

AVV Anlage 2o -- Managed Hosting

Produktspezifische Anlage zum Rahmen-Auftragsverarbeitungsvertrag

1. Bezeichnung des Services

Managed Hosting (Stufen Basis und Business)

2. Gegenstand der Verarbeitung

Automatisierter Betrieb von **Ubuntu-Server-Instanzen (LTS)** im Rechenzentrum. Der Service wird ausschließlich für Serverinstanzen erbracht, die über den Auftragnehmer bezogen werden; vom Auftraggeber beigestellte Instanzen sind nicht Gegenstand des Services. Der Auftragnehmer hält die verwalteten Systeme über eine zentrale Konfigurationsverwaltung in einem definierten, gehärteten Sollzustand, spielt Betriebssystem- und Sicherheitsaktualisierungen ein, erkennt Abweichungen vom Sollzustand automatisiert und überwacht die Systeme. In der Stufe **Business** erbringt der Auftragnehmer zusätzlich eine **dateibasierte Datensicherung** der vom Auftraggeber festgelegten Datenbestände in ein außerhalb des Rechenzentrums der gesicherten Instanz gelegenes Speicherziel.

Abgrenzung zur Bereitstellung der Infrastruktur: Die Bereitstellung der Serverinstanz und der Rechenzentrumsinfrastruktur ist nicht Gegenstand dieser Anlage; hierfür gilt die produktspezifische Anlage 2 -- Hosting. Der dort geführte Rechenzentrumsbetreiber ist zusätzlich in Abschnitt 9 dieser Anlage aufgeführt, weil die verwalteten Inhaltsdaten auf seiner Infrastruktur liegen. **Da der Service ausschließlich für über den Auftragnehmer bezogene Instanzen erbracht wird, ist die Verarbeitungskette vollständig in dieser Anlage und der Anlage 2 -- Hosting abgebildet.**

Umfang des Zugriffs auf Inhaltsdaten:

- a) In der Stufe **Basis** besteht kein zweckgerichteter Zugriff auf die auf dem System gespeicherten Inhaltsdaten. Ein Zugriff ist jedoch technisch nicht ausgeschlossen, weil der Auftragnehmer über einen administrativen Verwaltungszugang zum Betriebssystem verfügt, der für die Erbringung der Betriebsleistungen erforderlich ist.
- b) In der Stufe **Business** werden die im Sicherungsumfang enthaltenen Inhaltsdaten **zweckgerichtet verarbeitet**: sie werden gelesen, verschlüsselt, übertragen, im Speicherziel gespeichert, für die vereinbarte Aufbewahrungsdauer vorgehalten und auf Anforderung wiederhergestellt. Der Sicherungsumfang wird vom Auftraggeber festgelegt.

Im Übrigen verarbeitet der Auftragnehmer Bestands- und Kontaktdaten der Ansprechpartner, Zugangs- und Authentifizierungsdaten der verwalteten Systeme, technische Metadaten (insbesondere Hostnamen, IP-Adressen, Paket-, Konfigurations- und Härtingsstände), Protokoll-, Überwachungs- und Ereignisdaten der verwalteten Systeme sowie Ticket- und Kommunikationsdaten.

Dauer der Verarbeitung: für die Laufzeit des Servicevertrags; anschließend nach Maßgabe des Abschnitts 8 und des §10 des Rahmen-AVV.

3. Zweck der Verarbeitung

Betrieb, Härtung, Aktualisierung, Konfigurationsverwaltung und Überwachung der verwalteten Serverinstanzen. Erkennung und Rückführung von Abweichungen vom vereinbarten Sollzustand. In der Stufe Business zusätzlich: Erstellung, Übertragung, Speicherung, Aufbewahrung, Kontrolle und

Wiederherstellung von Datensicherungen sowie die Durchführung dokumentierter Wiederherstellungstests. Erfüllung der vertraglichen und gesetzlichen Pflichten des Auftragnehmers.

