

Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO

Anlage 2 zum Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Verantwortlich: Thomas Wiebe, Benediktusplatz 22, 52076 Aachen, hello@podsink.com Dienst: podsink
Version 1.10, Stand: 19. September 2026

0. Vorbemerkung

Dieses Dokument beschreibt die Maßnahmen, die der Auftragnehmer zum Schutz der im Auftrag verarbeiteten Daten getroffen hat. Es beschreibt den tatsächlichen Zustand. Maßnahmen, die nicht umgesetzt sind, stehen mit ihrer Begründung in Abschnitt 6, nicht in den Abschnitten davor.

Der Auftragnehmer ist ein Einzelunternehmen ohne Beschäftigte. Alle im Folgenden genannten Tätigkeiten führt der Auftragnehmer selbst aus; wo von "Zugriff" die Rede ist, gibt es genau eine zugriffsberechtigte Person.

Verarbeitungsumgebung

Ebene	Beschreibung
Anwendungsserver	Gemietete virtuelle Server der Hetzner Online GmbH, Rechenzentren innerhalb der EU. Betrieb in Containern, Administration ausschließlich durch den Auftragnehmer.
Objektspeicher	OVH GmbH (OVHcloud), Rechenzentren innerhalb der EU. Speicherung der Aufnahmen und der zugehörigen Archivmetadaten für die Dauer der Aufbewahrungsfrist.
Medienserver (SFU)	Auf derselben gemieteten Infrastruktur. Leitet Live-Audio und -Video zwischen Teilnehmenden weiter, ohne zu speichern.
Endgerät des Auftragnehmers	Verschlüsseltes Notebook. Administrativer Zugang; Auftragsdaten nur anlassbezogen und zeitlich begrenzt (siehe 2.3).

Die Protokoll- und Metrikverarbeitung des Auftragnehmers läuft getrennt von den Anwendungsservern und ausschließlich unter seiner eigenen Administration (siehe 4.4), derzeit auf eigener Hardware. Sie betrifft ausschließlich Daten, für die der Auftragnehmer selbst Verantwortlicher ist, nicht die Aufnahmeinhalte; Kennungen und Ereignisse sind in 4.4 beschrieben.

1. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a)

1.1 Verschlüsselung bei der Übertragung

- Sämtlicher Datenverkehr zwischen Browser und Server läuft über HTTPS mit TLS. Die Terminierung erfolgt auf einem vorgelagerten Reverse Proxy, HTTP-Anfragen werden auf HTTPS umgeleitet.

- Der Reverse Proxy setzt HTTP Strict Transport Security mit einer Laufzeit von einem Jahr einschließlich aller Subdomains. Ein Browser, der die Seite einmal über HTTPS geladen hat, stellt danach keine unverschlüsselte Anfrage mehr an sie; ein Herabstufen auf HTTP durch Dritte auf dem Übertragungsweg wird damit unterbunden.
- Die DNS-Zone der Domain trägt einen CAA-Eintrag, der die Ausstellung von Zertifikaten auf Let's Encrypt beschränkt und an das ACME-Konto des Auftragnehmers bindet, Wildcard-Zertifikate ausschließt und Meldungen über Ausstellungsversuche an den Auftragnehmer leitet.
- Der Upload der Aufnahmeabschnitte und die WebSocket-Verbindung für die Steuerung laufen über dieselbe verschlüsselte Verbindung.
- Live-Audio und -Video werden über WebRTC transportverschlüsselt übertragen (DTLS-SRTP). Der Medienserver entschlüsselt die Ströme, um sie zwischen den Teilnehmenden weiterzuleiten, und speichert sie nicht. Eine Ende-zu-Ende-Verschlüsselung zwischen den Teilnehmenden besteht nicht.
- Die Verbindung zum Objektspeicher, zum Abrechnungsanbieter und der Versand von E-Mails laufen ausschließlich über TLS.

