Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Im Rahmen der Leistungserbringung nach dem zwischen dem Kunden („**Auftraggeber**“) und der Thomas-Krenn.AG („**Auftragnehmer**“, Auftraggeber und Auftragnehmer im Folgenden auch einzeln als „**Partei**“ und gemeinsam als „**Parteien**“ bezeichnet) bestehenden Vertrag über exone.Cloud-Leistungen (nachfolgend „**Hauptvertrag**“) kann es erforderlich sein, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Daten**“ oder „**Auftraggeber-Daten**“). Diese Vereinbarung zur Auftragsverarbeitung (nachfolgend „**AV-Vertrag**“) konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers und eingeschalteter weiterer Auftragsverarbeiter als Subunternehmer mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Gegenstand der Datenverarbeitung nach diesem AV-Vertrag sind die Auftraggeber-Daten, wenn und soweit sie personenbezogene Daten enthalten.

1.2 Der Zweck der Datenverarbeitung im Rahmen dieses AV-Vertrags ist die Bereitstellung von Leistungen nach dem Hauptvertrag.

1.3 Die Art der Verarbeitung ist die Speicherung und Verarbeitung der Daten, wenn und soweit dies zur Erbringung der Leistungen erforderlich ist, die im Hauptvertrag näher beschrieben sind.

1.4 Es werden die Auftraggeber-Daten verarbeitet, die der Auftraggeber auf Grundlage des Hauptvertrags in der exone.Cloud speichert.

1.5 Zu den betroffenen Personen können gehören: Kunden, Mitarbeiter, Lieferanten und Endkunden.

1.6 Die Laufzeit dieses AV-Vertrags richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieses AV-Vertrags nicht darüber hinausgehende Verpflichtungen ergeben.

1.7 Die Erhebung, Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt.

2 Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Die Tätigkeiten sind im Hauptvertrag konkretisiert.

2.2 Der Auftraggeber ist im Rahmen des Hauptvertrags für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein Verantwortlicher im datenschutzrechtlichen Sinn.

2.3 Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

3 Anwendungsbereich und Verantwortlichkeit

3.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Die Weisungen des Auftraggebers sind abschließend im Hauptvertrag und in den Bestimmungen dieses AV-Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses AV-Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und sind zu dokumentieren. Sofern erforderlich, ist die Übernahme von Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln.

3.3 Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Meinung ist, eine Weisung verstoße gegen diesen AV-Vertrag oder gegen geltende Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

4 Sicherheit der Verarbeitung

4.1 Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers ergreifen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind.

4.2 Die vom Auftragnehmer insoweit getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO sind in **Anlage 1** zu dieser Vereinbarung dokumentiert.

4.3 Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrags zu ändern, etwa aufgrund von technischem Fortschritt und Weiterentwicklung, solange sie weiterhin den gesetzlichen Anforderungen genügen. Der Auftragnehmer wird insoweit das vertraglich vereinbarte Schutzniveau nicht unterschreiten und alternative adäquate Maßnahmen umzusetzen. Wesentliche Änderungen sind zu dokumentieren.

5 Mitteilungs- und Unterstützungspflichten des Auftragnehmers

5.1 Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber unverzüglich über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.

5.2 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und

sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

5.3 Der vom Auftragnehmer mit der Administration der exone.Cloud zugrundeliegenden IT-Systeme beauftragte weitere Auftragsverarbeiter setzt bei der Durchführung von Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen sowie zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

5.4 Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt, der seine Tätigkeit gemäß Art. 37, 38 DSGVO ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme auf Anforderung mitgeteilt.

5.5 Für sonstige Unterstützungsleistungen, die nicht Gegenstand der Leistung sind oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

6 Löschung und Rückgabe von personenbezogenen Daten

6.1 Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen.

6.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

7 Verantwortlichkeit des Auftraggebers

7.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrags Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

7.2 Der Auftraggeber hat den Auftragnehmer bei der Feststellung von Fehlern oder Unregelmäßigkeiten, die er insbesondere bei der Prüfung von Auftragsergebnissen feststellt, unverzüglich und vollständig zu informieren.

