VERTRAG UND ANLAGEN

# Vertragsdaten und Parteien

## Vereinbarung nach Art. 28 DSGVO

Produkt: KaBa Cloud. Fassung AVV-2026-11-04-1. Die Vereinbarung umfasst diese Vertragsdaten, die Ziffern 1 bis 10 und die Anlagen A bis D. Sie ergänzt den bezeichneten Hostingvertrag. Die Veröffentlichung oder eine Softwarebuchung allein bedeutet noch keinen Abschluss dieser AVV.

## Auftraggeber

Vollständiger Name / Firma: _____

Anschrift: _____

Vertreten durch / Funktion: _____

Bestellnummer und Instanzadresse: _____

Datenschutz- und Vorfallkontakt, E-Mail: _____

Weisungsberechtigte Person(en), Funktion und E-Mail: _____

Rolle: Verantwortlicher; bei eigener Auftragsverarbeitung zusätzlich die Berechtigung zur Unterbeauftragung und Weisungskette vor Abschluss mitteilen.

## Auftragsverarbeiterin

Julia Thiel, handelnd unter der Projektbezeichnung STRUEX
Hohenstaufenstraße 24a, 69412 Eberbach, Deutschland
Ansprechpartnerin für Datenschutz, Weisungen und Vorfälle: Julia Thiel
E-Mail: app@struex.com

Eine künftig gegründete Gesellschaft wird nicht automatisch Vertragspartei. Ein Wechsel der Auftragsverarbeiterin bedarf einer gesonderten Vereinbarung.

## Bezug und Beginn

Hauptvertrag / Beginn: _____

Die AVV gilt ab dokumentiertem Abschluss für die Laufzeit der beauftragten Verarbeitung einschließlich Rückgabe und Löschung. Bis dahin sind ausschließlich synthetische Beispieldaten zu verwenden. Abweichende oder zusätzliche Datenarten und Schutzanforderungen werden vor ihrem Einsatz in Anlage A ergänzt.

KABA CLOUD

# Vertragliche Regelungen · 1 bis 5

## 1. Gegenstand und Grenzen

Die Auftragsverarbeiterin betreibt die eigene KaBa-Instanz des Auftraggebers. Dies umfasst Bereitstellung, Speicherung, Abruf, technische Übermittlung, Sicherung, Wiederherstellung, Wartung, weisungsgebundenen Support sowie Rückgabe und Löschung der Auftragsdaten. Anwendungs-E-Mails sind erfasst, soweit sie im vereinbarten Betrieb ausgelöst werden. Umfang, Zwecke, Personen und Daten ergeben sich aus Anlage A.

Der Auftraggeber legt die fachlichen Zwecke, Inhalte, Zugriffsrechte und Rechtsgrundlagen fest. Die Auftragsverarbeiterin verwendet Auftragsdaten nicht für eigene Werbung, Profilbildung oder das Training von KI-Modellen. Eine kundenseitig aktivierte Fremdintegration ist ohne ausdrückliche Beauftragung nicht Bestandteil dieser AVV.

## 2. Dokumentierte Weisungen

Diese AVV, der Hauptvertrag und berechtigte Einstellungen innerhalb des vereinbarten Leistungsumfangs bilden die anfänglichen Weisungen. Ergänzende Weisungen gehen in Textform an app@struex.com oder über den zugeordneten Supportvorgang. Sicherheitsrelevante Weisungen werden nach Prüfung der Berechtigung ausgeführt; eine E-Mail-Absenderangabe allein genügt nicht als Identitätsnachweis. Mündliche Eilweisungen sind nachträglich zu dokumentieren.

Auftragsdaten werden nur auf dokumentierte Weisung verarbeitet, auch bei Drittlandübermittlungen. Zwingt Unionsrecht oder das Recht eines Mitgliedstaats zur Verarbeitung, informiert die Auftragsverarbeiterin vorab über die Verpflichtung, sofern das betreffende Recht dies nicht aus wichtigen Gründen des öffentlichen Interesses untersagt. Bei einer erkennbar rechtswidrigen Weisung informiert sie unverzüglich und setzt deren Ausführung bis zur Klärung aus.