1.2 Verschlüsselung bei der Speicherung

- Das Endgerät des Auftragnehmers ist vollständig verschlüsselt.
- Die Protokoll- und Metrikdaten (Abschnitt 4.4) liegen auf einer verschlüsselten Partition; das Betriebssystem dieser Server ist nicht verschlüsselt. Der Schlüssel liegt ausschließlich beim Auftragnehmer und ist auf dem Server nicht gespeichert.
- Die Aufnahmen im Objektspeicher werden mit einem Schlüssel verschlüsselt, den ausschließlich der Auftragnehmer vorhält und den der Anbieter nicht speichert (serverseitige Verschlüsselung mit kundeneigenem Schlüssel). Ohne diesen Schlüssel gibt der Objektspeicher die Aufnahmen nicht heraus.
- Die Verschlüsselung im Objektspeicher wirkt gegen den Anbieter des Objektspeichers und gegen einen Abfluss aus dem Objektspeicher. Sie wirkt nicht gegen den Auftragnehmer selbst, der die Aufnahmen zum Zusammensetzen und Ausliefern entschlüsseln muss; ein Schutz gegen den Auftragnehmer wäre nur durch Ende-zu-Ende-Verschlüsselung erreichbar, die es nach 1.1 nicht gibt. Der Schutz gegenüber dem Auftragnehmer beruht auf der Weisungsbindung nach § 4 des Vertrages.
- Das Schlüsselmaterial wird zusätzlich unabhängig von den Servern in einem verschlüsselten Passwortspeicher verwahrt, sodass es einen Verlust der Server und ihrer Momentaufnahmen übersteht.
- Die Datenträger der gemieteten Anwendungsserver sind nicht zusätzlich durch den Auftragnehmer verschlüsselt. Der Schutz beruht dort auf der physischen Sicherheit der Rechenzentren des Anbieters (Abschnitt 2.1) und auf der kurzen Aufbewahrungsfrist der Aufnahmedaten. Ist im Hauptvertrag eine längere Aufbewahrungsfrist vereinbart, trägt dieses zweite Element entsprechend weniger; der Auftragnehmer weist darauf bei der Vereinbarung hin. Siehe Abschnitt 6.

1.3 Pseudonymisierung

- Teilnehmende ohne Nutzerkonto werden ausschließlich über einen selbst gewählten Anzeigenamen und eine zufällige Kennung geführt. Eine Registrierung findet nicht statt.

- Wer über einen Zuhörlink zuhört, wird nicht identifiziert: kein Konto, keine Cookies, keine dauerhaften Kennungen.
 - Interne Kennungen für Sitzungen, Aufnahmen und Spuren sind zufällig erzeugt und lassen keinen Rückschluss auf Personen zu.
-

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b)

2.1 Zutrittskontrolle

Der Zutritt zu den Räumen, in denen Auftragsdaten verarbeitet werden, liegt vollständig bei den Unterauftragsverarbeitern. Beide betreiben nach ISO 27001 zertifizierte Rechenzentren mit Zutrittskontrolle, Videoüberwachung und Alarmanlagen; die jeweils aktuellen Zertifikate stellt der Auftragnehmer auf Anfrage zur Verfügung. Der Auftragnehmer selbst hat keinen physischen Zutritt zu dieser Hardware.

Das Endgerät des Auftragnehmers wird in privaten Räumen genutzt und ist bei Nichtbenutzung gesperrt.