7.3 Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftraggeber den Auftragnehmer bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

7.4 Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

7.5 Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

8 Verantwortlichkeit des Auftraggebers

8.1 Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte der betroffener Personen nachzukommen.

8.2 Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

9 Nachweise und Kontrolle

9.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer die Auftragskontrolle durchzuführen oder durch einen zu benennenden Prüfer durchführen zu lassen, sofern letzterer nicht in einem Wettbewerbsverhältnis mit dem Auftragnehmer steht. Auf Anforderung wird der Auftragnehmer dem Auftraggeber alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen, unter anderem durch die Vorlage eines der folgenden Dokumente: (i) die Ergebnisse eines Selbstaudits, (ii) Zertifikate über Datenschutz und/oder Informationssicherheit (z.B. ISO 27001) oder (iii) andere geeignete Zertifikate oder Dokumente im Rahmen einer IT-Sicherheits- oder Datenschutzüberprüfung (nachfolgend insgesamt "**Berichte**"). Der Auftraggeber wird die Berichte als vertrauliche Informationen des Auftragnehmers behandeln.

9.2 Der Auftraggeber hat das Recht, die Einhaltung dieses AV-Vertrags durch den Auftragnehmer selbst zu überprüfen, wenn er nach billigem Ermessen der Ansicht ist, dass die im vorherigen Absatz beschriebene Auftragskontrolle anhand von Berichten im Einzelfall nicht ausreichen oder wenn eine zuständige Datenschutzbehörde eine solche Prüfung verlangt. Wann immer dies nach vernünftigen Ermessen möglich ist, wird der Auftraggeber dabei auch weiterhin versuchen, von der im vorherigen Absatz beschriebenen Auftragskontrolle anhand von Berichten Gebrauch zu machen, bevor er eine Vor-Ort-Prüfung durchführt. Eine solche Prüfung wird während der normalen Geschäftszeiten ohne Unterbrechung des Geschäftsbetriebs des Auftragnehmers unter Berücksichtigung einer angemessenen Vorlaufzeit und einer rechtzeitigen vorherigen Anmeldung von mindestens dreißig (30) Tage durchgeführt, es sei denn, es besteht dringender Bedarf an einer früheren Prüfung. Der Auftragnehmer kann die Auftragskontrolle von der Unterzeichnung einer Vertraulichkeitsvereinbarung abhängig machen.

9.3 Der Auftraggeber wird seine Prüfungsrechte nicht häufiger als einmal innerhalb eines Zeitraums von zwölf (12) Monaten ausüben, es sei denn, (i) dies ist auf Anweisung einer Aufsichtsbehörde erforderlich oder (ii) der Auftraggeber ist der Ansicht, dass eine weitere Prüfung aufgrund einer Verletzung oder einer vermuteten Sicherheitsverletzung des Auftragnehmers erforderlich ist. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

9.4 Der Auftraggeber trägt seine eigenen Kosten im Rahmen der Auftragskontrolle. Der Auftraggeber erstattet dem Auftragnehmer (nach den zu dem Zeitpunkt geltenden Sätzen des Auftragnehmers) diejenigen Kosten, die durch die Bereitstellung interner Ressourcen für die Durchführung der Prüfung entstanden sind, es sei denn, die Prüfung ergibt, dass der Auftragnehmer seine Verpflichtungen aus diesem AV-Vertrag verletzt hat.

10 Subunternehmer/Unterauftragsverhältnisse

10.1 Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere sorgfältig ausgewählte Drittunternehmern hinsichtlich der Verarbeitung von Auftraggeber-Daten als Unterauftragsverarbeiter hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen Auftragsverarbeiter und weiteren Auftragsverarbeiter ergeben sich aus **Anlage 2** und gelten als genehmigt.