Eine Auswertung der Inhaltsdaten zu anderen Zwecken, eine Profilbildung oder eine automatisierte Entscheidungsfindung findet nicht statt. Eine Auswertung der Sicherungsdaten über die zur Erbringung der Sicherungs-, Kontroll- und Wiederherstellungsleistung erforderlichen Verarbeitungsschritte hinaus erfolgt nicht.

4. Kategorien personenbezogener Daten

- Bestands- und Kontaktdaten der Ansprechpartner des Auftraggebers (Name, Funktion, dienstliche E-Mail-Adresse, dienstliche Telefonnummer, Firmenanschrift)
- Zugangs- und Authentifizierungsdaten der verwalteten Systeme (Benutzerkennungen, Schlüsselmaterial der administrativen Zugänge, Zugänge zur Konfigurationsverwaltung, zur Überwachung und zur Sicherungslösung)
- Technische Metadaten der verwalteten Systeme (Hostnamen, IP-Adressen, Betriebssystem- und Paketstände, Konfigurations- und Härtingsstände, Zuordnung des Systems zum Auftraggeber, Inventardaten)
- Betriebssystem-Benutzerkonten der verwalteten Systeme einschließlich Rechtezuweisungen
- Protokoll-, Überwachungs- und Ereignisdaten (Systemprotokolle, Anmeldeereignisse, Dienststatus, Ressourcenauslastung, Ergebnisse der Konfigurations- und Härtingläufe, Ergebnisse der Abweichungserkennung, sicherheitsrelevante Ereignisse)
- Ergebnisse und Protokolle der Sicherungsläufe sowie der Wiederherstellungstests (Stufe Business)
- Ticket-, Störungs- und Kommunikationsdaten einschließlich der vom Auftraggeber übermittelten Angaben
- **Stufe Business:** Inhaltsdaten aus dem vom Auftraggeber festgelegten Sicherungsumfang -- insbesondere Dateien, Verzeichnisse, Datenbankauszüge und Anwendungsdaten -- einschließlich der darin enthaltenen personenbezogenen Daten
- **Stufe Basis:** Inhaltsdaten auf dem verwalteten System -- nicht zweckgerichtet verarbeitet, ein Zugriff über den administrativen Verwaltungszugang ist jedoch technisch nicht ausgeschlossen (siehe Abschnitt 2)

Besondere Kategorien (Art. 9 DSGVO): Nicht Gegenstand der beauftragten Verarbeitung. Legt der Auftraggeber in der Stufe Business Datenbestände in den Sicherungsumfang, die Daten besonderer Kategorien enthalten, werden diese im Rahmen der Sicherung mitverarbeitet. Der Auftraggeber ist verpflichtet, den Auftragnehmer hierauf vor Einrichtung der Sicherung hinzuweisen, damit die erforderlichen zusätzlichen Schutzmaßnahmen nach Art. 32 DSGVO vereinbart werden können. Die Verantwortung für die Zulässigkeit dieser Verarbeitung verbleibt beim Auftraggeber.

5. Kategorien betroffener Personen

- Beschäftigte und Ansprechpartner des Auftraggebers (technische Kontakte, Eskalationskontakte, Melder von Störungen)
- Inhaber administrativer Benutzerkonten auf den verwalteten Systemen
- Mittelbar: Personen, deren personenbezogene Daten der Auftraggeber auf den verwalteten Systemen verarbeitet und -- in der Stufe Business -- in den Sicherungsumfang aufnimmt (insbesondere Beschäftigte, Kunden, Interessenten, Lieferanten und Nutzer des Auftraggebers)

6. Art der Verarbeitung

Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung und Veränderung (Konfigurations-, Härtings- und Aktualisierungsläufe auf den verwalteten Systemen), Auslesen, Abfragen, Verwendung, Übermittlung (an die Anbieter der Sicherungslösung und des Objektspeichers zum Zweck der Datensicherung sowie an den Rechenzentrumsbetreiber zum Zweck der Störungsbeseitigung), Abgleich, Einschränkung, Löschen und Vernichten.