2.2 Zugangskontrolle (Schutz vor unbefugter Systemnutzung)

Für Nutzende des Dienstes:

- Die Anmeldung erfolgt ohne Passwort über einen zeitlich begrenzten Anmeldelink an die hinterlegte E-Mail-Adresse oder über einen registrierten Sicherheitsschlüssel (WebAuthn). Es werden keine Passwörter gespeichert, also können auch keine entwendet werden.
- Anmeldesitzungen laufen nach 30 Tagen ab. Das Sitzungs-Cookie ist HttpOnly, SameSite=Strict und wird nur über HTTPS übertragen.
- Die Anmelde-Endpunkte sind pro IP-Adresse mengenmäßig begrenzt.
- Der Sitzungslink trägt eine zufällig erzeugte Kennung von 12 Zeichen aus einem Alphabet von 36 Zeichen (rund 62 Bit) aus einem kryptographisch sicheren Zufallsgenerator; sie enthält keine fortlaufenden, zeitlichen oder auf Personen bezogenen Bestandteile. Kennungen von Sitzungen und Zuhörlinks werden in den Zugriffs- und Betriebsprotokollen geführt; diese liegen ausschließlich in der in 4.4 beschriebenen Umgebung und werden nach 4.5 gelöscht. Der Dienst zeigt den Sitzungslink und den Zuhörlink ausschließlich dem Host; die Weitergabe an die Teilnehmenden liegt beim Host. Der Host sieht jede beigetretene Person in der Teilnehmerliste und kann die Sitzung jederzeit beenden. Nach dem Ende der Sitzung lehnt der Dienst den Beitritt über den Sitzungslink ab.
- Das Live-Zuhören ist bei einer laufenden Sitzung ausgeschaltet, bis der Host es einschaltet. Erst dann erzeugt der Dienst einen eigenen Zuhörlink mit 16 Zeichen über demselben Alphabet (rund 82 Bit), der vom Sitzungslink unabhängig ist. Schaltet der Host das Live-Zuhören aus oder endet die Sitzung, wird der Link ungültig. Auf Wunsch des Auftraggebers wird das Live-Zuhören für sein Konto abgeschaltet; ein Host kann es dann nicht einschalten.
- Fehlversuche beim Aufruf eines Sitzungs- oder Zuhörlinks, also Aufrufe mit einer unbekannten oder ungültig gewordenen Kennung, sind pro IP-Adresse mengenmäßig begrenzt. Erfolgreiche Aufrufe unterliegen keiner Begrenzung.

Für den Auftragnehmer:

- Ein Paketfilter vor den Servern gibt nach außen nur die für den Betrieb des Dienstes erforderlichen Zugänge frei. Der Verwaltungszugang ist öffentlich nicht erreichbar; die Administration erfolgt ausschließlich über ein verschlüsseltes privates Netz.
- Der Zugang zu den Servern erfolgt über SSH mit Public-Key-Authentifizierung. Die Anmeldung mit Passwort ist deaktiviert.
- Alle Anbieterkonten (Serverhosting, Objektspeicher, Abrechnungsanbieter, Domainverwaltung) sind mit Zwei-Faktor-Authentifizierung gesichert. Zugangsdaten werden in einem Passwortmanager verwaltet.
- Der Quellcode liegt bei keinem Anbieter: Das Repository läuft auf eigener Hardware in den Räumen des Auftragnehmers, auf einem verschlüsselten Datenträger. Auftragsdaten sind darin nicht enthalten.
- Es gibt keine weitere Person mit Zugang zu Servern oder Anbieterkonten.