10.2 Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen AV-Vertrag mit einer Frist von 3 Monaten zu kündigen.

10.3 Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter ist so zu gestalten, dass sie den in diesem AV-Vertrag zwischen Auftragnehmer und Auftraggeber enthaltenen Datenschutzanforderungen und den Vorgaben der DSGVO entsprechen.

10.4 Der Auftragnehmer bleibt für die Erfüllung der Verpflichtungen, Dienstleistungen und Funktionen, die von einem seiner Subunternehmer übernommen werden, im selben Umfang verantwortlich, als wenn er die Verpflichtungen, Leistungen und Funktionen selbst erfüllen würde. Durch die Beauftragung des Subunternehmers wird der Auftragnehmer nicht von der Haftung gemäß diesem AV-Vertrag befreit.

11 Haftung

11.1 Für die Haftung des Auftragnehmers nach diesem AV-Vertrag gelten die Haftungsausschlüsse und -begrenzungen des Hauptvertrags. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diese Vereinbarung oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

11.2 Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

12 Schlussbestimmungen

12.1 Änderungen und Ergänzungen dieses AV-Vertrags und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann und eines ausdrücklichen Hinweises bedarf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

12.2 Bei etwaigen Widersprüchen zwischen diesem AV-Vertrag und dem Hauptvertrag gehen Regelungen dieses AV-Vertrags vor.

12.3 Sollten einzelne Bestimmungen dieses AV-Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

Anlage 1: Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO zur exone.Cloud

Anlage 2: Subunternehmer / weitere Auftragsverarbeiter

Anlage 1

Dokumentation der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO zur exone.Cloud

1. Gewährleistung der Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1.1 Zutrittskontrolle

Der Zutritt zum Rechenzentrum ist nur einem eingeschränkten Kreis von autorisierten Personen möglich.

1.1.1. Organisatorische Maßnahmen

Das Rechenzentrumsgebäude ist von außen neutral und nicht als Rechenzentrum erkenntlich. Der genaue Standort des Rechenzentrums ist nicht öffentlich bekannt. Externe Personen ohne besondere Sicherheitsfreigabe erhalten nur Zutritt in ständiger Begleitung eines internen Mitarbeiters, der durch seine Zutrittskarte entsprechende Berechtigungen in die jeweiligen Bereiche erhält. Jeder Zutritt wird in dem RZ-Logbuch festgehalten. Sollten Personen das Rechenzentrum betreten, die in Begleitung einer zutrittsberechtigten Person Zugang zum Rechenzentrum erhalten, so sind diese gesondert im Logbuch festzuhalten und vorher anzumelden. Die Identifizierung der Personen ist vorab durch einen gültigen amtlichen Lichtbildausweis festzustellen. Durch das installierte Zutrittskontrollsystem können nur Personen n das Rechenzentrum, die im Vorfeld entsprechende Berechtigungen erhalten haben. Die Zutrittsberechtigungen werden in einem zentralen System eingerichtet und verwaltet. Hierfür existiert ein formaler Genehmigungsprozess. Der Zutritt zum Rechenzentrum erfolgt über einen neutralen Transponder in Form einer Zutrittskarte oder einem Schlüsselanhänger, der eine Zuordnung zur Funktion nicht verdeutlicht. Der Transponder ist mithilfe einer AES256 Verschlüsselung gegen Kopieren geschützt. Die Vergabe der Zutrittskarten/-anhänger wird dokumentiert. Bei Verlust des Zutrittsmediums wird dieses sofort über das Zentrale System gesperrt. Die Berechtigungen können unabhängig davon, wo sich der Transponder befindet, geändert, gelöscht oder gesperrt werden.

