Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO) – Web-Bestätigungen

Fassung vom 03.11.2026

Parteien

- **Kunde (Verantwortlicher):** das Unternehmen, das den Dienst mit dem Antrag nach den Nutzungsbedingungen für die Web-Bestätigung beantragt, mit den Angaben aus seinem Antrag – im Folgenden „Kunde“
- **Auftragsverarbeiter:** DEKObyte Software & IT-Beratung, Inhaber Dennis Korittke, Am Feuerwehrhaus 5, 37191 Katlenburg-Lindau, Telefon +49 (0) 55 51 – 91 30 51, E-Mail info@palettenkonto.net – im Folgenden „DEKObyte“

Inhalt

Präambel · § 1 Begriffe · § 2 Gegenstand, Rollen und Aufgaben von DEKObyte · § 3 Dauer · § 4 Weisungen · § 5 Zweckbindung · § 6 Vertraulichkeit · § 7 Technische und organisatorische Maßnahmen · § 8 Unterauftragsverarbeiter · § 9 Rechte betroffener Personen · § 10 Aufbewahrung und Löschung · § 11 Belege bleiben unverändert · § 12 Ende des Hauptvertrags: Mandant beenden, Export, Archivphase · § 13 Mitteilungen von Tauschpartnern; Postfach des Absenders · § 14 Verletzungen des Schutzes personenbezogener Daten; weitere Unterstützung · § 15 Nachweise, Kontrollen, Verzeichnis · § 16 Angaben und Pflichten des Kunden; Information der Tauschpartner · § 17 Hinweis des Herstellers nach der Antwort · § 18 Haftung · § 19 Schlussbestimmungen · Anlage 1 Gegenstand, Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen · Anlage 2 Löschkonzept · Anlage 3 Unterauftragsverarbeiter · Anlage 4 Technische und organisatorische Maßnahmen

Vertrag

Präambel

Der Kunde nutzt das Zusatzmodul „Web-Bestätigungen“ zum Palettenkonto (im Folgenden „Web-Bestätigung“) nach den Nutzungsbedingungen für die Web-Bestätigung. Dabei verarbeitet DEKObyte personenbezogene Daten im Auftrag des Kunden. Dieser Vertrag regelt diese Verarbeitung nach Art. 28 DSGVO.

§ 1 Begriffe

(1) „Dienst“ ist die Web-Bestätigung unter confirm.palettenkonto.net, einschließlich der Schnittstelle, über die der Connector des Kunden Daten liefert und Antworten abholt.

(2) „Connector“ ist das Programm auf einem Rechner des Kunden, das Salden und Stammdaten aus der Palettenkonto-Datenbank des Kunden an den Dienst übermittelt und die Antworten der Tauschpartner abholt.

(3) „Tauschpartner“ sind die Geschäftspartner des Kunden, mit denen der Kunde über den Dienst Palettensalden abstimmt.

(4) „Aufstellung“ ist die Saldenaufstellung, die ein Tauschpartner über seinen persönlichen Link sieht und beantwortet.

(5) „Beleg“ ist das PDF über die Antwort eines Tauschpartners. „Entscheidungsprotokoll“ sind die nur anhängbaren Einträge des Dienstes über Antworten und Vorgänge.

(6) „Mandant“ ist der Bereich des Kunden im Dienst.

(7) „Hauptvertrag“ sind die Nutzungsbedingungen für die Web-Bestätigung mit Leistungsbeschreibung, die der Kunde mit seinem Antrag annimmt.

(8) „Auftragsverarbeiter“ in diesem Vertrag ist DEKObyte. „Unterauftragsverarbeiter“ sind die weiteren Auftragsverarbeiter nach Anlage 3.

(9) „Werktag“ ist Montag bis Freitag, außer an gesetzlichen Feiertagen in Niedersachsen.

§ 2 Gegenstand, Rollen und Aufgaben von DEKObyte

(1) DEKObyte stellt dem Kunden den Dienst nach dem Hauptvertrag bereit und verarbeitet dabei personenbezogene Daten im Auftrag des Kunden. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten und die Kategorien betroffener Personen beschreibt Anlage 1.

(2) Für die Daten seiner Tauschpartner ist allein der Kunde Verantwortlicher. DEKObyte ist sein Auftragsverarbeiter. DEKObyte betreibt den Dienst und setzt dafür die Unterauftragsverarbeiter nach Anlage 3 ein.

(3) DEKObyte nimmt die Weisungen des Kunden an, setzt sie um und gibt sie, soweit sie einen Unterauftragsverarbeiter betreffen, an diesen weiter. DEKObyte ist Anlaufstelle für Anfragen betroffener Personen und für Verletzungen des Schutzes personenbezogener Daten. DEKObyte leistet den Support; auf Daten der Tauschpartner greift DEKObyte nur zu, soweit Betrieb und Support es erfordern. DEKObyte kontrolliert seine Unterauftragsverarbeiter.

(4) DEKObyte haftet dem Kunden dafür, dass jeder Unterauftragsverarbeiter die Pflichten aus diesem Vertrag erfüllt (Art. 28 Abs. 4 Satz 2 DSGVO).

§ 3 Dauer

(1) Dieser Vertrag kommt zustande, wenn DEKObyte den Antrag annimmt, mit dem der Kunde diesen Vertrag in der dort genannten Fassung annimmt. Erklärungen per E-Mail genügen (Art. 28 Abs. 9 DSGVO).