In der Stufe Business zusätzlich: Vervielfältigung der Inhaltsdaten des Sicherungsumfangs zum Zweck der Datensicherung, verschlüsselte Übertragung, Speicherung im Objektspeicher, befristete Aufbewahrung sowie Wiederherstellung auf Anforderung des Auftraggebers.

Ein Auslesen der Inhaltsdaten auf den verwalteten Systemen außerhalb des Sicherungsvorgangs erfolgt ausschließlich auf dokumentierte Weisung des Auftraggebers im Einzelfall, insbesondere im Rahmen einer angeforderten Störungsanalyse.

7. Ort der Verarbeitung

Standort	Anbieter	Zweck
Deutschland (Hannover)	EXT IT GmbH	Administration und Steuerung der Konfigurationsverwaltung, der Überwachungs- und Verwaltungsplattform sowie der Sicherungslösung vom Arbeitsplatz aus; Störungsannahme; Abrechnung. Die Plattformen selbst werden auf der Infrastruktur gemäß nachfolgender Zeile betrieben
Deutschland (Rechenzentrum Düsseldorf)	WIIT AG (ehem. myLoc managed IT AG)	Physischer Betrieb der Serverinstanzen, auf denen der Service erbracht wird, sowie der Management-Infrastruktur des Auftragnehmers; Speicherung der Inhaltsdaten
Europäische Union	Xopero Software S.A.	Betrieb der Verwaltungsebene der Sicherungslösung (Steuerung der Sicherungsaufträge, Zeitpläne, Aufbewahrungsregeln, Protokolle und Ergebnisse der Sicherungsläufe)
Deutschland	Impossible Cloud GmbH	Speicherung der Sicherungsdaten im Objektspeicher (Stufe Business). Die Speicherregion wird bei der Einrichtung auf Deutschland festgelegt; der Anbieter setzt hierfür eine Beschränkung auf Länderebene ein.

Der konkrete Rechenzentrumsstandort der bereitgestellten Serverinstanz wird im jeweiligen Angebot bzw. Einzelauftrag ausgewiesen. Sämtliche Speicher- und Betriebsorte liegen in der Europäischen Union. Für Support-, Administrations- und Konzernfunktionen des Rechenzentrumsbetreibers ist eine Verarbeitung außerhalb der EU/des EWR derzeit nicht abschließend ausgeschlossen; insoweit gelten bis zur schriftlichen Bestätigung die Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914 als ergänzende Garantie (Einzelheiten in Abschnitt 9 und Anlage 3).

Eine Verlagerung der Speicherregion des Objektspeichers an einen Standort außerhalb Deutschlands erfolgt nicht ohne vorherige Mitteilung an den Auftraggeber in Textform; §6 Abs. 4 und 5 des Rahmen-AVV gelten entsprechend.

8. Aufbewahrungsdauer / Löschfristen

Datenkategorie	Aufbewahrungsdauer	Löschverfahren
Inhaltsdaten auf den verwalteten Systemen	Bis zum Ende des zugrunde liegenden Infrastrukturvertrags bzw. bis zur Rückgabe des	Bei Beendigung des Managed Hosting ohne Beendigung der Infrastruktur: Übergabe des Systems an den Auftraggeber, Entfernung der Verwaltungskomponenten, Löschung der Zugangsdaten beim Auftragnehmer. Bei Beendigung auch der Infrastruktur gilt die Anlage 2 -- Hosting.

