Vereinbarung zur Auftragsverarbeitung

FluffOps GmbH und die im Auftragsblatt benannte verantwortliche Einrichtung

Avapingu | Art. 28 DSGVO | Version 2026-11-03.1 | Stand 3. November 2026

Prüffassung zur kundenbezogenen Vervollständigung

Auftragsblatt

Auftragsverarbeiter: FluffOps GmbH, Käferflugstraße 45, 74076 Heilbronn. Vertreten durch Geschäftsführer Jürgen Dorsch. Amtsgericht Stuttgart, HRB 807707. Datenschutzkontakt und Weisungsempfänger: Jürgen Dorsch, info@avapingu.de.

Verantwortliche Einrichtung und gegebenenfalls abweichender Rechtsträger:

Name und Anschrift: _____

_____

Vertretungsberechtigte Person:

Name, Funktion und Vertretungsgrundlage: _____

Weisungsberechtigte Person und dienstlicher Kontakt:

Name und E-Mail: _____

Kontakt für Datenschutzanliegen und Vorfälle, falls abweichend: _____

Datenschutzbeauftragte Person und Kontakt, soweit benannt: _____

Umfang und Dauer des Auftrags:

Einrichtung, Mandantenkennung und zugeordnete Geräte oder Einsätze: _____

Hauptvertrag / Bestellung / Hostingvereinbarung: _____

Beginn der Verarbeitung: _____ Ende oder Beendigungskriterium: _____

Bereitstellendes Medienzentrum oder sonstiger Dritter, falls vorhanden: _____

Die folgenden Vertragsbedingungen und Anlagen 1 bis 3 gehören gemeinsam zu dieser Vereinbarung. Die Angaben werden vor Abschluss vervollständigt; Kindernamen sind dafür nicht erforderlich. Beim elektronischen Abschluss kann ein entsprechend ausgefülltes Portal-Auftragsblatt diese Eintragsfelder ersetzen.

Die Vereinbarung ist kostenlos. Sie kann unmittelbar zwischen einer Schule oder einer anderen verantwortlichen Einrichtung und FluffOps geschlossen werden, auch wenn ein Medienzentrum das Gerät bereitstellt oder bezahlt. Sie überträgt keine Kauf-, Miet- oder Zahlungsverpflichtungen eines Dritten und ersetzt keine Verträge mit Jürgen Dorsch als Einzelunternehmer.

1 Vertragsgegenstand und Dauer

FluffOps verarbeitet personenbezogene Daten im Auftrag der verantwortlichen Einrichtung für die technische Bereitstellung und den Betrieb von Avapingu. Dazu gehören Anmeldung, Geräteverwaltung, Liveübertragung von Bild und Ton, Gerätesteuerung, weisungsgebundener Support sowie die notwendigen Betriebs-, Sicherheits- und Sicherungsvorgänge. Daten, betroffene Personen und Fristen sind in Anlage 1 beschrieben.

Die Vereinbarung wird mit ihrem Abschluss wirksam. Die Verarbeitung beginnt frühestens danach zu dem im Auftragsblatt festgelegten Zeitpunkt; eine vorbereitende personenbezogene Konto- oder Geräteeinrichtung ist eingeschlossen. Sie endet zum vereinbarten Enddatum oder mit der in Textform erklärten Beendigung des Verarbeitungsauftrags. Schutz-, Rückgabe- und Löschpflichten gelten bis zur Erledigung fort.

Die Verarbeitung durch FluffOps erfolgt innerhalb der EU beziehungsweise des EWR an den in Anlage 3 genannten Orten. Eine Verarbeitung außerhalb dieses Gebiets setzt eine vorherige dokumentierte Weisung oder Genehmigung und die Voraussetzungen des Kapitels V DSGVO voraus.