(2) Dieser Vertrag gilt, solange der Hauptvertrag gilt. Der Hauptvertrag endet nach seinen Regeln (Nutzungsbedingungen § 4 und § 5): durch Kündigung, auch nach § 8 Abs. 3 dieses Vertrags; bei einem Antrag bis zum Stichtag ohne ausdrückliche kostenpflichtige Verlängerung mit Ablauf des Tages, an dem die kostenlose Nutzung dieses Kunden nach den Nutzungsbedingungen (§ 4 Abs. 2 bis 5) endet; nach einer kostenpflichtigen Verlängerung und bei einem von Anfang an kostenpflichtigen Antrag nach den dann mitgeteilten Bedingungen.

(3) Endet der Hauptvertrag, gilt dieser Vertrag für die Archivphase fort, bis alle Daten nach § 10 gelöscht oder herausgegeben sind.

§ 4 Weisungen

(1) DEKObyte verarbeitet die Daten nur auf dokumentierte Weisung des Kunden (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Weisungen sind der Hauptvertrag, dieser Vertrag mit seinen Anlagen und Einzelweisungen des Kunden in Textform.

(2) Weisungen gehen vom Kunden an DEKObyte. Betrifft eine Weisung einen Unterauftragsverarbeiter, gibt DEKObyte sie an ihn weiter. DEKObyte dokumentiert jede Einzelweisung und ihre Weitergabe mit Datum.

(3) Hält DEKObyte eine Weisung für rechtswidrig, weist DEKObyte den Kunden unverzüglich darauf hin (Art. 28 Abs. 3 Unterabs. 2 DSGVO). Weisungen, Belege oder Protokolleinträge zu verändern, führt DEKObyte nicht aus (§ 11).

(4) Weisungen nimmt DEKObyte unter info@palettenkonto.net entgegen. Weisungsberechtigt beim Kunden sind der im Antrag genannte Ansprechpartner und die gesetzlichen Vertreter des Kunden.

§ 5 Zweckbindung

Der Auftragsverarbeiter und seine Unterauftragsverarbeiter verarbeiten die Daten des Kunden und seiner Tauschpartner ausschließlich zur Erbringung des Dienstes nach der Leistungsbeschreibung und nach Weisung des Kunden. Sie verwenden sie insbesondere nicht für eigene Werbung, nicht zur Kontaktaufnahme mit Tauschpartnern außerhalb des Dienstes und nicht für Auswertungen über den einzelnen Kunden hinaus, und sie geben sie nicht an Dritte weiter. Zahlen ohne Personenbezug je Mandant (etwa die Zahl versandter Mails) dürfen für Betrieb und Abrechnung verwendet werden.

§ 6 Vertraulichkeit

(1) DEKObyte setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b DSGVO). Dieselbe Pflicht legt DEKObyte den Unterauftragsverarbeitern auf.

(2) Zugriff auf Daten der Tauschpartner erhält eine Person nur, soweit ihre Aufgabe ihn erfordert.

§ 7 Technische und organisatorische Maßnahmen

(1) DEKObyte trifft die Maßnahmen nach Art. 32 DSGVO, die Anlage 4 beschreibt, und sorgt dafür, dass die Unterauftragsverarbeiter die Maßnahmen umsetzen, die ihre Leistung betreffen.

(2) Anlage 4 beschreibt die Maßnahmen wahrheitsgemäß, einschließlich ihrer Grenzen. Maßnahmen, die erst mit einem späteren Update des Dienstes wirken, sind dort mit ihrem Zeitpunkt gekennzeichnet.

(3) DEKObyte darf die Maßnahmen der Anlage 4 an die technische Entwicklung anpassen und durch gleichwertige ersetzen, wenn das Schutzniveau dadurch nicht sinkt. DEKObyte dokumentiert jede Änderung und teilt wesentliche Änderungen dem Kunden in Textform mit.

§ 8 Unterauftragsverarbeiter

(1) Der Kunde genehmigt den Einsatz der in Anlage 3 („Unterauftragsverarbeiter“) genannten weiteren Auftragsverarbeiter (allgemeine schriftliche Genehmigung nach Art. 28 Abs. 2 DSGVO).

(2) DEKObyte informiert den Kunden in Textform, per E-Mail an die im Antrag für Mitteilungen zum Vertrag genannte Adresse (Nutzungsbedingungen § 13), mindestens vier Wochen vorher über jede beabsichtigte Hinzuziehung oder Ersetzung oder Änderung von Leistung oder Ort der Verarbeitung. Die Information nennt Firma, Anschrift, Leistung, Ort der Verarbeitung, den geplanten Beginn und bei einer Übermittlung in ein Drittland deren Grundlage. Neue Programmfassungen fallen nicht unter Satz 1.

(3) Der Kunde kann bis zum geplanten Einsatz aus datenschutzrechtlichen Gründen in Textform unter Angabe der Gründe Einspruch erheben. Hält DEKObyte an der Änderung fest, kann der Kunde den Hauptvertrag und diesen Vertrag zum Zeitpunkt des Einsatzes ohne Kosten kündigen.

(4) Fällt ein Unterauftragsverarbeiter unvorhergesehen aus, darf DEKObyte auf einen in Anlage 3 bereits für diese Leistung genannten Anbieter umstellen. DEKObyte informiert den Kunden unverzüglich.

(5) DEKObyte verpflichtet jeden Unterauftragsverarbeiter vertraglich auf die Pflichten dieses Vertrags und stellt sicher, dass dieser seine weiteren Auftragsverarbeiter ebenso verpflichtet.

(6) Die Daten werden in Deutschland verarbeitet. In ein Land außerhalb der EU und des EWR werden sie nicht übermittelt; eine solche Übermittlung wäre eine Änderung nach Absatz 2.