	Systems an den Auftraggeber	
Sicherungsdaten im Objektspeicher (Stufe Business)	Gemäß der im Einzelauftrag vereinbarten Aufbewahrungsdauer; ohne abweichende Vereinbarung 30 Tage rollierend	Automatisierte rollierende Löschung nach Ablauf der Aufbewahrungsdauer. Bei Vertragsende: Der Auftraggeber übt sein Wahlrecht nach Art. 28 Abs. 3 lit. g DSGVO und §10 Abs. 1 des Rahmen-AVV möglichst vier (4) Wochen vor dem Beendigungstermin aus. Wählt er die Rückgabe, werden die Sicherungsdaten für mindestens 30 Kalendertage ab Vertragsende zum Abruf bereitgehalten und anschließend gelöscht. Wählt er die Löschung oder übt er sein Wahlrecht nicht aus, erfolgt die Löschung nach Ablauf dieses Zeitraums. §10 Abs. 1 bis 3 des Rahmen-AVV geht dieser Anlage im Konfliktfall vor.
Konfigurations- und Härtingsbeschreibungen des verwalteten Systems (versioniert)	Dauer der Beauftragung zzgl. 12 Monate zum Nachweis der erbrachten Leistung	Löschung der kundenbezogenen Konfigurationsstände nach Ablauf der Frist im turnusmäßigen Löschlauf
Zugangs- und Authentifizierungsdaten der verwalteten Systeme	Dauer der Beauftragung	Löschung aus dem Passwortmanagement des Auftragnehmers, Entfernung des Verwaltungszugangs vom System, Widerruf des Schlüsselmaterials
Technische Metadaten und Inventardaten	Dauer der Beauftragung	Löschung bei Vertragsende
Protokoll-, Überwachungs- und Ereignisdaten der verwalteten Systeme	90 Tage	Automatisierte rollierende Löschung
Ergebnisse der Konfigurations- und Abweichungsläufe	90 Tage	Automatisierte rollierende Löschung
Protokolle der Sicherungsläufe und Sicherungskontrollen (Stufe Business)	12 Monate	Automatisierte rollierende Löschung
Dokumentation der Wiederherstellungstests (Stufe Business)	Dauer der Beauftragung zzgl. 12 Monate	Turnusmäßiger Löschlauf
Ticket-, Störungs- und Kommunikationsdaten	24 Monate nach Abschluss des Vorgangs, längstens bis zum Ablauf gesetzlicher	Turnusmäßiger Löschlauf

	Aufbewahrungs- und Verjährungsfristen	
Bestands- und Vertragsdaten der Ansprechpartner	Dauer des Vertragsverhältnisses; anschließend nach Maßgabe der handels- und steuerrechtlichen Aufbewahrungspflichten (§ 147 AO, § 257 HGB)	Sperrung nach Vertragsende, Löschung nach Ablauf der Aufbewahrungsfristen

Ergänzend gilt §10 des Rahmen-AVV (Beendigung -- Löschung und Rückgabe).

Hinweis zu Löschbegehren betroffener Personen bei bestehenden Sicherungen: Eine Löschung einzelner Datensätze aus bereits erstellten Sicherungsständen ist technisch nicht möglich. Löschbegehren werden im produktiven Datenbestand umgesetzt; die betroffenen Daten entfallen in den Sicherungsständen mit Ablauf der vereinbarten Aufbewahrungsdauer. Bis dahin werden die Sicherungsstände im Sinne des Art. 18 DSGVO ausschließlich zu Wiederherstellungszwecken vorgehalten und nicht anderweitig verarbeitet. Der Auftragnehmer stellt sicher, dass gelöschte Daten bei einer Wiederherstellung nicht ungeprüft wieder in den produktiven Datenbestand gelangen, indem er den Auftraggeber vor jeder Wiederherstellung auf zwischenzeitlich umgesetzte Löschbegehren hinweist. Die Verantwortung für die anschließende erneute Löschung im produktiven Bestand trägt der Auftraggeber.