## 3. Vertraulichkeit und Organisation

Zugriff erhalten ausschließlich erforderliche, autorisierte Personen mit Vertraulichkeitsverpflichtung oder angemessener gesetzlicher Verschwiegenheitspflicht. Berechtigungen werden auf die Aufgabe begrenzt und bei Wegfall entzogen. Die Auftragsverarbeiterin führt die erforderlichen Verzeichnisse und Nachweise, kooperiert mit Aufsichtsbehörden und benennt einen Datenschutzkontakt. Die Benennung einer Ansprechpartnerin ersetzt keine gesetzlich erforderliche Datenschutzbeauftragtenbestellung.

## 4. Technische und organisatorische Maßnahmen

Die Maßnahmen in Anlage B bilden das vereinbarte Schutzniveau. Die Auftragsverarbeiterin prüft ihre Wirksamkeit regelmäßig und nach wesentlichen Änderungen oder Vorfällen. Verbesserungen sind zulässig; eine wesentliche Absenkung des Schutzniveaus erfordert vorherige Vereinbarung. Für besondere Risiken werden vor Beginn zusätzliche Maßnahmen vereinbart.

## 5. Unterauftragnehmer und Drittlandübermittlungen

Der Auftraggeber genehmigt die Dienstleister und Tätigkeiten in Anlage C. Weitere oder ersetzende unmittelbare Unterauftragnehmer werden mindestens 30 Kalendertage vor ihrem Einsatz in Textform mit Name, Tätigkeit, Verarbeitungsort und Schutzgrundlage angekündigt. Der Auftraggeber kann innerhalb dieser Frist aus nachvollziehbaren Datenschutzgründen widersprechen. Ohne tragfähige Lösung erfolgt der beanstandete Einsatz nicht; erforderlichenfalls kann der betroffene Leistungsteil ohne zusätzliche Beendigungsgebühr beendet werden.

Bei Änderungen nachgelagerter Unterauftragnehmer informiert die Auftragsverarbeiterin unverzüglich nach Anbieterinformation. Die Weiterbeauftragung muss die erforderlichen Datenschutzpflichten und Widerspruchsmöglichkeiten erhalten. Können diese nicht gewahrt werden, sind eine Alternative oder die Aussetzung des betroffenen Verarbeitungsteils zu vereinbaren. Die Auftragsverarbeiterin bleibt für die Pflichterfüllung ihrer Unterauftragnehmer verantwortlich.

Übermittlungen außerhalb EU/EWR erfolgen nur im vereinbarten Umfang und bei wirksamer Grundlage nach Kapitel V DSGVO. Fällt diese weg, wird die betroffene Übermittlung ausgesetzt, bis eine rechtmäßige Alternative besteht. Die Beauftragung ist keine Einwilligung betroffener Personen nach Art. 49 DSGVO.

KABA CLOUD

# Vertragliche Regelungen · 6 bis 10

## 6. Rechte betroffener Personen

Die Auftragsverarbeiterin unterstützt den Auftraggeber durch geeignete technische und organisatorische Maßnahmen bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch. Sie leitet bei ihr eingegangene Anfragen zu Auftragsdaten unverzüglich an den benannten Kontakt weiter und beantwortet sie nur auf Weisung oder aufgrund eigener gesetzlicher Verpflichtung. Sie berücksichtigt mitgeteilte gesetzliche Fristen und stimmt erforderliche Identitätsprüfungen ab.

## 7. Datenschutzvorfälle und Unterstützung

Nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Auftragsdaten informiert die Auftragsverarbeiterin den Auftraggeber unverzüglich. Eine erste Meldung wartet nicht auf eine abgeschlossene Untersuchung. Sie enthält die verfügbaren Angaben zu Art und Zeitpunkt, betroffenen Daten und Personen, möglichen Folgen, ergriffenen Maßnahmen und einem erreichbaren Kontakt. Fehlende Angaben folgen ohne unangemessene Verzögerung.

Sie sichert relevante Nachweise, begrenzt Schäden und unterstützt unter Berücksichtigung ihrer Informationen und der Art der Verarbeitung bei Art. 32 bis 36 DSGVO, insbesondere Meldungen, Benachrichtigungen, Datenschutz-Folgenabschätzungen und vorheriger Konsultation. Die Entscheidung über Meldungen des Auftraggebers trifft dieser; eigene gesetzliche Pflichten der Auftragsverarbeiterin bleiben bestehen. Eine Anbieterfreigabe darf gesetzliche Meldungen nicht verzögern.