1.1.2. Technische Maßnahmen

Das Rechenzentrum wird durch folgende technische Maßnahmen vor unberechtigtem Zutritt geschützt:

- Zutrittskontrollsystem
- Einbruchmeldeanlage
- Videokameras
- Sicherheitstüren

Der Standort des Rechenzentrums verfügt über Zugangsleser an allen Außen- und sicherheitsrelevanten Türen. Alle Zugänge sind videoüberwacht; die Videoüberwachung wird durch eine zentrale Anlage gesteuert. Die Aufzeichnungen werden über einen Zeitraum von 6 Monaten gespeichert. Zutritt erfolgt je nach Sicherheitsklassifizierung am Zugangsleser über eine zwei Faktor oder drei Faktor Authentifizierung (Transponder mit PIN oder Transponder mit wechselnder PIN alle 60 Sekunden). Beim Verlassen der letzten anwesenden Person wird die Einbruchmeldeanlage automatisch scharf geschaltet. Die Videoüberwachungsanlage setzt moderne Analysemethoden (wie z.B. Gesichtserkennung, verdächtiges Verhalten, ... ein), um entsprechend proaktiv Alarme auslösen zu können.

1.2. Zugangskontrolle

Folgende technische und organisatorische Maßnahmen zur Benutzeridentifikation und Authentifizierung sind vorhanden:

Aufgrund des im Unternehmen geltenden Berechtigungskonzeptes wurde ein formaler Prozess eingerichtet. Ausschließlich auf der Grundlage dieses Prozesses werden Zugänge zum Datenverarbeitungssystem eingeräumt. Berechtigungen werden bei Verlassen des Unternehmens gesperrt. Gleiches gilt, sobald die Berechtigung nicht mehr benötigt wird bzw. bei missbräuchlicher und unberechtigter Verwendung. Die Zugangsberechtigungen sind so konfiguriert, dass Personen lediglich in den vorher definierten Bereichen Zugang zur Datenverarbeitung haben; Benutzerrechte werden eindeutig zugeordnet. Jeder Fernzugriff auf interne Systeme ist nur in authentifizierter Form möglich.

Im Einzelnen wurden folgende Maßnahmen getroffen:

- Einrichten einer formalen Benutzerverwaltung
- Nur bei uns registrierte Kunden erhalten einen Benutzerzugriff
- Einsatz eines Virtuellen privaten Netzwerkes (VPN)
- Verschlüsselungstechnik bei schutzbedürftigen Daten entsprechend dem aktuellen Stand der Technik
- Protokollierung der Besucher des Rechenzentrums
- Sorgfältige Auswahl des Reinigungspersonals

1.3. Zugriffskontrolle

Es wird gewährleistet, dass ein Zugriff ausschließlich auf die der Zugriffsberechtigung unterliegenden Daten erfolgt und dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten nach ihrer Speicherung stattfindet.

Die Zugriffsbefugnisse werden entsprechend dem Berechtigungskonzept erstellt und kontrolliert. Der Zugreifende wird identifiziert. Zugriffe auf Anwendungen (insbesondere bei der Eingabe, Änderung und Löschung der Daten) sowie Missbrauchsversuche werden protokolliert. Die Protokolle werden regelmäßig ausgewertet. Für die Protokollierung steht ein zentraler Server zur Verfügung, auf den lediglich autorisierte Administratoren lesenden Zugriff erhalten. Auffällige Zugriffsversuche lösen einen Alarm aus, der an die verantwortliche Stelle gesendet wird.

Passwörter werden nach aktuellem Stand der Technik und des Sicherheitsstandards generisch erzwungen.

Ist eine Änderung der Zugriffsberechtigung erforderlich, wird diese ausschließlich von hierfür bestimmten Administratoren vorgenommen. Dabei wird nach dem Mehraugenprinzip verfahren, so dass jeweils Rücksprache mit einer weiteren zuständigen Person (ggf. einem Vorgesetzten) erfolgt. Lediglich ausgewählte Mitarbeiter erhalten administrative Rechte, die für einzelne Netzbereiche zugewiesen werden. Die entsprechende Beschränkung des Zugriffs wird durch die Konfiguration des Systems erzwungen. Benutzerberechtigungen, deren Grundlage entfallen ist, werden umgehend gelöscht; dies erfolgt auch automatisiert im Rahmen der Systemdiagnose.