9. Eingesetzte Unterauftragsverarbeiter

Für diesen Service werden die folgenden **produktspezifischen** Unterauftragsverarbeiter eingesetzt:

Nr.	Firma	Sitz	Verarbeitungszweck	Drittlandtransfer	Garantien
Z6	WIIT AG (ehem. myLoc manage d IT AG)	Joachim-Erwin-Platz 3, 40212 Düsseldorf, Deutschland (EU), AG Düsseldorf HRB 99481; Rechenzentren am Standort Düsseldorf	Physischer Betrieb der Server-, Virtualisierungs-, Speicher- und Netzwerkinfrastruktur, auf der die verwalteten Serverinstanzen betrieben werden, sowie der Management-Infrastruktur des Auftragnehmers. Auf dieser Infrastruktur werden die Inhaltsdaten des Auftraggebers gespeichert.	Speicherung und Betrieb ausschließlich in Deutschland (EU). Für Support-, Administrations- und Konzernfunktionen ist eine Verarbeitung außerhalb der EU/des EWR derzeit nicht abschließend ausgeschlossen; der Auftragnehmer hat dies angefragt. Der Abschluss des Art.-28-Vertrags einschließlich der Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914 ist angefordert; bis dahin besteht insoweit keine vertragliche Transfergarantie, der Schutz stützt sich auf die Verschlüsselung der Datenträger mit ausschließlich beim Auftragnehmer verwalteten Schlüsseln.	Siehe Anlage 3

Z12	Xopero Software S.A.	ul. Herberta 3, 66-400 Gorzów Wielkopolski, Polen (EU)	Sicherungslösung (Stufe Business): Bereitstellung und Betrieb der Verwaltungsebene der Sicherungssoftware -- Steuerung der Sicherungsaufträge, Zeitpläne und Aufbewahrungsregeln, Protokollierung und Auswertung der Sicherungsergebnisse, Steuerung der Wiederherstellung. Verarbeitung von Metadaten der Sicherung (Dateinamen, Pfade, Größen, Zeitstempel, Sicherungsstatus).	Verarbeitung ausschließlich innerhalb der EU. Kein Drittlandtransfer.	ISO/IEC 27001, SOC 2 Type II (Anbieterangabe). Art.-28-Vertrag in Abschluss; aktueller Status siehe Anlage 3
Z13	Impossible Cloud GmbH	Friesenweg 12 (Haus 5), 22763 Hamburg, Deutschland (EU), AG Hamburg HRB 170423	Objektspeicher (Stufe Business): Speicherung, Vorhaltung und Bereitstellung der verschlüsselten Sicherungsdaten für die vereinbarte Aufbewahrungsdauer. Speicherregion Deutschland ; der Anbieter setzt eine Beschränkung der Speicherregion auf Länderebene ein.	Speicherung ausschließlich in Deutschland (EU). Kein Drittlandtransfer.	ISO/IEC 27001, SOC 2 Type II, PCI-DSS; Anforderungen des BSI-C5-Katalogs nach Anbieterangabe erfüllt. Art.-28-Vertrag in Abschluss; aktueller Status siehe Anlage 3

Verschlüsselung der Sicherungsdaten: Die Sicherungsdaten werden vor der Übertragung verschlüsselt und ausschließlich verschlüsselt im Objektspeicher abgelegt. Der Anbieter des Objektspeichers verarbeitet damit ausschließlich verschlüsselte Datenbestände; eine inhaltliche Kenntnisnahme ist ihm nicht möglich, solange die Schlüsselverwaltung beim Auftragnehmer liegt. Die Schlüsselverwaltung erfolgt beim Auftragnehmer nach Maßgabe der Anlage 1 (TOMs).

Weitere Auftragsverarbeiter der Unterauftragsverarbeiter: Die vorgenannten Unterauftragsverarbeiter setzen ihrerseits weitere Auftragsverarbeiter ein, insbesondere Betreiber der von ihnen genutzten Rechenzentren. Sie dürfen dies nur nach Maßgabe der jeweils mit dem Auftragnehmer geschlossenen Auftragsverarbeitungsverträge. Der Auftragnehmer hat namentliche Listen dieser weiteren Auftragsverarbeiter sowie die Zusicherung angefordert, über beabsichtigte Hinzuziehungen und Ersetzungen mindestens 30 Tage vorab informiert zu werden; er gibt diese Information nach §6 Abs. 4 des Rahmen-AVV an den Auftraggeber weiter. Bis zum Vorliegen dieser Zusicherung informiert der Auftragnehmer den Auftraggeber unverzüglich nach eigener Kenntniserlangung; §6 Abs. 5 des Rahmen-AVV (Sonderkündigungsrecht) gilt entsprechend. Die aktuellen Listen sind über den Auftragnehmer in Textform abrufbar.