## 8. Information, Kontrollen und Nachweise

Die Auftragsverarbeiterin stellt die erforderlichen Informationen zum Nachweis ihrer Pflichten bereit und ermöglicht sowie unterstützt Prüfungen einschließlich Inspektionen durch den Auftraggeber oder einen geeigneten beauftragten Prüfer. Regelmäßige Prüfungen werden angemessen angekündigt; bei Vorfällen, begründetem Verdacht oder behördlicher Anordnung ist eine kurzfristige Prüfung möglich.

Vertraulichkeit, Sicherheit und Rechte anderer Kunden werden durch geeignete Abläufe geschützt. Diese Abstimmung darf das Kontrollrecht nicht ausschließen. Auskünfte, Dokumente und gegebenenfalls Prüfberichte können eine Prüfung vorbereiten, ersetzen aber nicht pauschal erforderliche Inspektionen. Feststellungen und Abhilfemaßnahmen werden dokumentiert. Aufsichtsrechte bleiben unberührt.

## 9. Vertragsende, Rückgabe und Löschung

Nach Ende der beauftragten Verarbeitung werden Auftragsdaten nach Wahl des Auftraggebers zurückgegeben oder gelöscht; vorhandene Kopien werden nach Anlage D gelöscht. Gesetzliche Aufbewahrungspflichten bleiben bestehen. In diesem Fall werden Daten auf die Pflicht beschränkt, von weiterer Nutzung ausgeschlossen und nach Fristablauf gelöscht. Die bloße Vertragsbeendigung oder das Anhalten eines Containers ist keine Löschung.

Die Auftragsverarbeiterin informiert den Auftraggeber über konkrete Hinderungsgründe und dokumentiert eine erforderliche Restaufbewahrung mit Rechtsgrund, Datenumfang und Frist. Aufbewahrung eigener Rechnungs- und Vertragsnachweise berechtigt nicht zur pauschalen weiteren Speicherung sämtlicher Anwendungsdaten. Auch Transferarchive, Supportkopien und Wiederherstellungstests sind einzubeziehen.

## 10. Abschluss, Änderungen und Vorrang

Der Abschluss erfolgt durch beiderseitige Unterschrift oder übereinstimmende dokumentierte Erklärungen in Textform, jeweils mit ausgefüllten Vertragsdaten, Bezug auf diese Fassung und den Anlagen. Beide Parteien erhalten eine speicherbare Kopie. Neue Websitefassungen ändern bestehende Vereinbarungen nicht rückwirkend. Änderungen werden ausdrücklich vereinbart; das Verfahren für Unterauftragnehmer nach Ziffer 5 bleibt anwendbar.

In Datenschutzfragen hat diese AVV Vorrang vor allgemeinen Leistungsbedingungen. Haftung und Rechte betroffener Personen richten sich nach den gesetzlichen Vorschriften; es wird kein besonderer Haftungsausschluss vereinbart. Gesetzlich gebotene Unterstützung darf nicht von einer vorherigen Zahlung abhängig gemacht werden. Etwaige zusätzliche Leistungen und deren Vergütung bedürfen einer gesonderten Vereinbarung.

KABA CLOUD

# Anlage A · Verarbeitung und Weisungen

## A.1 Zweck und betroffene Personen

Organisation von Aufgaben und Arbeitsabläufen auf Kanban-Boards einschließlich Zuständigkeiten, Terminen, Unterlagen und Kommentaren.

Betroffene Personen: Teammitglieder, Beschäftigte, Gäste und sonstige in Aufgaben oder Unterlagen benannte Personen.

## A.2 Datenarten

Namen, Kontakt- und Profilangaben; Board-Mitgliedschaften und Rollen; Karten, Aufgabenbeschreibungen, Zuständigkeiten, Termine, Status, Kommentare, Anhänge und Vorgangsverläufe, soweit die verwendete Funktion sie führt.

Zusätzlich technisch erforderliche Konten-, Rollen-, Anmelde- und Sitzungsdaten, gehashte Passwörter beziehungsweise Authentisierungsinformationen, IP-Adressen, Zeitpunkte, Fehler- und Betriebsprotokolle. Nutzungsinhalte werden nur in dem vom Auftraggeber festgelegten Umfang verarbeitet. Veröffentlichungen und Empfänger bestimmt der Auftraggeber über berechtigte Funktionen und Weisungen.