Datenträger werden sicher aufbewahrt und vor ihrer Wiederverwendung physisch gelöscht. Eine ordnungsgemäße Vernichtung nicht mehr benötigter Datenträger ist gesichert, die verantwortlichen Personen werden jeweils eingewiesen. Die Vernichtung wird protokolliert.

1.4. Trennungskontrolle

Es wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Mandantentrennung wird softwareseitig durchgeführt; auch die Zugriffsregelung gewährleistet die erforderliche Trennung. Test- und Routineprogramme werden getrennt; Gleiches gilt für Test- und Produktivdaten; durch Netzwerksegmentierung werden Entwicklungssysteme technisch getrennt Dateiseparierung ist vorhanden; Kopien von Produktivdaten werden nicht zu Testzwecken verwendet.

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

2.1. Weitergabekontrolle

Es wird gewährleistet, dass die Weitergabe personenbezogener Daten durch Einrichtungen der Datenübertragung überprüft- und nachvollziehbar ist und der Zugriff Unbefugter auf dem Transportweg verhindert wird. Hierzu wird eine Übersicht angelegt, die erkennen lässt, an welchen Stellen, während welcher Zeitspannen, welche personenbezogenen Daten durch Übertragungseinrichtungen übermittelt werden. Diese Übersicht wird ständig aktualisiert. Dokumentiert werden auch die Abruf- und Übermittlungsprogramme, die Übermittlungswege (soweit das Übermittlungsverfahren dies zulässt) und -stellen sowie die entsprechende Übermittlungs-Hardware. Es erfolgt eine Protokollierung der Abruf- und Übermittlungsaktivitäten.

Daten werden generell nur auf eigenen Systemen innerhalb Deutschlands gespeichert. Grundsätzlich können auf die Systeme, die personenbezogene Daten verarbeiten, nur autorisierte Nutzer zugreifen. Alle personenbezogenen Daten werden in kennwortgeschützten Datenbanken gespeichert.

Verlassen die Daten beim Transport über Dateitransfer das separierte Netz des Rechenzentrums, werden zusätzlich SSL/TLS-, IPSec oder VPN-Verbindungen verwendet. Ausgenommen hiervon ist die Korrespondenz per E-Mail zur Auftragsbearbeitung, die unverschlüsselt stattfindet.

Der Zugriffsschutz auf Systeme mit sensiblen Informationen wird auf mehreren Ebenen realisiert: Auf Dateisystem-, auf Betriebssystem- und auf Netzwerkebene.

Der Zugriff und die Aktivitäten der Administratoren werden in speziellen Protokolldateien aufgezeichnet.

Die Protokollierung der Zugriffe erfolgt auf einem zentralen, dedizierten Protokollierungsserver, der von den zu protokollierenden Systemen getrennt installiert ist.

2.2. Eingabekontrolle

Der Auftragnehmer ist in der Lage, nachträglich festzustellen und zu überprüfen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Details zur Protokollierung wurden unter Ziff. 4.1 beschrieben. Es existieren Datenerfassungsanweisungen. Die Berechtigungen zur Eingabe, Änderung und Löschung von Daten sind dokumentiert. Protokollauswertungen werden regelmäßig von den Systemadministratoren vorgenommen, dabei wird ein festgelegtes Auswertungsverfahren für die automatisiert erstellten Protokolldaten angewandt.

2.3. Auftragskontrolle

Mitarbeiter des weiteren Auftragsverarbeiters werden ausschließlich auf Anweisung der Vorgesetzten im Rahmen der Auftragsverarbeitung tätig. Ein Datenschutzbeauftragter ist bestellt. Die Einzelheiten der Auftragskontrolle sind im Übrigen im AV-Vertrag zwischen Auftraggeber und Auftragnehmer geregelt.