2.3 Zugriffskontrolle (Schutz vor unbefugtem Lesen und Verändern)

- Der Anwendungsdienst läuft in einem Container unter einem unprivilegierten Systembenutzer, nicht als Systemverwalter.
- Zugriffsrechte innerhalb der Anwendung sind an das Konto gebunden: eine Aufnahme ist ausschließlich für den Host der Sitzung und für Administratoren des Dienstes abrufbar. Jeder Endpunkt prüft die Berechtigung serverseitig; auf Angaben des Browsers wird dabei nicht vertraut.
- Die Administratorrolle innerhalb der Anwendung wirkt nur bei Anfragen aus dem verschlüsselten privaten Netz des Auftragnehmers (siehe 2.2). Von jeder anderen Adresse aus ist ein Administratorkonto ein gewöhnliches Nutzerkonto ohne Zugriff auf fremde Aufnahmen oder Konten; ein entwendetes Sitzungs-Cookie eines Administrators eröffnet außerhalb dieses Netzes keinen erweiterten Zugriff.
- Datenbankabfragen werden ausschließlich parametrisiert ausgeführt und zur Bauzeit gegen das Schema geprüft, wodurch SQL-Injektion ausgeschlossen ist.
- Auftragsdaten werden nicht dauerhaft auf dem Endgerät des Auftragnehmers gespeichert. Wird zur Fehleranalyse ausnahmsweise eine Kopie benötigt, wird sie auf dem verschlüsselten Endgerät abgelegt, ausschließlich zu diesem Zweck verwendet und nach Abschluss der Analyse gelöscht.

2.4 Trennungskontrolle

- Entwicklung und Produktion sind vollständig getrennt: eigene Datenbank, eigener Objektspeicher, eigene Zugangsschlüssel.
- Echte Aufnahmedaten werden in der Entwicklung nicht verwendet.
- Die Daten verschiedener Auftraggeber sind innerhalb der Anwendung über die Kontozuordnung getrennt; jede Abfrage ist an die Kontokennung gebunden.
- Aufnahmedateien liegen je Sitzung und je Spur in getrennten Ablagepfaden.

3. Integrität (Art. 32 Abs. 1 lit. b)

3.1 Weitergabekontrolle

- Eine Weitergabe von Auftragsdaten an Dritte findet außerhalb der in Anlage 3 des Auftragsverarbeitungsvertrages genannten Unterauftragsverarbeiter nicht statt.
- Die Paddle.com Market Limited als Merchant of Record erhält keinen Zugang zu Auftragsdaten.
- Die Herausgabe der fertigen Aufnahme erfolgt ausschließlich an den angemeldeten Host über eine verschlüsselte Verbindung.
- Jeder hochgeladene Abschnitt wird mit einer Prüfsumme versehen. Vor dem Verwerfen der lokalen Kopie wird die Kopie im Objektspeicher anhand dieser Prüfsumme verifiziert; schlägt die Prüfung fehl, bleibt die lokale Kopie bestehen.

3.2 Eingabekontrolle

- Sicherheits- und betriebsrelevante Vorgänge werden in einem Ereignisprotokoll festgehalten, unter anderem Anmeldungen, administrative Eingriffe, Tarifwechsel, Löschungen von Aufnahmen und Kontoänderungen. Festgehalten werden Zeitpunkt, Ereignisart, handelnde Person und betroffenes Objekt.
 - Das Ereignisprotokoll ist über die Anwendung nicht veränderbar.
 - Zugriffe auf den Server werden im Systemprotokoll erfasst.
-

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c)

4.1 Schutz vor Verlust während der Aufnahme

Die Aufnahme entsteht lokal im Browser jeder teilnehmenden Person und wird in Abschnitten hochgeladen. Die Warteschlange für den Upload verwirft keinen Abschnitt: fehlgeschlagene Übertragungen werden unbegrenzt mit wachsendem Abstand wiederholt, solange der Browser geöffnet bleibt. Ein Verbindungsabbruch führt daher nicht zu einer Lücke in der Aufnahme, sondern zu einer Verzögerung.

4.2 Redundanz und Wiederherstellung

- Die Datenträger der gemieteten Server werden vom Anbieter gespiegelt betrieben.
- Von den Datenträgern bestehen tägliche Momentaufnahmen (Snapshots) beim Serveranbieter, sieben Stück in Rotation. Zur Bedeutung für die Löschfristen siehe Abschnitt 0 des Verzeichnisses von Verarbeitungstätigkeiten.
- Die Aufnahmedateien liegen zunächst auf dem Datenträger des Anwendungsservers und werden anschließend in den Objektspeicher übertragen. Die lokale Kopie wird erst verworfen, nachdem Vorhandensein und Prüfsumme der Kopie im Objektspeicher bestätigt sind (siehe 3.1); bis dahin bestehen zwei Kopien an getrennten Standorten. Danach ist der Objektspeicher der alleinige Aufbewahrungsort.

