüglich an den Auftraggeber weiterzuleiten.
2. Der Ansprechpartner des Auftraggebers wird das Ersuchen nach § 7 (1) S. 2 unverzüglich prüfen und dem Auftragnehmer schriftlich mitteilen, ob es berechnete war oder nicht und den Auftragnehmer anweisen, die Berichtigung, Löschung oder Sperrung vorzunehmen.
3. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder wie in Anhang 1 beschrieben zu löschen. Der Auftraggeber hat die Entscheidung hierüber spätestens bei der Kündigungserklärung - oder im Fall von Laufzeitverträgen min. 6 Wochen vor Laufzeitende – in Textform anzuzeigen.

§ 8 Sonstige Bestimmungen

1. Bei Widersprüchen zwischen diesem AV-Vertrag und seinen Anhängen gehen die Regelungen dieses AV-Vertrags vor.
2. Der ausschließliche Gerichtsstand und Leistungsort für diesen AV-Vertrag ist Augsburg.

3. Sollten einzelne Bestimmungen dieses AV-Vertrags unwirksam oder lückenhaft sein, so bleiben die übrigen Bestimmungen wirksam. Sollten zur Ausfüllung lückenhafter oder unwirksamer Bestimmungen mehrere gesetzliche Bestimmungen alternativ zur Anwendung kommen können, so gilt jene gesetzliche Bestimmung, die dem wirtschaftlichen Willen der Parteien am nächsten kommt.

Anhänge:

- 1 - Technisch-organisatorische Maßnahmen
- 2 – Subunternehmer

Anhang 1 - Technisch-organisatorische Maßnahmen

Datenschutzbeauftragter des Auftragnehmers:

DataCo GmbH
Sandstraße 33
80335 München
Deutschland
www.dataguard.de

A. Pseudonymisierungs- und Verschlüsselungsmaßnahmen

Siehe Ziff.

- B.2 Punkt 3
- B.4. Punkte 3 und 4
- B.7. Punkt 3

B. Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer

1. Zutrittskontrolle, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet und genutzt werden, verwehrt:
 - Die Geschäftsräume des Auftragnehmers werden nach Dienstschluss abgesperrt.
 - Es existiert eine protokollierte Schlüsselvergabe der Schlüssel für die Geschäftsräume des Kunden.
2. Zugangskontrolle, die es verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:
 - Der Auftragnehmer unterhält schriftliche Regelungen für die Nutzung von Datenträgern und Notebooks seiner Arbeitnehmer.
 - Der Auftragnehmer überprüft die schriftlichen Regelungen für die Nutzung von Datenträgern und Notebooks seiner Arbeitnehmer.
 - Die Dateisysteme von Xentral sind verschlüsselt mit FileVault MacOS.
3. Zugriffskontrolle, die sicherstellt, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können:
 - Der Zugriff auf die verarbeiteten Daten in Xentral erfolgen auf Grundlage des Need-to-know-Prinzips.
 - Der Auftragnehmer protokolliert die Datenverarbeitung in Xentral.
 - Der Auftragnehmer überprüft regelmäßig die Einrichtung des Berechtigungskonzepts.
4. Weitergabekontrolle, mit der dafür gesorgt wird, 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 welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:
 - Der Datenaustausch im Rahmen von Xentral wird verschlüsselt mit FileVault MacOS.
 - Der Datenaustausch über Xentral wird im Webserver des Auftragnehmers protokolliert.
 - Daten auf physikalischen Datenträgern des Auftraggebers beim Auftragnehmer werden digitalisiert, verschlüsselt und anschließend verbleibende Datenträger vernichtet.
 - Datenfernzugriffe des Auftragnehmer werden nach Verschlüsselungsverfahren des Auftraggebers durchgeführt oder nach SSH-Standard des Auftragnehmers.
5. Eingabekontrolle, mit deren Hilfe nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
 - Datenverarbeitungsvorgänge in Xentral werden durch den Auftragnehmer protokolliert.
6. Auftragskontrolle, die dafür sorgt, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
 - Der Auftraggeber und seine Mitarbeiter werden durch die ihm überlassenen

Zugangsdaten für das Ticket-Center für Xentral identifiziert.

7. Verfügbarkeitskontrolle, d.h. es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:
 - Virenkontrolle für eingehende Dateien per Mail
 - Der Auftragnehmer unterhält ein Firewall-Konzept
 - Der Auftragnehmer führt regelmäßige Datensicherungen durch; Datensicherungen werden verschlüsselt gelagert.
8. Trennungskontrolle, die sicherstellt, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:
 - Es erfolgt eine Trennung per individuellen und passwortgeschützten Zugang durch die Xentral-Instanz des Kunden, auf die der Auftragnehmer Zugang erhält.
 - Es besteht eine Trennung zwischen Entwicklungs-, Test- und Produktivsystem von Xentral.

C. Maßnahmen zur Verfügbarkeit der personenbezogenen Daten und um den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Siehe Ziff. B.7. Punkt 3

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

- jährliches Datenschutzaudit durch unabhängige Datenschutzorganisation
- formalisierte Prozesse für Datenschutzvorfälle
- Weisungen des Auftraggebers werden dokumentiert

Anhang 2 – Subunternehmer

Subunternehmer	Kontaktdaten	Tätigkeit
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxemburg	Hosting, Infrastructure/Plattform/Software as a Service (zusammen "SaaS")
Intercom R&D Unlimited Company	124 St Stephen's Green Dublin 2, D02 C628 Irland	Support-Ticket-System
Planhat AB	c/o WeWork, Regeringsgatan 29, 111 53 Stockholm, Schweden	Onboarding/Support-System