§ 9 Rechte betroffener Personen

(1) Anfragen betroffener Personen beantwortet der Kunde. Gehen sie bei DEKObyte oder einem Unterauftragsverarbeiter ein, werden sie unverzüglich, spätestens am folgenden Werktag, an den Kunden weitergeleitet; der betroffenen Person wird nur die Weiterleitung bestätigt. Der Auftragsverarbeiter stellt dem Kunden auf Anforderung innerhalb von fünf Werktagen alle zu einer betroffenen Person gespeicherten Daten in einem gängigen Format zur Verfügung und führt Löschungen, Berichtigungsvermerke und Einschränkungen nach Weisung aus. Auf Weisung in Textform beantwortet DEKObyte Anfragen im Namen des Kunden.

(2) Zu den Daten nach Absatz 1 gehören die Stammdaten des Tauschpartners, seine Aufstellungen, Entscheidungen und Belege, die Einträge des Entscheidungsprotokolls mit IP-Adresse und Browserkennung und die Versanddaten. Auf Verlangen nennt DEKObyte die konkreten Empfänger.

(3) Berichtigt der Kunde Stammdaten im Palettenkonto, übernimmt der nächste Upload sie. Belege und Protokolleinträge bleiben unverändert; einen Einwand der betroffenen Person ergänzt DEKObyte auf Weisung des Kunden als Vermerk.

(4) Möchte ein Tauschpartner keine Bestätigungsanfragen mehr erhalten, setzt der Kunde ihn im Palettenkonto auf inaktiv oder ändert die Adresse; der Dienst schreibt ihn dann nicht mehr an.

(5) Für die Antwort auf ein Löschverlangen während der Aufbewahrungsfristen stellt DEKObyte dem Kunden eine Antwortvorlage auf Deutsch und Englisch bereit (Anhang der Kundenanleitung).

§ 10 Aufbewahrung und Löschung

(1) Der Auftragsverarbeiter speichert die Daten nach den Fristen der Anlage „Löschkonzept“ (Anlage 2; Standardfristen). Der Kunde teilt mit, ob er Kaufmann oder nach Steuergesetzen zur Führung von Büchern oder Aufzeichnungen verpflichtet ist. Will der Kunde andere Fristen, vereinbaren die Parteien sie vor dem ersten Versand in Textform; der Kunde informiert seine Tauschpartner dann selbst über die abweichenden Fristen, bevor ihnen die erste E-Mail zugeht.

(2) Belege und die zugehörigen Einträge des Entscheidungsprotokolls werden während der Frist nicht verändert. Sie werden während der Frist nur zur Aufbewahrung, zur Bereitstellung an den Kunden nach Absatz 2a, zur Beantwortung von Anfragen des Kunden und betroffener Personen und zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Kunden verwendet.

(2a) Während der Fristen stellt der Auftragsverarbeiter dem Kunden auf Anforderung unverzüglich, spätestens innerhalb von fünf Werktagen, die Belege und das Entscheidungsprotokoll eines Zeitraums als Kopie zur Verfügung: die Belege als PDF mit SHA-256-Prüfsummen, das Protokoll in einem maschinell auswertbaren Format. Verlangt die Finanzbehörde im Rahmen einer Außenprüfung Zugriff auf diese Daten (§ 147 Abs. 6 AO), wirkt der Auftragsverarbeiter mit. Die gespeicherten Belege bleiben davon unberührt.

(3) Nach Fristablauf löscht der Auftragsverarbeiter die Daten innerhalb von drei Monaten in einem protokollierten Löschlauf. Das Löschprotokoll nennt Datenkategorie, Mandant, Zeitraum, Zahl der gelöschten Einträge und Zeitpunkt und enthält keine personenbezogenen Daten. Sicherungskopien werden nicht einzeln bereinigt; sie werden nach höchstens 30 Tagen überschrieben. Wird eine Sicherung zurückgespielt, läuft der Löschlauf erneut, bevor der Dienst wieder Anfragen annimmt. Ab wann der Löschlauf in Betrieb ist, steht in Anlage 2 Nr. 2.4.

(4) Verlangt eine betroffene Person Löschung, leitet der Auftragsverarbeiter das Verlangen unverzüglich, spätestens am folgenden Werktag, an den Kunden weiter. Er löscht nur auf Weisung des Kunden in Textform.

(5) Endet der Hauptvertrag, gilt dieser Vertrag für die Archivphase fort. In ihr speichert der Auftragsverarbeiter Belege, Entscheidungsprotokoll und die zugehörigen Aufstellungen bis zum Ablauf der Fristen nach Absatz 1 und löscht sie dann, es sei denn, der Kunde verlangt in Textform Herausgabe und Löschung. Auf Verlangen erhält der Kunde vorher eine vollständige Kopie nach Absatz 2a. Während der Archivphase verarbeitet der Auftragsverarbeiter die Daten nur noch zur Aufbewahrung, zur Herausgabe an den Kunden, zur Mitwirkung nach § 147 Abs. 6 AO und zur Beantwortung von Anfragen nach Weisung. Alle übrigen Daten werden spätestens drei Monate nach Ende des Hauptvertrags gelöscht.

(6) Der Tauschpartner kann seinen Beleg über die Links in seinen E-Mails bis zwölf Monate nach seiner Antwort erneut herunterladen, in der Archivphase nicht.