- Darüber hinaus besteht von den Aufnahmedateien bewusst keine unabhängige Sicherung. Die Aufbewahrungsfrist beträgt je nach Tarif 3 oder 7 Tage, sofern im Hauptvertrag keine längere Frist vereinbart ist; die Aufnahme ist Arbeitsmaterial, das der Auftraggeber innerhalb dieser Frist abrufen. Auf diese Eigenschaft wird im Auftragsverarbeitungsvertrag ausdrücklich hingewiesen.
- Ausgeführte Kontolöschungen hält der Auftragnehmer außerhalb der gesicherten Systeme fest, damit sie nach einer Wiederherstellung erneut ausgeführt werden können. Der Eintrag im Ereignisprotokoll allein trüge das nicht, weil er auf denselben Datenträgern liegt und mit der Momentaufnahme zurückfiele.
- Die Wiederherstellung aus einer Momentaufnahme wurde am 21. August 2026 auf einem neu erstellten Server durchgeführt und protokolliert. Der Dienst war nach 15 Minuten wieder verfügbar; Datenbestand, Anmeldung und die Auslieferung einer Aufnahme aus dem verschlüsselten Objektspeicher waren vollständig funktionsfähig. Die Übung wird jährlich wiederholt; das Protokoll wird auf Anforderung vorgelegt.

4.3 Betriebssicherheit

- Der Anwendungsdienst startet nach einem Ausfall automatisch neu.
- Betriebssystemaktualisierungen des Servers werden automatisiert eingespielt.
- Die Container werden neu gebaut, sobald eine Änderung ansteht oder eine Sicherheitsmeldung zu einer eingesetzten Fremdkomponente vorliegt. Die eingesetzten Basis-Images sind versionsfest angegeben, ein Werkzeug meldet Abweichungen zum aktuellen Stand.
- Der Dienst begrenzt die Menge an Nachrichten pro Verbindung sowie die Anzahl von Anfragen pro IP-Adresse an den Anmelde-Endpunkten.

4.4 Protokolle und Metriken

Die Protokoll- und Metrikverarbeitung läuft getrennt von den Anwendungsservern, innerhalb der Europäischen Union und angebunden über ein verschlüsseltes privates Netz (VPN). Die Protokoll- und Metrikdaten liegen auf einer verschlüsselten Partition; das Betriebssystem selbst ist nicht verschlüsselt. Der Schlüssel liegt ausschließlich beim Auftragnehmer und ist auf dem Server nicht gespeichert: nach einem Neustart entschlüsselt er die Partition von Hand, bevor die Protokoll- und Metrikverarbeitung startet. Administrativen Zugang hat ausschließlich der Auftragnehmer. Derzeit läuft die Verarbeitung auf eigener Hardware des Auftragnehmers. Es handelt sich um Server- und Sicherheitsprotokolle sowie um das Ereignisprotokoll, also um Daten, für die der Auftragnehmer selbst Verantwortlicher ist, soweit sie der Abwehr von Missbrauch, der Fehlersuche und der Erfüllung eigener Rechenschaftspflichten dienen. Aufnahmeinhalte, Chatnachrichten, Anzeigenamen und Markerbezeichnungen werden dort nicht verarbeitet. Zugesagt sind die vorstehenden Eigenschaften, nicht der Betriebsort; er kann sich nach § 6 Absatz 2 des Auftragsvertrags ändern.

Verarbeitet werden vier Bestände:

- **Zugriffsprotokoll des Anwendungsservers:** Zeitpunkt, Methode, angefragter Pfad einschließlich der darin enthaltenen Kennungen von Sitzungen und Zuhörlinks, jedoch ohne den Query-String, der Statuscode und die Antwortzeit. Das Zugriffsprotokoll des vorgeschalteten Reverse Proxys enthält zusätzlich die IP-Adresse des Aufrufers; es wird in dasselbe System geführt und unterliegt derselben Aufbewahrung.