## A.3 Verarbeitung und Dauer

Fortlaufende Verarbeitung während des vereinbarten Betriebs; Zugriff bei Bedarf für technische Betreuung. Datensicherungen erfolgen täglich. Anwendungsnachrichten werden bei den vom Auftraggeber veranlassten Ereignissen verarbeitet. Nach Ende gilt Anlage D. Ort des Instanzbetriebs und der S3-Sicherungen: Deutschland; für Anwendungs-E-Mails zusätzlich Anlage C.

## A.4 Besondere Anforderungen

Nicht vom Standardumfang umfasst sind gezielt verarbeitete besondere Kategorien nach Art. 9 DSGVO, Daten nach Art. 10 DSGVO oder Inhalte mit vergleichbar hohem Schutzbedarf. Dazu können etwa Gesundheitsangaben in Formularen gehören. Solche Verarbeitungen dürfen erst nach gesonderter Prüfung, dokumentierter Erweiterung und gegebenenfalls zusätzlichen Maßnahmen beginnen. Auch eine erhebliche Verarbeitung von Kinderdaten oder systematische Überwachung ist vorab mitzuteilen. Freitext- oder Uploadfunktionen beseitigen diese Beschränkung nicht.

## A.5 Rollenabgrenzung

Der Auftraggeber bestimmt Berechtigungen und Empfänger innerhalb seiner Instanz. Er verantwortet Datenminimierung, Rechtsgrundlagen und Informationen an betroffene Personen. Eigene gesetzliche Pflichten der Auftragsverarbeiterin bleiben unberührt. Bei Weiterbeauftragung durch einen selbst als Auftragsverarbeiter handelnden Auftraggeber müssen die erforderlichen Genehmigungen und Weisungen des Verantwortlichen vorliegen.

Kaufmännische Kundenkonten, Abrechnung und eigene Vertragskommunikation der Auftragsverarbeiterin werden für deren eigene Zwecke verarbeitet und sind gesondert beschrieben. Stripe ist für die Zahlungsabwicklung eingebunden und wird durch diese AVV nicht zum Unterauftragnehmer für Anwendungsinhalte. Supportnachrichten mit beigefügten Anwendungsdaten fallen hinsichtlich dieser Inhalte unter die Weisungsbindung.

## A.6 Ergänzungen für diesen Auftrag

Zusätzliche Funktionen / Datenarten / Personen / Löschweisungen: _____

_____

_____

Ohne bestätigte Ergänzung gelten ausschließlich die oben beschriebenen Standardverarbeitungen. Zusätzliche weisungsberechtigte Personen werden über einen bereits verifizierten Kontakt benannt.

KABA CLOUD

# Anlage B · Schutzmaßnahmen

## B.1 Zugang und Berechtigungen

Die zentrale Verwaltung verwendet persönliche Konten, Rollen und verpflichtende Zwei-Faktor-Authentisierung. Sitzungen und sensible Aktionen sind serverseitig geschützt; Wiederherstellungscodes sind einmalig verwendbar und gehasht gespeichert. Kundenkonten sind produktgebunden. Berechtigungen werden bei Änderungen und mindestens jährlich überprüft; ausgeschiedene Berechtigte verlieren ihren Zugriff unverzüglich.

Administrationsrechner verfügen über Laufwerksverschlüsselung, persönliche Anmeldung und automatische Bildschirmsperre. Die Auftragsverarbeiterin sorgt für aktuelle Sicherheitssoftware und Betriebssystemupdates. Serverzugänge erfolgen über geschützte SSH-Schlüssel; Schlüssel und Wiederherstellungszugänge werden nicht in öffentlichen Quellcode oder Kundennachrichten aufgenommen.

## B.2 Trennung und Zugriff auf Inhalte

Jeder Kunde erhält eine eigene Anwendungsinstallation mit eigenen Datenbanken, Zugangsdaten und Datenvolumes. Die zugrunde liegenden Server können mehrere Instanzen tragen; ein ausschließlich physisch zugeordneter Server ist nicht Bestandteil des Standardtarifs. Datenzugriffe für Wartung und Support erfolgen nur soweit erforderlich und werden anhand des Betriebs- oder Supportvorgangs dokumentiert. Test- und Wiederherstellungsumgebungen werden getrennt betrieben; echte Daten sind auf das Erforderliche zu beschränken und anschließend zu löschen.