2.4 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. Die getroffenen technischen Maßnahmen ermöglichen den Betroffenen eine einfache Ausübung des Widerrufsrechts.

3. Fähigkeit der Verfügbarkeit und Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DSGVO)

Zum Schutz gegen die zufällige Zerstörung oder den Verlust von Daten werden Firewalls sowie ein Virenschutz installiert, der Hackerangriffe abwehrt.

Alle sensiblen und kritischen Systeme sind mit einem fehlertoleranten Festplattenverbund (i.d.R. RAID5 oder höher) ausgestattet. Zusätzlich ist jedes Rack mit mindestens drei unabhängigen Phasen angebunden. Jedes kritische System besitzt redundante Netzteile zur Stromversorgung. Die Stromversorgung wird durch USV und Netzersatzanlagen (Dieselgenerator) gesichert. Die Daten werden täglich gesichert. Ein Backup- und Recoverykonzept wurde erstellt.

Die Verantwortlichkeit im Falle eines Notfalls wurde festgelegt und kommuniziert. Die schriftlichen Anleitungen für den Notfall bestimmen die erforderlichen Abläufe im Einzelnen (insbesondere die Informationswege und die Weiterleitung des Alarms an die zuständigen Stellen sowie die im Notfall zwingend vorgesehenen Handlungsschritte).

Um einen Brandfall im Vorfeld zu verhindern, werden kritische Bereiche mit einer Brandfrüherkennungsanlage überwacht; Feuerlöschgeräte sind vorhanden. Die Serverräume enthalten die zur Messung von Temperatur und Feuchtigkeit erforderlichen Geräte.

4. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die Verantwortlichkeit im Falle eines Notfalls wurde festgelegt und kommuniziert. Schriftliche Anleitungen für den Notfall bestimmen die erforderlichen Abläufe im Einzelnen (insbesondere die Informationswege und die Weiterleitung des Alarms an die zuständigen Stellen sowie die im Notfall zwingend vorgesehenen Handlungsschritte). Die Vorgehensweise zum Umgang mit Sicherheitsvorfällen ist dokumentiert. Es gibt einen formalen Prozess, der die Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen festlegt.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO

Ein Datenschutzmanagement wurde eingerichtet. Durch interne Audits findet regelmäßig eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung statt.

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

6.1. Technische Maßnahmen

Im Fall der Pseudonymisierung findet die Trennung der Zuordnungsdaten und die Aufbewahrung in einem getrennten, abgesicherten System (verschlüsselt) statt.

6.2. Organisatorische Maßnahmen

Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf einer gesetzlichen Löschfrist zu anonymisieren / pseudonymisieren.

7. Verschlüsselung (Art. 32 Abs. 1 lit. b DSGVO) – Technische Maßnahmen

- Sensible personenbezogene Daten werden verschlüsselt übertragen
- Externer Zugang nur über sichere Verschlüsselte Verbindung möglich (VPN oder vergleichbar)
- Verschlüsselte Speicherung von User-Passwörter
- Verschlüsseltes WLAN nach aktuellem Standard
- Verschlüsselung mobiler Datenträger (z.B. Notebooks, Smartphones, usw.)
- Verschlüsselung sensibler Daten

Anlage 2

Subunternehmer / weitere Auftragsverarbeiter

Unternehmen	Anschrift/Land	Leistung
EXTRA Computer GmbH	Brühlstrasse 12 89537 Giengen-Sachsenhausen Deutschland	Betreiber der Veeam-Storage-Lösung und eines Backup-Servers am Unternehmens-standort in Deutschland
Server-Ware GmbH (weiterer Auftrags-verarbeiter der EXTRA Computer GmbH)	Hafenbad 11 89073 Ulm Deutschland	Betrieb und Wartung der Cloud-Plattform und der zugrundeliegenden IT-Systeme mit Serverstandort (Rechenzentrum) in Ulm/Deutschland; Bereitstellung der Netzwerkinfrastruktur