2 Verantwortung der Einrichtung

Die Einrichtung entscheidet über Zweck, Einsatzzeiten, Teilnehmer und Aufnahmebereich von Kamera und Mikrofon. Sie ist für die Rechtsgrundlage des Unterrichtseinsatzes, die Information der Betroffenen und gegebenenfalls erforderliche Einwilligungen verantwortlich. Bei möglichen Gesundheitsdaten berücksichtigt sie Artikel 9 DSGVO; sie prüft auch, ob eine Datenschutz-Folgenabschätzung erforderlich ist.

Käufer, Medienzentrum und datenschutzrechtlich verantwortliche Einrichtung können unterschiedlich sein. Eine Einladung oder Gerätebereitstellung begründet keine Vertretungsmacht für eine Schule. Handelt ein Medienzentrum selbst als Auftragsverarbeiter einer anderen Stelle, ist die Verarbeitungskette gesondert zu vereinbaren.

3 Weisungen

FluffOps verarbeitet Auftragsdaten ausschließlich auf dokumentierte Weisung der Einrichtung, auch hinsichtlich einer Drittlandübermittlung. Eine gesetzlich vorgeschriebene Verarbeitung bleibt vorbehalten; FluffOps informiert die Einrichtung vorab, soweit das betreffende Recht dies erlaubt. Eine Nutzung schulischer Auftragsdaten für eigene, nicht vom Auftrag gedeckte Zwecke ist ausgeschlossen. Dies umfasst auch Modelltraining, Fine-Tuning und sonstige Modellverbesserung.

Diese Vereinbarung enthält die anfänglichen Weisungen. Weitere Weisungen erteilen die im Auftragsblatt benannten Personen in Textform, insbesondere per dienstlicher E-Mail. Änderungen der Ansprechpartner werden unverzüglich mitgeteilt. Mündliche Notfallweisungen werden nachträglich dokumentiert. Beide Parteien halten erteilte Weisungen nachvollziehbar fest.

Hält FluffOps eine Weisung für datenschutzrechtswidrig, informiert FluffOps die Einrichtung unverzüglich und setzt die betroffene Ausführung bis zur Klärung aus. Offensichtlich rechtswidrige Weisungen werden nicht ausgeführt.

4 Vertraulichkeit und Sicherheit

FluffOps beschränkt den Datenzugriff auf befugte Personen und das für ihre Aufgabe Erforderliche. Diese Personen sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht; die Verpflichtung besteht nach Ende ihrer Tätigkeit fort.

FluffOps trifft geeignete technische und organisatorische Maßnahmen nach Artikel 32 DSGVO. Die vereinbarten Maßnahmen sind in Anlage 2 beschrieben und müssen vor der betroffenen Verarbeitung wirksam sein. Sie dürfen weiterentwickelt werden, ohne das vereinbarte Schutzniveau zu vermindern. Wesentliche Änderungen werden der Einrichtung rechtzeitig mitgeteilt.

5 Unterauftragsverarbeiter

Die Einrichtung genehmigt mit Abschluss die in Anlage 3 aufgeführten Unterauftragsverarbeiter. Für weitere Unterauftragsverarbeiter erteilt sie eine allgemeine Genehmigung nach Artikel 28 Absatz 2 DSGVO unter den folgenden Bedingungen.

FluffOps informiert mindestens 30 Tage vor einer Hinzunahme oder Ersetzung über Unternehmen, Leistung, Verarbeitungsort und wesentliche Schutzmaßnahmen. Die Einrichtung kann innerhalb dieser Frist aus begründeten Datenschutzgründen widersprechen. Bis zur Klärung werden ihre Daten nicht durch den neuen Dienstleister verarbeitet. Ist keine geeignete Lösung möglich, vereinbaren die Parteien die sichere Beendigung der betroffenen Verarbeitung.

FluffOps verpflichtet Unterauftragsverarbeiter vertraglich zu den einschlägigen Datenschutzpflichten dieser Vereinbarung und bleibt für deren Einhaltung gegenüber der Einrichtung verantwortlich. Die erforderlichen Vereinbarungen und Nachweise werden auf Anforderung in geeigneter Weise bereitgestellt.