(7) Fordert der Kunde über den Support von DEKObyte unter Angabe der Vorgangsnummer den genauen Wortlaut einer Antwort seines Tauschpartners an, liest DEKObyte ihn aus dem Entscheidungsprotokoll und übermittelt ihn dem Kunden innerhalb von fünf Werktagen. Weitere Daten werden dabei nicht übermittelt.

§ 11 Belege bleiben unverändert

Der Kunde weist den Auftragsverarbeiter an, Belege und Entscheidungsprotokoll unverändert und für den Kunden nicht änderbar bis zum Ablauf der Fristen nach Anlage „Löschkonzept“ aufzubewahren. Eine Löschung vor Fristablauf erfolgt nur auf ausdrückliche Weisung des Kunden in Textform und wird mit Datum und Umfang protokolliert. Weisungen, Belege oder Protokolleinträge zu verändern, führt der Auftragsverarbeiter nicht aus; er weist den Kunden auf die Rechtswidrigkeit hin.

§ 12 Ende des Hauptvertrags: Mandant beenden, Export, Archivphase

(1) Endet der Hauptvertrag, gleich aus welchem Grund, beendet DEKObyte den Mandanten des Kunden nur in diesem Ablauf und protokolliert jeden Schritt mit Zeitpunkt:

1. Der Mandant wird deaktiviert.
2. Ab dann nimmt der Dienst über die Links dieses Kunden keine neue Antwort mehr an und bittet die Tauschpartner, sich direkt an den Kunden zu wenden. Wer schon geantwortet hat, erhält seinen Beleg bis zur Grenze nach § 10 Abs. 6 weiter.
3. Offene Antworten holt der Connector des Kunden während der Abholfrist der Nutzungsbedingungen (§ 6 Abs. 1) noch ab. Ist der Connector schon entfernt, übergibt DEKObyte sie dem Kunden als Export. Antworten, die nicht an das Palettenkonto weitergegeben wurden, teilt DEKObyte dem Kunden mit.
4. Erst dann wird das letzte Zertifikat widerrufen.
5. Die Daten gehen in die Archivphase nach § 10 Abs. 5 über oder werden gelöscht.

Ein bloßer Widerruf des Zertifikats beendet einen Mandanten nicht.

Schritt 1 folgt am Tag nach dem Ende des Hauptvertrags, vor dem täglichen Versandlauf. Die Archivphase beginnt mit Schritt 5. Die Abholfrist beträgt 30 Tage (Nutzungsbedingungen § 6 Abs. 1).

(2) Mit dem Ende des Hauptvertrags teilt DEKObyte dem Kunden den letzten Tag der Abholfrist mit.

(3) Nach dem Ende des Hauptvertrags erhebt der Dienst keine neuen Daten der Tauschpartner mehr. Die schon gespeicherten Belege und das Entscheidungsprotokoll bewahrt DEKObyte nach § 10 Abs. 5 auf; alles Übrige wird nach Art. 28 Abs. 3 Satz 2 lit. g DSGVO gelöscht oder zurückgegeben.

(4) Nach dem Ende des Hauptvertrags kann der Kunde seine Daten im Dienst – Entscheidungen seiner Tauschpartner, Belege und Protokoll – noch mindestens 30 Tage lang als Export (Belege als PDF, Daten in einem maschinenlesbaren Format) bei DEKObyte anfordern. Danach werden sie gelöscht, soweit sie nicht nach § 10 bis zum Ablauf der Aufbewahrungsfristen aufbewahrt werden. Was nicht in die Archivphase geht, wird erst nach diesen 30 Tagen gelöscht, spätestens drei Monate nach dem Ende des Hauptvertrags.

(5) Die Vergütung der Archivphase regelt der Hauptvertrag; sie ist kostenfrei (Nutzungsbedingungen § 6 Abs. 4).

§ 13 Mitteilungen von Tauschpartnern; Postfach des Absenders

(1) Für Rückfragen und Einwände verweist der Dienst die Tauschpartner direkt an den Kunden. DEKObyte und seine Unterauftragsverarbeiter treten den Tauschpartnern gegenüber außerhalb des Dienstes nicht als Empfangsstelle für Mitteilungen an den Kunden auf; dass der Dienst Empfangseinrichtung des Kunden für die Antworten ist (Nutzungsbedingungen § 7), § 2 Abs. 3, § 9 und Absatz 2 bleiben unberührt.

(2) Erhält DEKObyte oder ein Unterauftragsverarbeiter Mitteilungen eines Tauschpartners des Kunden, mit denen dieser eine über die Web-Bestätigung abgegebene Antwort zurücknehmen, anfechten oder berichtigen will, leitet DEKObyte sie unverändert und unverzüglich, spätestens am folgenden Werktag, an den Kunden weiter und hält Eingang und Weiterleitung mit Datum fest.

(3) Die Absenderadresse der E-Mails an die Tauschpartner, technik@confirm.palettenkonto.net, ist ein Postfach von DEKObyte. Mails dorthin, die keine Alarme sind, sichtet DEKObyte werktäglich. Anfragen nach Art. 15 bis 21 DSGVO und Mitteilungen nach Absatz 2 leitet DEKObyte unverzüglich, spätestens am folgenden Werktag, an den Kunden weiter.

§ 14 Verletzungen des Schutzes personenbezogener Daten; weitere Unterstützung

(1) DEKObyte meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt; fehlende Angaben werden nachgereicht. Die Meldung hängt nicht davon ab, ob die Verletzung voraussichtlich zu einem Risiko führt.