Der unter Z6 genannte Unterauftragsverarbeiter ist zusätzlich in Abschnitt 3 der Anlage 3 als produktübergreifender Unterauftragsverarbeiter für den Betrieb der Management-Infrastruktur des Auftragnehmers geführt. Für den Service Managed Hosting gilt der vorstehend beschriebene, weitergehende Verarbeitungszweck.

Die vollständigen DPA-Details, Zertifizierungen und Garantien sind zentral in **Anlage 3** geführt. Ergänzend kommen die in Abschnitt 3 der Anlage 3 gelisteten produktübergreifenden Unterauftragsverarbeiter zum Einsatz.

Endpoint Security ist nicht Bestandteil dieses Services. Der für die Managed-Detection-and-Response-Leistungen eingesetzte Unterauftragsverarbeiter kommt bei Managed Hosting nicht zum Einsatz, solange der Auftraggeber die Zusatzleistung Endpoint Security nicht gesondert beauftragt. In diesem Fall gilt die dortige produktspezifische Anlage 2 zusätzlich.

10. Besondere Hinweise

- **Administrativer Verwaltungszugang:** Zur Erbringung des Services unterhält der Auftragnehmer einen dauerhaften administrativen Zugang zu den verwalteten Systemen. Dieser Zugang ermöglicht technisch die Kenntnisnahme aller auf dem System gespeicherten Daten. Der Zugang wird nach dem Least-Privilege-Prinzip eingerichtet, ist auf benannte Beschäftigte des Auftragnehmers beschränkt, wird durch Schlüsselmateriale und Mehr-Faktor-Authentifizierung abgesichert und ist protokolliert. Ein Zugriff auf Inhaltsdaten außerhalb des Sicherungsvorgangs erfolgt ausschließlich auf dokumentierte Weisung des Auftraggebers gemäß §4 Abs. 1 des Rahmen-AVV; derartige Zugriffe werden dokumentiert.
- **Automatisierte Veränderung der Systemkonfiguration:** Der Service verändert die Konfiguration der verwalteten Systeme automatisiert und wiederkehrend, um den vereinbarten Sollzustand herzustellen. Hiervon können auch Benutzerkonten, Rechtezuweisungen, Protokollierungseinstellungen und Zugriffsregeln erfasst sein. Der verwaltete Konfigurationsumfang wird beim Onboarding festgelegt und dokumentiert; er ist Bestandteil der Weisungslage nach §4 des Rahmen-AVV. Manuelle Änderungen des Auftraggebers innerhalb dieses Umfangs werden automatisiert zurückgeführt.
- **Zweckgerichtete Verarbeitung der Sicherungsdaten (Stufe Business):** Anders als bei der reinen Infrastrukturbereitstellung werden die Inhaltsdaten des Sicherungsumfangs vom Auftragnehmer zweckgerichtet verarbeitet. Der Auftraggeber legt den Sicherungsumfang fest und prüft in eigener Verantwortung, ob die Aufnahme bestimmter Datenbestände in die Sicherung sowie deren Aufbewahrungsdauer mit seinen datenschutzrechtlichen Pflichten -- insbesondere Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO und Löschpflichten -- vereinbar ist.
- **Grenzen der TOM-Verantwortung:** Die physische Sicherheit der Infrastruktur wird durch den Rechenzentrumsbetreiber, die Sicherheit des Objektspeichers durch dessen Anbieter erbracht. Der Auftragnehmer hat die Dokumentation der hierauf bezogenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO bei den jeweiligen Anbietern angefordert; bis zu deren Vorliegen stützt er sich auf deren Zertifizierungen (siehe Abschnitt 9) sowie auf die in Anlage 1 dokumentierten eigenen Maßnahmen. Nach Vorliegen prüft er die Dokumentation regelmäßig und stellt sie dem Auftraggeber auf Anforderung in Textform zur Verfügung. **Die Verantwortung des Auftragnehmers nach Art. 28 Abs. 4 Satz 2 DSGVO bleibt unberührt.** Die Sicherheit innerhalb der vom Auftraggeber betriebenen Anwendungen -- insbesondere Anwendungskonfiguration, Anwendungsbenutzer und Anwendungsdaten -- obliegt dem Auftraggeber.
- **Abgrenzung der Sicherungsleistung:** Die Datensicherung erfolgt auf Datei-Ebene und umfasst kein Abbild des Gesamtsystems. Die Wiederherstellung eines vollständig ausgefallenen Systems erfolgt zweistufig durch Neuaufbau aus der Konfigurationsverwaltung und anschließendes Rückspielen der gesicherten Daten. Der Auftraggeber ist verpflichtet, alle auf dem System betriebenen Datenbanken und vergleichbaren Anwendungen zu benennen, damit eine konsistente Sicherung eingerichtet werden kann. Für nicht benannte Anwendungen kann die Konsistenz des Sicherungsstands und damit die Wiederherstellbarkeit nicht gewährleistet werden.