## B.3 Transport und gespeicherte Daten

Webzugriffe verwenden HTTPS. Administrations- und Datentransferverbindungen nutzen verschlüsselte Protokolle. Die Übermittlung an den Maildienst erfolgt über dessen TLS-/HTTPS-Schnittstellen; gewöhnliche E-Mail bietet keine Ende-zu-Ende-Verschlüsselung und die Zustellung an Empfängerserver hängt auch von deren Unterstützung ab. Besonders schutzbedürftige Inhalte gehören ohne zusätzliche Vereinbarung nicht in E-Mails.

Zentrale Instanzgeheimnisse, Vertragsnachweise sowie Inhalte und Anhänge des zentralen Posteingangs werden anwendungsseitig verschlüsselt. Die Control-Sicherung ist zusätzlich mit Restic verschlüsselt. Eine durchgehende Ende-zu-Ende-Verschlüsselung sämtlicher App-Daten oder zusätzliche clientseitige Verschlüsselung aller Kunden-Volume-Backups wird nicht zugesagt. Datenzugriff durch berechtigte Administratoren bleibt technisch möglich.

## B.4 Verfügbarkeit und Wiederherstellung

Tägliche Sicherungen der vorgesehenen Kundenvolumes werden extern in Hetzner Object Storage gespeichert. Die Plattformdatenbank wird konsistent gesichert. Volume-Backups können eine kurze Betriebsunterbrechung erfordern. Wiederherstellbarkeit wurde an isolierten Installationen geprüft; solche Prüfungen werden mindestens jährlich sowie nach wesentlichen Änderungen wiederholt und dokumentiert. Eine garantierte Wiederherstellungszeit oder Hochverfügbarkeitsarchitektur wird damit nicht vereinbart.

Überwachung erfasst Erreichbarkeit, Auslastung, Bereitstellung, Sicherungen und Mailwarteschlange. Ein zusätzlicher Prüfprozess auf dem Demo-Server prüft die Plattform unabhängig. Gleichzeitiger Ausfall mehrerer Prüfserver oder des Maildienstes kann die Alarmierung beeinträchtigen; die Kontrolle der Berichte bleibt Teil des Betriebs.

## B.5 Änderungen, Nachweise und Vorfälle

Zentrale administrative Betriebsaktionen und sicherheitsrelevante Ereignisse werden protokolliert. Eine vollständige manipulationssichere Protokollierung jeder Änderung in jeder App wird nicht zugesagt. Sicherheitsupdates werden risikobasiert bewertet, getestet und eingespielt; akute Schwachstellen werden vorrangig behandelt. Schutzmaßnahmen und Vorfallablauf werden mindestens jährlich und anlassbezogen überprüft. Verantwortliche Ansprechpartnerin ist Julia Thiel.

Die Auftragsverarbeiterin dokumentiert Sicherheitsvorfälle, Maßnahmen, Meldungen und Löschungen. Der Zutritt zu Rechenzentren unterliegt den physischen Schutzmaßnahmen von Hetzner. Kundenseitige Rollen, Inhalte und Endgeräte bleiben im Verantwortungsbereich des Auftraggebers.

KABA CLOUD

# Anlage C · Unterauftragnehmer

## C.1 Hetzner Online GmbH

Industriestr. 25, 91710 Gunzenhausen, Deutschland. Tätigkeit: virtuelle Server, Netzwerk- und Speicherinfrastruktur sowie externe S3-Sicherungen. Verarbeitungsort der hier eingesetzten Infrastruktur: Deutschland; Object Storage in Falkenstein (fsn1). Betroffene Daten: die in Anlage A beschriebenen gehosteten Daten, Sicherungskopien und technische Betriebsdaten. Grundlage: Vereinbarung zur Auftragsverarbeitung mit Hetzner.

## C.2 AC PM LLC · Postmark

1 N Dearborn Street, Suite 500, Chicago, IL 60602, USA. Tätigkeit: Transport, Empfang und technische Zustellverarbeitung von Anwendungs-E-Mails einschließlich Nachrichtenhistorie und erforderlicher Sperrlisten. Verarbeitungsort: USA. Umfang: Empfänger-/Absenderadressen, Betreff, Nachrichtentext, gegebenenfalls Anhänge sowie Zustell- und Fehlerdaten; keine pauschale Übermittlung der gesamten Anwendungsdatenbank.

Grundlage: einbezogene Postmark-DPA einschließlich der einschlägigen EU-Standardvertragsklauseln für die Verarbeitungskette, bei Auftragsdaten grundsätzlich Modul 3. Soweit ein wirksamer und für den konkreten Empfänger geltender Angemessenheitsbeschluss greift, kann die Übermittlung darauf gestützt werden. Der jeweils genutzte Mechanismus, dessen Geltung und gegebenenfalls erforderliche ergänzende Maßnahmen sind von der Auftragsverarbeiterin zu dokumentieren und auf berechtigte Anfrage nachzuweisen.