(2) Eine Verletzung nach Absatz 1 ist auch eine Belegkopie, die an eine Adresse gegangen ist, die einem Unbefugten gehört (Fehlzustellung eines Belegs). Erfährt DEKObyte davon, meldet DEKObyte es dem Kunden unverzüglich.

(3) Bei Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen (Art. 33, 34 DSGVO), bei einer Datenschutz-Folgenabschätzung und bei einer vorherigen Konsultation (Art. 35, 36 DSGVO) unterstützt DEKObyte den Kunden mit den Informationen, die DEKObyte und seinen Unterauftragsverarbeitern vorliegen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO).

(4) Meldungen an den Kunden gehen an die E-Mail-Adresse, die der Kunde im Antrag für Mitteilungen zum Vertrag genannt hat (Nutzungsbedingungen § 13).

§ 15 Nachweise, Kontrollen, Verzeichnis

(1) DEKObyte stellt dem Kunden auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Pflichten aus diesem Vertrag nötig sind (Art. 28 Abs. 3 Satz 2 lit. h DSGVO): Anlage 4 in der geltenden Fassung, Anlage 3, die datenschutzrelevanten Teile der Verträge mit den Unterauftragsverarbeitern und vorhandene Nachweise der Rechenzentrumsbetreiber, etwa Zertifikate nach ISO 27001.

(2) Der Kunde kann die Einhaltung dieses Vertrags selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer bei DEKObyte kontrollieren; DEKObyte ermöglicht das und wirkt mit. Kontrollen vor Ort kündigt der Kunde mindestens zwei Wochen vorher in Textform an; sie finden zu den Geschäftszeiten statt, ohne besonderen Anlass höchstens einmal im Kalenderjahr. Jede Partei trägt ihre Kosten.

(3) Für die Rechenzentren der Unterauftragsverarbeiter genügen deren Nachweise nach Absatz 1.

(4) DEKObyte führt ein Verzeichnis nach Art. 30 Abs. 2 DSGVO.

§ 16 Angaben und Pflichten des Kunden; Information der Tauschpartner

(1) Der Kunde ist als Verantwortlicher für die Zulässigkeit der Verarbeitung gegenüber seinen Tauschpartnern verantwortlich. Er legt die Aufbewahrungsfristen fest (§ 10 Abs. 1) und beantwortet Anfragen betroffener Personen (§ 9).

(2) Der Kunde teilt im Antrag mit, ob er Kaufmann oder nach Steuergesetzen zur Führung von Büchern oder Aufzeichnungen verpflichtet ist und ob er die Standardfristen der Anlage 2 übernimmt.

(3) Der Kunde stellt, bevor der erste Link zur Bestätigung per Mail hinausgeht, seinen Namen, seine Anschrift, eine E-Mail-Adresse für Datenschutzanfragen und gegebenenfalls den Kontakt seines Datenschutzbeauftragten zur Verfügung. DEKObyte stellt einen Datenschutzhinweis bereit, den der Kunde als Information nach Art. 13 und 14 DSGVO gegenüber seinen Tauschpartnern verwendet; der Kunde prüft ihn und teilt Abweichungen mit. Der Hinweis nennt die Standardfristen; vereinbart der Kunde andere Fristen, informiert er seine Tauschpartner insoweit selbst.

(4) Ohne die Angaben nach Absatz 2 und 3 richtet DEKObyte den Mandanten nicht ein und gibt den Versand nicht frei; es geht kein Link zur Bestätigung per Mail hinaus.

(5) Der Kunde stellt sicher, dass seine allgemeine Datenschutzinformation für Geschäftspartner Dienstleister für Software und Hosting als Empfänger nennt. Für Tauschpartner, die der Dienst anschreibt, stellt DEKObyte den Datenschutzhinweis unter https://confirm.palettenkonto.net/datenschutz (englisch: https://confirm.palettenkonto.net/datenschutz/en) bereit.

(6) Ändern sich die Angaben nach Absatz 2 und 3, teilt der Kunde das DEKObyte unverzüglich mit.

§ 17 Hinweis des Herstellers nach der Antwort

(1) Nach der Antwort des Tauschpartners zeigt der Dienst auf der Abschlussseite einen als Hinweis von DEKObyte gekennzeichneten Hinweis auf die Software Palettenkonto mit Links auf palettenkonto.net; dazu gehört ein Link auf palettenkonto.net im Fuß der Danke- und der Abschlussseite (Herstellerhinweis). Der Herstellerhinweis erscheint nicht vor der Antwort, nicht in E-Mails und nicht im Beleg. Der Kunde weist DEKObyte an, den Herstellerhinweis als Teil des Dienstes anzuzeigen, solange er ihn nicht nach Absatz 3 abschaltet.

(2) Der Herstellerhinweis ist für alle Empfänger gleich. Für ihn werden personenbezogene Daten des Kunden und seiner Tauschpartner weder verwendet noch ausgewertet noch weitergegeben. Die Links tragen ausschließlich feste, für alle Empfänger gleiche Kampagnenangaben und keine Kennung des Kunden, des Tauschpartners oder des Vorgangs. Der Dienst erfasst nicht, wer den Hinweis sieht oder anklickt, und setzt dafür keine Cookies, Zählpixel oder vergleichbaren Techniken ein. DEKObyte und seine Unterauftragsverarbeiter nehmen aus Anlass des Dienstes keinen Kontakt zu Tauschpartnern des Kunden auf, es sei denn, der Tauschpartner fordert ihn selbst an, etwa über palettenkonto.net. Ruft ein Tauschpartner palettenkonto.net auf, ist DEKObyte für die dortige Verarbeitung selbst verantwortlich.