6 Unterstützung und Betroffenenrechte

FluffOps unterstützt die Einrichtung angesichts der Art der Verarbeitung nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei Betroffenenrechten nach Artikeln 12 bis 22 DSGVO. Unter Berücksichtigung der Verarbeitung und der verfügbaren Informationen unterstützt FluffOps außerdem die Pflichten nach Artikeln 32 bis 36 DSGVO. Dies umfasst insbesondere Auskunft, Berichtigung, Löschung, Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsicht.

Direkt bei FluffOps eingehende Anträge Betroffener werden unverzüglich an die Einrichtung weitergeleitet. FluffOps beantwortet sie im Namen der Einrichtung nur auf deren Weisung. Informationen für deren Verzeichnis der Verarbeitungstätigkeiten werden im erforderlichen Umfang bereitgestellt.

7 Datenschutzverletzungen

FluffOps meldet der Einrichtung bekannt gewordene Verletzungen des Schutzes ihrer personenbezogenen Daten unverzüglich. Die Meldung enthält, soweit bekannt, Art und Umfang, betroffene Personen und Datenkategorien, wahrscheinliche Folgen, getroffene oder vorgeschlagene Abhilfemaßnahmen und einen Kontakt für Rückfragen. Fehlende Angaben werden ohne unangemessene Verzögerung ergänzt.

FluffOps sichert betroffene Daten, begrenzt mögliche Folgen und unterstützt Meldungen und Benachrichtigungen nach Artikeln 33 und 34 DSGVO. Die Entscheidung und Verantwortung dafür liegen bei der Einrichtung. Eine interne Untersuchung verzögert die Erstmeldung nicht.

8 Kontrolle und Nachweise

FluffOps stellt alle zur Prüfung der Pflichten aus Artikel 28 DSGVO erforderlichen Informationen bereit und ermöglicht Überprüfungen einschließlich Inspektionen durch die Einrichtung oder einen von ihr beauftragten Prüfer. Dazu gehören erforderliche Nachweise über Schutzmaßnahmen und Vertraulichkeitsverpflichtungen.

Termin und Ablauf werden angemessen abgestimmt; Vertraulichkeit, Betriebsabläufe und Daten anderer Auftraggeber werden geschützt. Diese Abstimmung darf notwendige Prüfungen, insbesondere bei einem begründeten Sicherheitsvorfall, nicht verhindern. Die Pflichten gegenüber zuständigen Aufsichtsbehörden bleiben unberührt.

9 Rückgabe und Löschung

Nach Auftragsende oder berechtigter Weisung gibt FluffOps die Auftragsdaten nach Wahl der Einrichtung zurück oder löscht sie. Auch bei Rückgabe löscht FluffOps die bei ihm verbleibenden Auftragsdaten und Kopien, soweit keine gesetzliche Speicherungspflicht besteht. Rückgabeumfang, geeignetes Format und sicherer Übermittlungsweg werden abgestimmt. Die Fristen in Anlage 1 gelten auch für betroffene Zugangs-, Versions- und Sicherungskopien. An schulischen Auftragsdaten besteht kein Zurückbehaltungsrecht wegen offener Zahlungsansprüche.

Während eines erforderlichen zeitversetzten Sicherungsablaufs sind die Daten zugriffsbeschränkt und werden nicht für andere Zwecke verwendet. Wird eine Sicherung wiederhergestellt, sind frühere Löschungen vor erneuter produktiver Nutzung nachzuvollziehen. Kopieren oder Wiederherstellen verlängert die Löschfrist nicht.

FluffOps bestätigt den Abschluss der Löschung einschließlich betroffener Kopien in Textform. Gesetzlich erforderliche Ausnahmen werden mit Grund, Umfang und Dauer benannt. Eigene Geschäftsbelege, etwa Rechnungen, werden getrennt aufbewahrt und erlauben keine längere Speicherung schulischer Auftragsdaten.

10 Haftung und Beendigung

Die Haftung richtet sich nach den gesetzlichen Vorschriften, insbesondere Artikel 82 DSGVO. Die Vereinbarung beschränkt keine gesetzlichen Rechte betroffener Personen. Es gilt deutsches Recht unter Beachtung des unmittelbar geltenden Unionsrechts. Es wird kein zusätzlicher Gerichtsstand vereinbart; die gesetzlichen Zuständigkeiten bleiben bestehen.