- **Betriebsprotokoll:** Kennungen von Sitzungen, Aufnahmen, Spuren und Teilnehmenden, Zeitpunkte, Zählerstände, die Browserkennung sowie Ereignisart und Zeitpunkt; bei einem gesetzten Marker dessen Art und Zeitversatz, nicht seine Bezeichnung.
- **Ereignisprotokoll (Abschnitt 3.2):** zusätzlich die IP-Adresse und die E-Mail-Adresse des Kontos, mit dem der Host angemeldet ist, sowie der Sitzungstitel.
- **Metriken:** Summenzähler ohne Bezug zu einer Sitzung, einem Konto oder einem Gerät. Sie werden beim Empfang der Diagnosedaten nach Anlage 1 des Auftragsverarbeitungsvertrages gebildet.

4.5 Löschung

- Aufnahmedaten werden nach Ablauf der tarifabhängigen Aufbewahrungsfrist automatisiert gelöscht, sowohl lokal als auch im Objektspeicher. Der Lauf erfolgt wiederkehrend und ohne manuelles Zutun.
- Zugriffs- und Betriebsprotokolle (Abschnitt 4.4) werden spätestens nach 90 Tagen gelöscht. Metriken enthalten keinen Personenbezug (Abschnitt 4.4) und unterliegen keiner Löschfrist.
- Das Ereignisprotokoll (Abschnitt 3.2) wird nach 12 Monaten automatisiert gelöscht.
- Unterlagen, die der Auftragnehmer steuerrechtlich aufbewahren muss, insbesondere Ausgangsrechnungen und Buchungsbelege aus einem unmittelbar geschlossenen Vertrag, sind von den automatisierten Löschläufen ausgenommen. Sie werden getrennt von den Betriebsdaten geführt, für die Dauer der gesetzlichen Frist in der Verarbeitung eingeschränkt und danach gelöscht.
- Die Vernichtung von Datenträgern obliegt den Anbietern und ist Bestandteil ihrer Zertifizierung. Eigene Datenträger mit Auftragsdaten sind nicht im Einsatz.

5. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d)

5.1 Datenschutz-Management

- Der Auftragnehmer nimmt die Aufgaben des Datenschutzes selbst wahr. Eine Bestellpflicht für einen Datenschutzbeauftragten besteht nicht.
- Ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO wird geführt, sowohl für die Verarbeitungen in eigener Verantwortlichkeit (Art. 30 Abs. 1) als auch für die Verarbeitungen im Auftrag (Art. 30 Abs. 2). Es wird als gesondertes Dokument geführt und mindestens einmal jährlich überprüft; es wird der Aufsichtsbehörde auf Anforderung vorgelegt und nicht veröffentlicht. Gegenüber Auftraggebern wird der sie betreffende Teil B als Nachweis nach § 8 Absatz 1 des Vertrages vorgelegt; Angaben zu anderen Auftraggebern werden dabei nicht offengelegt.
- Die Verpflichtung auf Vertraulichkeit betrifft den Auftragnehmer selbst; Beschäftigte gibt es nicht. Werden künftig Personen beauftragt, erfolgt die Verpflichtung schriftlich vor der ersten Kenntnissnahme von Daten.
- Dieses Dokument wird bei jeder wesentlichen Änderung der Verarbeitung überprüft, mindestens jedoch einmal jährlich.