(3) Der Kunde kann den Herstellerhinweis jederzeit ohne Angabe von Gründen und ohne Mehrkosten durch Mitteilung in Textform an DEKObyte abschalten lassen. DEKObyte setzt die Abschaltung innerhalb von fünf Werktagen um und bestätigt sie in Textform. Die Abschaltung gilt für alle Tauschpartner des Kunden.

(4) Der Herstellerhinweis erscheint nur auf den deutschsprachigen Seiten.

§ 18 Haftung

Für die Haftung gilt der Hauptvertrag (Nutzungsbedingungen § 12). Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

§ 19 Schlussbestimmungen

(1) Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag vor, soweit es um die Verarbeitung personenbezogener Daten geht.

(2) Es gilt dieser Vertrag in der Fassung, deren Datum der Antrag nennt: Fassung vom 03.11.2026, abrufbar unter https://palettenkonto.net/vertragsunterlagen/. DEKObyte bewahrt jede Fassung als PDF auf.

(3) Änderungen dieses Vertrags vereinbaren die Parteien in Textform. DEKObyte schickt eine neue Fassung jedem Kunden einzeln per E-Mail an die im Antrag für Mitteilungen zum Vertrag genannte Adresse (Nutzungsbedingungen § 13). Für Änderungen der Unterauftragsverarbeiter gilt § 8, für Anpassungen der Anlage 4 § 7 Abs. 3.

Anlage 1 · Gegenstand, Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen

1.1 Gegenstand

- Der Connector übermittelt regelmäßig und verschlüsselt die Salden des letzten abgeschlossenen Monats mit den Stammdaten der Tauschpartner an den Dienst.
- Gibt es für einen Tauschpartner etwas zu beantworten, schickt der Dienst ihm nach einem Monatsende höchstens einmal im Monat einen persönlichen Link zur Bestätigung per Mail, der zu einer Aufstellung führt, und, solange er nicht antwortet, bis zu zwei Erinnerungen. Salden ohne Bewegung fragt der Dienst nicht ab.
- Der Tauschpartner bestätigt oder korrigiert online. Der Dienst speichert die Antwort, erzeugt einen Beleg, schickt dem Tauschpartner eine Kopie per E-Mail und stellt die Antwort dem Connector zum Abholen bereit.
- Der Dienst bewahrt Belege, Entscheidungsprotokoll und Aufstellungen nach Anlage 2 auf und stellt sie dem Kunden nach § 10 Abs. 2a bereit.
- DEKObyte betreibt den Dienst, gibt im Versandmodus „nur nach Freigabe“ Empfängeradressen vor der ersten E-Mail frei, stellt die Zertifikate für den Connector aus und leistet den Support.
- Den Versandmodus („automatisch“ oder „nur nach Freigabe“) wählt der Kunde; die Wahl ist seine Weisung nach § 4. DEKObyte fragt sie vor der Einrichtung per E-Mail beim Kunden ab; der Kunde teilt sie in Textform mit.

Der Herstellerhinweis nach § 17 verwendet keine personenbezogenen Daten.

Nicht Gegenstand dieses Vertrags sind Daten, die der Connector auf dem Rechner des Kunden speichert, und Daten, die DEKObyte für Abschluss und Abwicklung des Hauptvertrags mit dem Kunden selbst verarbeitet (etwa Ansprechpartner und Rechnungsanschrift).

1.2 Art der Verarbeitung

Erheben (Upload durch den Connector, Eingaben des Tauschpartners), Speichern, Abgleichen und Aufbereiten zu Aufstellungen, Versenden per E-Mail, Erzeugen von Belegen, Übermitteln an den

Kunden, Bereitstellen an den Tauschpartner, Aufbewahren, Einschränken, Löschen und Schwärzen, Export.

1.3 Zwecke

1. Saldo abstimmen: Aufstellungen nach einem Monatsende, wenn es für den Tauschpartner etwas zu beantworten gibt, bis zu zwei Erinnerungen je Aufstellung, Antwort entgegennehmen und an den Kunden übermitteln.
2. Die Antwort nachweisbar festhalten: Beleg und Kopie für den Tauschpartner per E-Mail.
3. Aufbewahrung nach Weisung des Kunden (§ 10, § 11).
4. Sicherheit: Prüfung und Freigabe von Adressen im Versandmodus „nur nach Freigabe“, den der Kunde gewählt hat (1.1); Schutz vor massenhaftem Ausprobieren von Links.
5. Unterstützung des Kunden: Support, Kopien, Auskunft, Wortlaut aus dem Protokoll (§ 9, § 10 Abs. 2a und 7).
6. Betrieb und Abrechnung, nur mit Zahlen ohne Personenbezug (§ 5).