Bei einem erheblichen Datenschutzverstoß oder einer vertragswidrigen Verweigerung von Weisungen oder Kontrollen kann die Einrichtung den Verarbeitungsauftrag aus wichtigem Grund beenden. Die Beendigung dieser Vereinbarung ändert nicht automatisch Kauf-, Miet- oder Zahlungsvereinbarungen mit einem bereitstellenden Dritten. Die Pflichten nach Abschnitt 9 bleiben bestehen.

11 Vertragsabschluss

Die Parteien schließen die Vereinbarung schriftlich oder in einem dokumentierten elektronischen Format. Beim elektronischen Abschluss stellt FluffOps ein verbindliches Angebot mit vollständig ausgefülltem Auftragsblatt und identischen, versionierten Anlagen bereit. Mit Zugang der ausdrücklichen Annahmeerklärung der vertretungsberechtigten Person kommt der Vertrag zustande; eine weitere Gegenzeichnung ist dann nicht erforderlich. Die bloße Bereitstellung eines leeren Musters ist kein Angebot.

Der Abschlussnachweis hält Parteien, Vertretung, Vertrags- und Anlagenversion, Annahmeerklärung und Zeitpunkt fest; beim Portalabschluss zusätzlich Angebotskennung und Dokumentprüfsummen. Beide Parteien erhalten ein übereinstimmendes, dauerhaft speicherbares Exemplar. Alternativ unterzeichnen beide Parteien die vollständige Fassung einschließlich der Anlagen.

Diese Vereinbarung hat für die Auftragsverarbeitung Vorrang vor widersprechenden Leistungsbedingungen. Änderungen erfolgen in Textform oder einem dokumentierten elektronischen Format. Individuelle Vereinbarungen bleiben vorrangig; unwirksame Einzelbestimmungen berühren die übrige Vereinbarung nicht.

Für die verantwortliche Einrichtung

Name und Funktion: _____

Ort, Datum, Unterschrift: _____

Für die FluffOps GmbH

Jürgen Dorsch, Geschäftsführer

Ort, Datum, Unterschrift: _____

Anlage 1 Datenverarbeitung und Löschfristen

Zweck und betroffene Personen

Zweck ist die von der Einrichtung bestimmte Teilnahme am Unterricht mit einem Avapingu. Betroffen sein können zugeschaltete Schülerinnen und Schüler, Mitschülerinnen und Mitschüler, Lehrkräfte, weitere Personen im Aufnahmebereich oder am Teilnahmeort sowie berechtigte Schul- und Supportpersonen.

Die Verarbeitung umfasst Übermitteln und Bereitstellen von Live-Medien sowie Erheben, Speichern, Abfragen, Berichtigung und Löschung notwendiger Verwaltungs-, Geräte-, Zugangs- und Verbindungsdaten. Pseudonyme Kontokennungen werden bevorzugt; sie sind keine Anonymisierung.

Daten und Speicherorte

Vorgang	Daten und Umfang	Verarbeitung und Speicherung
Anmeldung und Verwaltung	Organisations- und Kontaktdaten, Kontokennungen, Rollen, Gerätezuordnung und Passwortprüfwerte	Plattform bei Hetzner in Nürnberg; asynchrone Datenbankreplikation nach Helsinki, Finnland
Livekommunikation	Bild, Ton, Verbindungs- und Steuerungsdaten	Verschlüsselt zwischen den Endgeräten; bei Bedarf über den eigenen Relay bei Hetzner in Falkenstein
Geräte und Zugangsverwahrung	Geräteauthentisierung, WLAN-Konfiguration und erforderliche wiederherstellbare Zugangsdaten	Gerät; geschützter Kundentresor in der eigenen Nextcloud bei Hetzner in Nürnberg; notwendige lokale Arbeitskopien
Betrieb und Support	IP-Adressen, Sitzungs-, Fehler- und Sicherheitsdaten sowie erforderliche Supportangaben	Plattform, Relay und geschützte auftragsbezogene Supportunterlagen