5.2 Datenschutz durch Technikgestaltung und Voreinstellungen (Art. 25)

- Es werden keine Analyse- oder Trackingdienste eingesetzt. Der Dienst setzt ein einziges technisch notwendiges Cookie.
- Wer über einen Zuhörlink zuhört, wird vom Dienst nicht identifiziert: kein Konto, keine Cookies, keine dauerhaften Kennungen. Die Zugriffsprotokolle enthalten, wie bei jedem Webdienst, IP-Adresse, Zeitpunkt und Pfad und unterliegen 4.4 und 4.5.
- Aufnahmedaten werden nach kurzer, tarifabhängiger Frist automatisch gelöscht; eine dauerhafte Speicherung ist nicht vorgesehen und nicht einstellbar.
- Es werden nur die Daten erhoben, die für die Durchführung einer Aufnahme erforderlich sind.

5.3 Auftragskontrolle

- Mit allen Unterauftragsverarbeitern bestehen Verträge nach Art. 28 DSGVO.
- Der gewählte Rechenzentrumsstandort ist vertraglich an die Bestellung gebunden und kann vom Anbieter nicht einseitig geändert werden.
- Die Anbieter informieren über Wechsel ihrer eigenen Unterauftragsverarbeiter mit Vorlauf; der Auftragnehmer wertet solche Mitteilungen aus und unterrichtet die Auftraggeber, soweit die Änderung die Verarbeitung der Auftragsdaten berührt.
- Weisungen des Auftraggebers werden dokumentiert.

5.4 Verfahren bei Sicherheitsvorfällen

Bei einem Verdacht auf eine Verletzung des Schutzes personenbezogener Daten gilt:

1. Sofortige Eindämmung: betroffene Zugänge sperren, betroffene Dienste bei Bedarf abschalten.
2. Feststellung des Sachverhalts anhand der Protokolle: Zeitraum, betroffene Daten, betroffene Personenkreise, Ursache.
3. Benachrichtigung der betroffenen Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden, nachdem der Auftragnehmer mit hinreichender Sicherheit festgestellt hat, dass eine Verletzung des Schutzes personenbezogener Daten eingetreten ist, die die Auftragsdaten betrifft; mit den zu diesem Zeitpunkt bekannten Angaben und Ergänzung, sobald weitere vorliegen. Eine erste Meldung wahrt die Frist.
4. Unterstützung des Auftraggebers bei dessen Meldung nach Art. 33 DSGVO und bei der Benachrichtigung betroffener Personen nach Art. 34 DSGVO.
5. Beseitigung der Ursache und Dokumentation des Vorgangs einschließlich der getroffenen Maßnahmen.

Für Verarbeitungen, bei denen der Auftragnehmer selbst Verantwortlicher ist, meldet er die Verletzung unmittelbar der zuständigen Aufsichtsbehörde.

6. Nicht umgesetzte Maßnahmen und ihre Bewertung

Der Auftragnehmer führt die nicht umgesetzten Maßnahmen hier offen auf, statt sie oben als umgesetzt darzustellen. Es handelt sich um Abwägungen, nicht um Vorhaben: was hier steht, ist bewusst so entschieden und wird regelmäßig neu bewertet.

Nr.	Maßnahme	Stand	Bewertung
1	Verschlüsselung der Datenträger der gemieteten Server	nicht umgesetzt	Bewusste Entscheidung, siehe unten
2	DNSSEC für die Domain	nicht umgesetzt	Bewusste Entscheidung, siehe unten

Zur Vertretung der einen Person, die den Dienst betreibt, ist hier bewusst kein Punkt aufgeführt. Die Begründung steht in Abschnitt 7: Was ein Vertreter zu tun hätte, läuft bereits ohne ihn, und was dann noch fehlt, ließe sich durch eine Vertretungsregelung nicht herstellen.

Zu Nummer 1: Eine Verschlüsselung der Serverdatenträger würde bei jedem Neustart eine manuelle Freigabe erfordern und damit die Verfügbarkeit des Dienstes an die Erreichbarkeit einer einzelnen Person binden. Der Auftragnehmer hält den dadurch entstehenden Verfügbarkeitschaden derzeit für größer als den Sicherheitsgewinn gegenüber einem zertifizierten Rechenzentrum. Die Bewertung wird jährlich überprüft.