- **Betroffenenrechte:** Der Auftragnehmer unterstützt den Auftraggeber gemäß §8 des Rahmen-AVV. In der Stufe Business kann er Auskunft darüber erteilen, ob und für welche Zeiträume Sicherungsstände eines benannten Datenbestands vorliegen, und einzelne Datenbestände auf Weisung wiederherstellen. Eine inhaltliche Suche nach personenbezogenen Daten einzelner betroffener Personen innerhalb der Sicherungsstände ist dem Auftragnehmer nicht möglich, da er die Struktur und Semantik der gesicherten Anwendungsdaten nicht kennt. Der Auftraggeber bleibt insoweit allein handlungsfähig. Zu Löschbegehren siehe Abschnitt 8.
- **Meldung von Sicherheitsvorfällen:** Der Auftragnehmer überwacht die verwalteten Systeme innerhalb des in der Leistungsbeschreibung festgelegten Umfangs und meldet erkannte Vorfälle nach Maßgabe des §7 des Rahmen-AVV. **Der Service umfasst keine Managed Detection and Response;** eine Erkennung gezielter Angriffe, von Schadsoftware oder von Kompromittierungen auf Anwendungsebene ist nicht geschuldet und kann durch die Überwachung nicht gewährleistet werden. Der Auftraggeber informiert den Auftragnehmer unverzüglich über ihm bekannt gewordene Vorfälle, die die verwalteten Systeme betreffen.
- **Fehlgeschlagene Sicherungen:** Der Auftragnehmer kontrolliert das Ergebnis der Sicherungsläufe arbeitstäglich innerhalb der Servicezeiten und meldet fehlgeschlagene Sicherungen dem Auftraggeber. Eine Überwachung und Reaktion außerhalb der Servicezeiten ist nicht Bestandteil des Services, soweit nicht gesondert vereinbart.
- **Verweigerter Neustart:** Erfordert eine Sicherheitsaktualisierung einen Neustart und verweigert der Auftraggeber diesen dauerhaft oder wird kein Wartungsfenster vereinbart, kann der vollständige Aktualisierungsstand der Systeme nicht gewährleistet werden. Der Auftragnehmer weist den Auftraggeber hierauf in Textform hin. Die Verantwortung für die daraus folgenden Risiken nach Art. 32 DSGVO geht insoweit auf den Auftraggeber über.
- **Weisungsbindung und Grenzen der Umsetzbarkeit:** Weisungen des Auftraggebers, die Eingriffe in die Infrastruktur des Rechenzentrumsbetreibers oder in die Plattformen der Sicherungs- und Speicheranbieter erfordern, kann der Auftragnehmer nur im Rahmen der ihm tatsächlich und vertraglich zur Verfügung stehenden Möglichkeiten umsetzen. Er unterrichtet den Auftraggeber unverzüglich, wenn eine Weisung aus diesen Gründen nicht oder nur eingeschränkt umsetzbar ist. §4 Abs. 5 des Rahmen-AVV bleibt unberührt.
- **Umfang der Sicherheitsaktualisierungen als Faktor nach Art. 32 DSGVO:** Die herstellerseitige Sicherheitswartung für Ubuntu LTS umfasst standardmäßig nur die Paketquelle „main“. Für Pakete aus der Paketquelle „universe“ besteht keine zugesicherte Wartung durch den Hersteller. Der Auftragnehmer spielt alle verfügbaren Sicherheitsaktualisierungen ein, kann Verfügbarkeit und Zeitpunkt für Pakete aus „universe“ jedoch nicht gewährleisten. Der Auftragnehmer weist den Auftraggeber hierauf hin; setzt der Auftraggeber solche Pakete für die Verarbeitung personenbezogener Daten ein, prüft er in eigener Verantwortung, ob eine erweiterte Sicherheitswartung nach Art. 32 DSGVO geboten ist.
- **Ablauf der LTS-Sicherheitswartung:** Ubuntu-LTS-Versionen erhalten fünf Jahre Sicherheitswartung. Der Auftragnehmer weist spätestens zwölf Monate vor Ablauf auf den erforderlichen Versionswechsel hin. Führt der Auftraggeber den Versionswechsel nicht durch, kann der Auftragnehmer den Sicherheitsstand nach Ablauf nicht mehr gewährleisten; die Verantwortung für die daraus folgenden Risiken nach Art. 32 DSGVO geht insoweit auf den Auftraggeber über.
- **Härtung ohne Zertifizierung:** Die Härtung erfolgt in Anlehnung an den CIS-Benchmark für Ubuntu Server (Level 1), umgesetzt über die Konfigurationsverwaltung des Auftragnehmers. Eine zertifizierte oder auditierte CIS-Konformität wird nicht geschuldet; ein Compliance-Nachweis nach CIS kann aus dieser Anlage nicht abgeleitet werden.