Eine serverseitige Aufzeichnung von Bild oder Ton gehört nicht zur Leistung. Externe Aufzeichnungen auf Teilnehmergeräten werden dadurch nicht technisch verhindert und sind durch die Einrichtung zu regeln. Diagnosen oder Behandlungsunterlagen werden für die Bereitstellung nicht benötigt. Der Einsatz bei erkrankten oder beeinträchtigten Kindern und Inhalte der Livekommunikation können dennoch Gesundheitsdaten oder andere besondere Datenkategorien nach Artikel 9 DSGVO erkennen lassen; sie unterliegen den vereinbarten Schutzmaßnahmen.

Anlage 1 (Fortsetzung): Löschfristen

Datenklasse	Frist
Personenbezogene Routine-, Verbindungs- und Nutzungsprotokolle	Höchstens 7 Tage ab Ereignis beziehungsweise Sitzungsende
Sicherheitsprotokolle	Höchstens 30 Tage ab Ereignis; erforderliche Beweissicherung eines konkreten Vorfalls gesondert und befristet
Aktive Auftragsdaten bei Auftragsende oder berechtigter Löschweisung	Ohne unnötigen Aufschub, spätestens innerhalb von 30 Tagen; kürzere Pflichten und Weisungen gehen vor
Betroffene Sicherungen und Versionen	Spätestens 35 Kalendertage nach der aktiven Löschung der jeweiligen Daten; umfasst auch Snapshots, Sonderkopien, Tresorhistorien, Dateiversionen, Papierkorb und lokale Sicherungen

Die 30 Tage sind keine Wartefrist. Bei Ausschöpfung beider Löschfenster kann die Entfernung letzter Sicherungskopien bis zu 65 Tage dauern. Ein zeitversetzter Sicherungsablauf setzt voraus, dass gleichzeitige gezielte Löschung technisch nicht möglich oder unverhältnismäßig ist und die Kopien bis dahin geschützt bleiben. Eine dokumentierte manuelle Ausführung ist zulässig; Kopieren oder Wiederherstellen beginnt keine neue Frist.

Anlage 2 Technische und organisatorische Maßnahmen

Die Maßnahmen gelten für den vereinbarten zentralen Avapingu-Betrieb. FluffOps überprüft ihre Wirksamkeit regelmäßig und nach wesentlichen Änderungen. Erforderliche weiterführende Nachweise werden nach Abschnitt 8 bereitgestellt.

Verschlüsselte Kommunikation

Anmeldung und Verwaltung nutzen HTTPS beziehungsweise WSS mit gültigen TLS-Zertifikaten. Bild und Ton werden durch WebRTC mit DTLS-SRTP verschlüsselt übertragen. Für den Verbindungsaufbau und erforderliches Relay werden die eigenen STUN-/TURN-Dienste auf der in Anlage 3 beschriebenen Infrastruktur verwendet. Es erfolgt keine serverseitige Medienaufzeichnung.

Zugriffsbegrenzung und Kontentrennung

Rollen und Mandantenprüfungen beschränken den Zugriff auf zugeordnete Konten und Geräte. Kundenverwaltung, Kinderzugang und privilegierte Administration haben unterschiedliche Berechtigungen. Der zentrale Superadmin-Zugang ist durch Zwei-Faktor-Anmeldung geschützt; notwendige Infrastrukturzugriffe sind auf befugte Personen beschränkt. Die Datenbank ist nicht öffentlich erreichbar.

Die Anwendung speichert Passwortprüfwerte mit Argon2. Für die geschützte Übergabe erforderliche wiederherstellbare Zugänge werden getrennt in verschlüsselten Kundentresoren verwahrt und nur befugten Personen zugänglich gemacht. Zugangsdaten werden geschützt übergeben; kompromittierte Zugänge werden gesperrt beziehungsweise erneuert. Sitzungscookies besitzen Schutzattribute und eine begrenzte Gültigkeit.