Zu Nummer 2: Der DNS-Anbieter bietet DNSSEC in der genutzten Verwaltung nicht an. Der Schutz der Zertifikatsausstellung beruht auf dem CAA-Eintrag (Abschnitt 1.1); Let's Encrypt prüft ihn aus mehreren Netzperspektiven, sodass eine Manipulation der DNS-Antwort auf einem einzelnen Weg nicht genügt. Die Bewertung wird überprüft, sobald der Anbieter DNSSEC anbietet.

7. Hinweis zur Betriebsgröße

Der Auftragnehmer ist ein Einzelunternehmen. Daraus folgen zwei Eigenschaften, die ein Auftraggeber bei seiner eigenen Risikobewertung berücksichtigen sollte:

- **Der Kreis der Zugriffsberechtigten ist minimal.** Es gibt genau eine Person mit Zugang zu Systemen und Daten. Das schließt die häufigste Ursache von Datenschutzvorfällen, den Innentäter oder das kompromittierte Mitarbeiterkonto, weitgehend aus.

- **Es besteht keine Vertretungsregelung.** Bei einem längeren Ausfall der Person, die den Dienst betreibt, ist mit verzögerter Reaktion auf Anfragen und Störungen zu rechnen. Drei Dinge regeln sich dabei ohne ihr Zutun, und sie decken den größten Teil des Schadens ab:
 - Der Abruf einer Aufnahme braucht keine Freigabe durch den Auftragnehmer. Vor Ablauf der Aufbewahrungsfrist versendet der Dienst zusätzlich automatisch eine Erinnerung an das Konto, dem die Aufnahme gehört, ebenfalls ohne Zutun des Auftragnehmers. Ob sie den Empfänger erreicht, liegt außerhalb der Kontrolle des Auftragnehmers; der Abruf hängt nicht von ihr ab.
 - Es wächst kein Datenbestand an. Die Aufbewahrungsfrist beträgt je nach Tarif 3 oder 7 Tage, sofern im Hauptvertrag nichts anderes vereinbart ist, und der Löschlauf arbeitet ohne Eingriff weiter. Nach Ablauf der jeweils vereinbarten Frist, im Regelfall also nach etwa einer Woche ohne Betreuung, sind keine Aufnahmedaten mehr vorhanden.
 - Das Abonnement endet ohne den Auftragnehmer, soweit es über den Bestellprozess gebucht wurde. Vertragspartner des Kaufvertrages ist dann die Paddle.com Market Limited als Merchant of Record; dort wird gekündigt, und Ansprüche wegen ausbleibender Leistung richten sich ebenfalls gegen sie. Bei einem unmittelbar mit dem Auftragnehmer geschlossenen Vertrag besteht dieser Weg nicht: gekündigt wird gegenüber dem Auftragnehmer, und Ansprüche richten sich gegen ihn. Der Auftraggeber sollte das bei Laufzeit und Zahlungsweise berücksichtigen; eine kurze Laufzeit oder eine nachschüssige Abrechnung begrenzt den Schaden hier wirksamer als eine Vertragsklausel.

Offen bleibt die Erreichbarkeit einer Person: Anfragen betroffener Personen nach Art. 15 bis 22 DSGVO und eine Meldung nach Art. 33 DSGVO setzen ein Handeln voraus, und dafür gibt es während eines längeren Ausfalls keinen Ansprechpartner. Eine benannte Vertretung würde daran wenig ändern, da sie den Dienst weder betreiben noch einen Vorfall fachlich beurteilen könnte. Bei einem dauerhaften Ausfall tritt die gesetzliche Rechtsnachfolge ein. Das ist keine geplante Maßnahme, sondern die Rechtslage, und der Auftraggeber sollte sie in seiner eigenen Risikobewertung als solche behandeln.