Änderungshistorie

Versio n	Datum	Änderung	Verantw ortlich
-------------	-------	----------	--------------------

1.3	2026-08-12	Interne Dokumentenprüfung vom 12.08.2026 eingearbeitet: Betrieb der Verwaltungsplattform in Abschnitt 7 richtig verortet (Düsseldorf statt Hannover). SCC-Angabe zu Z6 korrigiert – ohne Art.-28-Vertrag besteht keine vertragliche Transfergarantie.	Geschäftsführung
1.2	2026-08-01	Drittland-Aussage in Abschnitt 7 an die Z6-Einordnung angeglichen (Support-/Konzernfunktionen nicht abschließend ausgeschlossen, SCCs als ergänzende Garantie); DPA-Status zu Z12/Z13 wahrheitsgemäß als „in Abschluss“ ausgewiesen; TOM-Aussage zu Rechenzentrums- und Objektspeicher-Anbieter wahrheitsgemäß gefasst (Dokumentation angefordert)	Geschäftsführung
1.1	2026-07-31	Service auf Ubuntu Server (LTS) und auf über den Auftragnehmer bezogene Instanzen eingegrenzt; Passus zu beigestellten Instanzen entfallen, Verarbeitungskette damit geschlossen; Hinweise zum Umfang der Sicherheitsaktualisierungen, zum Ablauf der LTS-Wartung und zur Härtung ohne Zertifizierung ergänzt	Geschäftsführung
1.0	2026-07-31	Erstveröffentlichung	Geschäftsführung

Stand: 2026-08-12