Support und Arbeitsplätze

Nach der technischen Geräteübergabe erfordern Herstellerzugriffe auf Bild und Ton sowie Gerätefernwartung eine widerrufbare Kundenfreigabe von höchstens 72 Stunden. Die Übergabe ist vor Unterrichtseinsatz abzuschließen. Zweckgebundene Serveradministration und Passwortzurücksetzungen bleiben getrennt: Der Superadmin darf Kunden-Adminpasswörter nach Berechtigungsprüfung protokolliert zurücksetzen; dafür sind weder Medienfreigabe noch Zugriff auf Unterrichtsinhalte nötig. Dies berechtigt nicht zur Teilnahme an Unterrichtskonferenzen.

Support erfolgt auf Weisung und nur im erforderlichen Umfang. Arbeitsplätze und lokale Auftragskopien werden gegen unbefugte Einsicht und Zugriff geschützt. Unterrichtsinhalte und Geheimnisse werden nicht in allgemein zugängliche Tickets oder Protokolle übernommen. Auch lokale Kopien unterliegen den vereinbarten Löschfristen.

Sicherung und Wiederherstellung

Regelmäßige geschützte Datenbank- und Serversicherungen dienen der Wiederherstellung nach Störungen. Die regulär erstellten Datenbanksicherungen sind verschlüsselt. Weitere Sicherungskopien unterliegen ebenfalls angemessenem Zugriffsschutz und den Fristen aus Anlage 1. Datenbankwiederherstellung, gezielte Rückgabe und Löschung werden geprüft. Vor produktiver Nutzung einer Rücksicherung sind frühere Löschungen erneut anzuwenden. Eine Vollverschlüsselung sämtlicher laufender Systeme wird damit nicht zugesagt.

Sicherer Betrieb und Organisation

Softwareänderungen werden geprüft und nachvollziehbar bereitgestellt. Schutzmaßnahmen gegen unberechtigte Netzwerkzugriffe und wiederholte Anmeldeversuche sowie zweckgebundene Betriebs- und Sicherheitsprotokollierung sind eingerichtet. Berechtigungen werden bedarfsbezogen vergeben und bei Wegfall entzogen. Befugte Personen sind zur Vertraulichkeit verpflichtet; Weisungen, Supportfreigaben, Datenschutzanfragen und Sicherheitsvorfälle werden nachvollziehbar bearbeitet.

Anlage 3 Unterauftragsverarbeiter und Standorte

Genehmigter Unterauftragsverarbeiter: Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland. Ein Auftragsverarbeitungsvertrag zwischen FluffOps GmbH und Hetzner ist abgeschlossen.

Leistung	Betroffene Daten	Standort
Hosting der Plattform und der selbst betriebenen Nextcloud	Konten-, Geräte-, Verwaltungs-, Betriebs-, Zugangs- und Sicherungsdaten	Nürnberg, Deutschland
Infrastruktur für den eigenen STUN-/TURN-Dienst	Verbindungsmetadaten und beim Relay verschlüsselte Medienpakete	Falkenstein, Deutschland
Cloud-Backups und Snapshots der genannten Server	Darin enthaltene Auftragsdaten	Backups am Ursprungsstandort; Snapshots innerhalb der europäischen Netzwerkzone in Deutschland oder Finnland
Datenbank-Replikation; Abgleich von Dateien und Software	Replizierte Konten-, Geräte-, Verwaltungs- und Betriebsdaten; abgeglichene Serverdateien einschließlich Konfiguration und Zertifikaten	Helsinki, Finnland (Hetzner)

Für die aufgeführten Hetzner-Leistungen bleibt Abschnitt 5 maßgeblich. Daneben besteht seit November 2026 eine zusätzliche verschlüsselte Sicherung bei Scaleway in Paris. Ihr technischer Umfang und die noch offenen vertraglichen Nachweise sind im nachstehenden Prüfhinweis getrennt ausgewiesen; sie wird dadurch nicht als bereits genehmigter Unterauftragsverarbeiter behandelt.