1.4 Art der Daten

Gruppe	Daten	Herkunft
Stammdaten der Tauschpartner	Kurzbezeichnung, Referenznummer, Bezeichnung (Firma oder Name, zwei Zeilen), Land, E-Mail-Adresse, Kennzeichen „inaktiv“; auch für Tauschpartner, die der Dienst nie anschreibt	Connector (Palettenkonto des Kunden)
Salden und Buchungen	Salden je Ladungsträger, Übertrag als Summe, Einzelbuchungen mit Belegnummer, Zeitpunkt, Mengen und den Freitexten „Kopftext“ und „Bemerkung“	Connector
Eigene Firma des Kunden	Bezeichnung und E-Mail-Adresse aus den Stammdaten (Antwortadresse der Mails an Tauschpartner)	Connector
Pflichtangaben des Kunden	rechtlicher Name, Anschrift, E-Mail-Adresse für Datenschutzanfragen, Kontakt des Datenschutzbeauftragten (falls benannt)	Antrag
Abrufdaten	Zeitpunkt, IP-Adresse und Browserkennung beim ersten Öffnen eines Links; Zahl der Aufrufe ohne IP-Adresse; Zeitpunkt des letzten Aufrufs	Browser des Öffnenden
Antworten	je Ladungsträger „Bestätigen“ oder „Korrigieren“, je Einzelbuchung Zustimmung oder Widerspruch, eine genannte Zahl, Begründung oder Kommentar; beim Absenden Zeitpunkt, IP-Adresse, Browserkennung und Anzeigesprache	Tauschpartner
Ratenbremse	IP-Adresse, je Zugriffsart und Stunde gezählt	Browser des Öffnenden
Versand und Zustellung	Empfängeradresse, Versandart und -zeit, Kennung des Mailversands, Unzustellbarkeitsmeldungen mit Adresse	Dienst
Belege	PDF mit Salden, Antwort, Zeitpunkt, IP-Adresse, Browserkennung; Prüfsumme	Dienst
Entscheidungsprotokoll	Einträge zu Entscheidungen und Belegen, Freigabe und Sperre von Adressen mit Notiz oder Grund, Unzustellbarkeit	Dienst
Kommandos an den Connector	Entscheidung, Kopie des Kommentars, Adresse („bestätigt von“), Zeitpunkt	Dienst

Gruppe	Daten	Herkunft
Hinweise an den Connector	etwa zur Unzustellbarkeit: betroffene E-Mail-Adresse, Text und Einzelheiten	Dienst
Mitteilungen und Anfragen	Inhalt von E-Mails der Tauschpartner an DEKObyte und an technik@confirm.palettenkonto.net	Tauschpartner
Betriebsdaten	Laufprotokoll, Befunde der Überwachung mit Mandantenkürzel	Dienst

Ist der Tauschpartner eine juristische Person, sind die Salden selbst keine personenbezogenen Daten; die übrigen Daten sind es meist trotzdem. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht vorgesehen.

1.5 Betroffene Personen

- Tauschpartner des Kunden, soweit sie natürliche Personen sind, insbesondere Einzelunternehmer.
- Mitarbeiter und Ansprechpartner der Tauschpartner, deren Namen oder Adressen in Stammdaten, E-Mails oder Antworten vorkommen, und Personen, die einen Link öffnen oder über ihn antworten.
- Personen, die in Freitexten genannt sind (Buchungstexte, Bemerkungen, Kommentare).
- Ansprechpartner und Beschäftigte des Kunden, soweit ihre Daten im Dienst stehen (Antwortadresse, Pflichtangaben, Datenschutzbeauftragter).

1.6 Ort und Dauer

Ort der Verarbeitung ist Deutschland; eine Übermittlung in ein Drittland findet nicht statt (§ 8 Abs. 6, Anlage 3). Die Dauer richtet sich nach § 3, die Speicherfristen nach Anlage 2.

Anlage 2 · Löschkonzept

Die Fristen legt der Kunde als Verantwortlicher fest. Diese Anlage bringt Standardfristen mit, die der Kunde mit dem Antrag übernimmt oder nach § 10 Abs. 1 durch andere ersetzt.

2.1 Standardfristen

Daten	Standardfrist	Grund
Beleg (PDF, einschließlich der darauf gedruckten IP-Adresse und Browserkennung)	Ende des 8. Kalenderjahres nach dem Jahr der Entscheidung	§ 257 Abs. 1 Nr. 2 und 4, Abs. 4 HGB; § 147 Abs. 1 Nr. 2 und 4, Abs. 3 AO; Art. 17 Abs. 3 lit. b und e
Entscheidung (`confirmations`, `confirmation_lines`), audit_log-Einträge `entscheidung` und `beleg_erzeugt`, `mail_jobs` und `magic_links` der beantworteten Aufstellung	wie der Beleg	wie oben; für IP und Browserkennung in diesen Tabellen: Art. 17 Abs. 3 lit. e, Art. 6 Abs. 1 lit. f (Zurechnung der Erklärung)
Aufstellung, auf die geantwortet wurde (`balance_snapshots`, `snapshot_lines`, `snapshot_buchungen`)	wie der Beleg	Gegenstand der Erklärung