Die Zustimmung zu dieser Anlage umfasst den beschriebenen Mailversand in die USA unter diesen Voraussetzungen. Sie ersetzt weder die Information betroffener Personen noch die Prüfung der Übermittlungsgrundlage. Die Auftragsverarbeiterin reduziert Mailinhalte auf das Erforderliche und übermittelt keine besonderen Datenkategorien ohne vorherige gesonderte Vereinbarung.

## C.3 Nachgelagerte Verarbeitung

Die benannten Anbieter dürfen weitere Auftragsverarbeiter nur im Rahmen ihrer datenschutzrechtlichen Verpflichtungen und der erforderlichen Genehmigungen einsetzen. Die Auftragsverarbeiterin hält die für ihren Auftrag geltenden Anbieterlisten und Änderungsnachweise vor und macht sie dem Auftraggeber zugänglich. Ihre Informations- und Abhilfepflichten nach Ziffer 5 gelten auch bei Änderungen dieser Verarbeitungskette. Eine Website-Verlinkung allein ersetzt keine notwendige Änderungsmitteilung.

## C.4 Abgrenzung und Nachweise

Coolify wird auf eigener Infrastruktur betrieben und ist als selbst betriebene Software kein zusätzlicher Hosting-Unterauftragnehmer. Kundenbeauftragte Fremdintegrationen werden nur nach gesonderter Rollen- und Vertragsklärung Teil dieser AVV. Zahlungsabwicklung und eigene kaufmännische Kommunikation sind nach Anlage A.5 abzugrenzen.

Anbieterinformationen: https://docs.hetzner.com/general/company-and-policy/data-protection-at-hetzner/ sowie https://postmarkapp.com/dpa und https://postmarkapp.com/eu-privacy. Maßgeblich bleiben die tatsächlich vereinbarten Vertragsfassungen und nachgewiesenen Schutzgrundlagen.

KABA CLOUD

# Anlage D · Rückgabe und Löschung

## D.1 Wahl und Export

Spätestens bei Vertragsende teilt der Auftraggeber mit, ob er die Rückgabe mit anschließender Löschung oder unmittelbar die Löschung wünscht. Fehlt eine Weisung, fordert die Auftragsverarbeiterin sie an; für die Zeit bis zur Klärung wird die Instanz angehalten und auf Rückgabe, Löschung und erforderliche Sicherung beschränkt. Ohne anderslautende vereinbarte Weisung werden Primärdaten spätestens 30 Kalendertage nach Ende der beauftragten Verarbeitung gelöscht. Rechtzeitig verlangte Rückgabe ist vorher zu ermöglichen.

Rückgabe erfolgt über vorhandene App-Exporte und, soweit damit nicht vollständig, als instanzbezogener Datenbankexport einschließlich zugehöriger Originaldateien und einer Formatbeschreibung. Technische Zugangsschlüssel anderer Systeme oder anderer Kunden sind ausgeschlossen. SQL-/strukturierte Exporte und Originaldateien sind möglich; eine automatische Importierbarkeit in jedes Fremdsystem wird nicht zugesagt.

Die Übergabe erfolgt an einen verifizierten Berechtigten über einen befristeten geschützten Download oder ein verschlüsseltes Archiv mit getrennt übermitteltem Schlüssel. Eine gewöhnliche E-Mail mit offenem Datenarchiv ist kein vereinbarter Übergabeweg. Nach Übergabe besteht innerhalb der Löschfrist regelmäßig eine Prüffrist von sieben Kalendertagen; notwendige Abweichungen werden dokumentiert abgestimmt.

## D.2 Primärdaten und Arbeitskopien

Zur Löschung gehören Datenbank, Dateivolumes, individuelle Transferarchive, Exportdateien, Supportkopien und Wiederherstellungstestkopien, soweit keine belegte gesetzliche Pflicht entgegensteht. Vor Ausführung werden Auftrag, Berechtigung und exakte Instanzzuordnung geprüft. Eine Sperre ohne dokumentierten Hinderungsgrund rechtfertigt keine unbefristete Aufbewahrung. Gesetzliche Löschansprüche werden nicht durch die Höchstfristen ausgeschlossen.