Die Verarbeitung auf Geräten der Einrichtung beziehungsweise der Teilnehmer erfolgt unter Verantwortung der Einrichtung. Technische Begleitverbindungen, etwa für Namensauflösung, Zertifikate oder Softwareaktualisierung, sind von der Unterrichtsübertragung zu unterscheiden. Soweit dabei personenbezogene Auftragsdaten an zusätzliche Empfänger oder in Drittländer übermittelt werden, berücksichtigt FluffOps sie vor Einsatz nach den Abschnitten 1 und 5. Die Standortangaben sind keine pauschale Aussage über jede Internetverbindung eines Teilnehmergeräts.

Für rein kaufmännische Vorgänge wie Rechnungen ist FluffOps selbst verantwortlich. Deren Dienste erhalten dadurch keine Berechtigung, schulische Auftragsdaten für andere Zwecke zu verarbeiten.

Technischer Änderungs- und Prüfhinweis

Stand 3. November 2026 · zur Prüffassung 2026-11-03.1. Dieser Hinweis dokumentiert den technischen Iststand und offene Nachweise. Er erteilt keine zusätzliche Genehmigung nach Abschnitt 5 und ändert keine Vertragsbedingungen oder Löschfristen.

Helsinki: Die PostgreSQL-Datenbank wird asynchron auf einen Ersatzserver bei Hetzner repliziert. Serverdateien und Softwarestände werden zusätzlich periodisch abgeglichen. Dies ist eine laufende Replikation beziehungsweise ein Datei-/Softwareabgleich und kein bloßer Cloud-Snapshot. Die Statusprüfung vom 3. November bestätigt eine frische Replikation. Eine automatische Umschaltung, ein verlustfreier Wiederanlauf oder eine bestimmte Wiederherstellungsdauer sind damit nicht nachgewiesen oder zugesagt.

Zusätzliche Sicherung in Paris: Ein täglicher Sicherungslauf überträgt vor dem Upload mit age verschlüsselte PostgreSQL-Dumps sowie ausgewählte Laufzeit-, Serverdatei-/Konfigurations-, Zertifikats- und Softwareimage-Archive zu Scaleway (Region Paris, Frankreich). Darin können personenbezogene Auftragsdaten enthalten sein. Diese Sicherung ist von der laufenden Helsinki-Replikation und von Hetzner-Backups beziehungsweise Snapshots zu unterscheiden. Der Sicherungslauf vom 3. November 2026 wurde als geprüft abgeschlossen gemeldet; dies ist kein vollständiger Wiederanlaufnachweis.

Offene vertragliche Prüfung: Ein abgeschlossener Auftragsverarbeitungsvertrag mit Scaleway und die konkrete Erfüllung des Informations-/Genehmigungsverfahrens nach Abschnitt 5 sind in den geprüften Unterlagen noch nicht belegt. Scaleway wird hier als tatsächlich verwendeter Sicherungsdienst benannt, nicht der Liste bereits genehmigter Unterauftragsverarbeiter hinzugefügt. Diese Lücke ist vor einem Vertragsabschluss beziehungsweise einer entsprechenden Einsatzfreigabe zu klären; die technische Nutzung allein ersetzt die erforderlichen Nachweise nicht.

Offener Lösch- und Kopiennachweis: Die konfigurierte Scaleway-Aufbewahrung beträgt 30 Tage für aktuelle Objekte, einen Tag für nichtaktuelle Versionen nach deren Statuswechsel und einen Tag für abgebrochene mehrteilige Uploads; hinzu kommt eine siebentägige Governance-Aufbewahrungssperre. Das beweist für sich allein nicht die Einhaltung der vereinbarten Fristen für jede Kopie. Für Helsinki-Erfolgsstände und sämtliche betroffenen Sicherungs-/Dateiversionen ist der vollständige Löschablauf einschließlich Nachweis noch zu verifizieren. Die Fristen in Anlage 1 bleiben unverändert; Kopieren oder Wiederherstellen setzt sie nicht neu in Gang.