## D.3 Sicherungen

Im regulären Betrieb sind bis zu sieben lokale und 30 externe tägliche Kunden-Sicherungsstände vorgesehen. Nach Löschung der Primärdaten werden verbliebene Kopien unverzüglich von regulärer Nutzung ausgeschlossen und spätestens nach weiteren 30 Kalendertagen entfernt; soweit gefahrlos möglich früher. Stillgelegte Backuppläne, zusätzliche Snapshots und Testarchive sind ausdrücklich zu prüfen. Die Frist wird nicht allein durch die konfigurierte Zahl der Sicherungsstände als erfüllt angesehen.

Nicht einzeln herauslösbare Daten in gemeinsamen Sicherungen bleiben bis zur fristgerechten Entfernung der betroffenen Sicherung gesperrt. Die Auftragsverarbeiterin führt einen Löschvermerk und setzt bei einer notwendigen Wiederherstellung bereits erteilte Löschweisungen erneut um, bevor die wiederhergestellten Daten regulär genutzt werden.

## D.4 Maildaten und sonstige Restbestände

Für Postmark-Nachrichten gilt die für den Auftrag dokumentierte Aufbewahrung, im Standard höchstens 45 Tage ab jeweiliger Nachricht. Längere anbieterbezogene Einstellungen werden für Auftragsdaten nicht ohne Vereinbarung verwendet. Erforderliche Löschungen werden auch gegenüber dem Maildienst geltend gemacht. Sperrlisten zu Beschwerden, Abmeldungen und Unzustellbarkeit werden gesondert geprüft: unnötige Einträge werden entfernt; weiterhin notwendige minimale Sperrinformationen dürfen nicht für Werbung oder andere Zwecke genutzt werden. Konkrete gesetzliche Restaufbewahrung ist zu begründen.

Support- und Plattformkopien von Anwendungsinhalten sind in den Löschauftrag einzubeziehen. Eigene Rechnungs-, Vertrags- und Nachweisdaten unterliegen gesonderten gesetzlichen Zwecken und Fristen; dies rechtfertigt keine Aufbewahrung vollständiger Kundeninhalte.

## D.5 Nachweis

Die Auftragsverarbeiterin bestätigt in Textform, welche Instanz und Datenbestände wann gelöscht wurden, wann verbliebene Sicherungen entfallen und welche konkret begründeten Restbestände bestehen. Nach deren Entfernung wird der Nachweis vervollständigt. Die beschriebenen Schritte werden administrativ veranlasst und kontrolliert; Vertragsende löst derzeit keine pauschale automatische Löschung aller Kunden- und Maildaten aus.

KABA CLOUD

# Abschluss und individuelle Ergänzungen

## Einbezogene Unterlagen

Diese Vereinbarung in der Fassung AVV-2026-11-04-1 für KaBa Cloud einschließlich der ausgefüllten Vertragsdaten, Ziffern 1 bis 10 und Anlagen A bis D. Besondere Vereinbarungen sind unten zu dokumentieren und von beiden Parteien zu bestätigen. Ohne solche Ergänzungen gelten die beschriebenen Standardbedingungen.

## Ergänzende Vereinbarungen

_____
_____
_____
_____
_____
_____

## Auftraggeber

Name und Funktion der erklärenden Person: _____
Ort und Datum: _____
Unterschrift oder dokumentierte Erklärung in Textform: _____

## Auftragsverarbeiterin

Julia Thiel
Ort und Datum: _____
Unterschrift oder dokumentierte Erklärung in Textform: _____

## Abschluss in Textform

Alternativ zur Unterschrift senden die Parteien übereinstimmende Erklärungen mit Produkt, Bestellnummer, Vertragsdaten und Versionskennung. Beispiel: „Ich bestätige die beigefügte Vereinbarung zur Auftragsverarbeitung AVV-2026-11-04-1 für KaBa Cloud einschließlich der ausgefüllten Vertragsdaten und Anlagen A bis D.“ Die jeweilige Vertretungsberechtigung muss bestehen.

Die Auftragsverarbeiterin bestätigt den Abschluss gesondert und stellt beiden Parteien die endgültige speicherbare Fassung bereit. Eine nur heruntergeladene Vorlage oder ein vorausgefüllter Entwurf ist noch kein Abschlussnachweis. Ein Datenverarbeitungsbeginn wird dadurch nicht rückwirkend genehmigt.