Daten	Standardfrist	Grund
Freigabe der Adresse, an die ein beantworteter Link ging (audit_log)	wie der Beleg	Zurechnung der Antwort
IP und Browserkennung beim ersten Öffnen eines Links (`angesehen`) zu einer beantworteten Aufstellung	Ende des 3. Kalenderjahres nach dem Jahr der Entscheidung; dann Felder schwärzen, Zeitpunkt und Zahl bleiben	Regelverjährung, §§ 195, 199 BGB; Art. 6 Abs. 1 lit. f
Aufstellung, `magic_links` und `mail_jobs` ohne Antwort	Ende des 6. Kalenderjahres nach dem Versand	§ 257 Abs. 1 Nr. 3 HGB, § 147 Abs. 1 Nr. 3 AO
IP und Browserkennung beim ersten Öffnen eines Links ohne Entscheidung	6 Monate nach Ablauf des Links; dann Felder schwärzen. Ein Link gilt 14 Tage; die Frist endet also spätestens sechs Monate und 14 Tage nach dem Versand	Datenminimierung; monatliche Wiederholung bei Partnern ohne Antwort
`uploads.payload` zu einer aufbewahrten Aufstellung	90 Tage nach Ablauf des letzten Links auf die Teile kürzen, auf die sich eine aufbewahrte Aufstellung bezieht; Periode, Stichtag und Salden bleiben vollständig, es entfallen nur Stammdaten von Tauschpartnern, die von keiner aufbewahrten Aufstellung betroffen sind	Art. 5 Abs. 1 lit. c, Abs. 2
Uploads ohne eingefrorene Aufstellung	löschen, sobald ein neuerer Upload derselben Periode eingefroren ist, spätestens nach 90 Tagen	
`commands`	90 Tage nach Quittung durch den Connector	Die Entscheidung steht in `confirmations`
Übrige Freigabe-, Sperr- und Unzustellbarkeitseinträge (audit_log, `hinweise`)	6 Monate, nachdem die Adresse ersetzt oder der Partner entfernt wurde	
Partnerstammdaten (`partners`)	solange der Kunde sie hochlädt; danach 90 Tage, soweit aufbewahrte Daten sie nicht brauchen	
Ratenbremse (IP-Adresse)	höchstens 2 Tage	Art. 32
Betriebsdaten (`laufprotokoll`, `befunde`)	90 Tage	
Webserver- und Containerprotokolle	ohne Token; IP-Adressen nur bei abgewiesenen Zugriffen auf Betriebs- und Webhook-Endpunkte; zusätzlich höchstens 14 Tage für alle Containerprotokolle	Art. 5 Abs. 1 lit. e, Art. 32
Sicherungen	Überschreiben nach 30 Tagen	
Abruf des Belegs durch den Tauschpartner über die Links	bis zwölf Monate nach seiner Antwort; in der Archivphase nicht	Datenminimierung (Art. 5 Abs. 1 lit. b, c und f, Art. 32)
Mitteilungen und Anfragen von Tauschpartnern sowie Alarmberichte in den Postfächern von DEKObyte (info@palettenkonto.net, technik@confirm.palettenkonto.net)	nach der Auffangregel (letzte Zeile)	
Auffangregel: alle übrigen Daten und Protokolleinträge	wie die Aufstellung, auf die sie sich beziehen; ohne solchen Bezug 90 Tage	

2.2 Fristbeginn und Verlängerung

Die Fristen nach Kalenderjahren beginnen mit dem Schluss des Kalenderjahres, in dem der Brief empfangen oder abgesandt wurde oder die Entscheidung fiel. Solange Unterlagen für eine noch nicht abgelaufene steuerliche Festsetzungsfrist von Bedeutung sind, verlängert der Kunde die Frist für diese Unterlagen durch Weisung in Textform.

2.3 Abweichende Fristen

- Ist der Kunde weder Kaufmann noch nach Steuergesetzen zur Führung von Büchern oder Aufzeichnungen verpflichtet, schlägt DEKObyte als abweichende Frist nach § 10 Abs. 1 vor: Beleg, Entscheidung und beantwortete Aufstellung bis zum Ende des 4. Kalenderjahres nach dem Jahr der Entscheidung.
- Führt der Kunde die Bestätigungen als Teil seines Inventars, gelten auf seine Weisung 10 Jahre.
- Vereinbart der Kunde andere Fristen, informiert er seine Tauschpartner selbst, bevor ihnen die erste E-Mail zugeht; für ihn gilt der Datenschutzhinweis insoweit nicht.

2.4 Wie gelöscht wird

Gelöscht oder geschwärzt wird in einem eigenen, protokollierten Löschlauf über eine eigene Rolle, nicht über die Anwendungsrolle des Dienstes. Der Löschlauf erfasst auch deaktivierte Mandanten und Mandanten in der Archivphase. Das Löschprotokoll ist nur anhängbar und enthält keine personenbezogenen Daten (§ 10 Abs. 3). Der Löschlauf kommt mit einem Folge-Update, spätestens 90 Tage nachdem der Dienst die ersten Kundendaten verarbeitet hat, also vor der ersten fälligen Löschung.

2.5 Ende des Hauptvertrags

Ablauf, Export und Archivphase: § 10 Abs. 5 und § 12. Die Archivphase ist kostenfrei (§ 12 Abs. 5). Nach Ablauf der Abrufdauer und in der Archivphase zeigt die Seite dem Tauschpartner statt des Belegs: „Eine Kopie Ihres Belegs erhalten Sie auf Anfrage bei {firma}.“

Anlage 3 · Unterauftragsverarbeiter

Stand: 03.11.2026

Nr.	Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	beauftragt von	Drittland
1	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Server einschließlich Sicherungen	Rechenzentren in Deutschland (Nürnberg, Falkenstein); der Server steht in Nürnberg	DEKObyte	nein
2	Strato AG, Otto-Ostrowski-Straße 7, 10249 Berlin	Versand der E-Mails (SMTP-Relay) und Postfach technik@confirm.palettenkonto.net	Deutschland	DEKObyte	nein

Hinweise zur Liste:

1. Die Liste nennt für jeden Unterauftragsverarbeiter Firma und Anschrift, Leistung, Ort der Verarbeitung, wer ihn beauftragt hat, und bei Drittlandbezug die Grundlage der Übermittlung.
2. Nicht im Einsatz: ein Mailversand mit Sitz oder Verarbeitung außerhalb der EU (etwa Postmark) und eine Storage Box bei Hetzner für Sicherungen. Ein solcher Mailversand ist nicht gelistet; vor seinem Einsatz gilt § 8 Abs. 2. Eine Storage Box am Standort Falkenstein fällt unter Nr. 1 („Server einschließlich Sicherungen“, Deutschland) und braucht keine Ankündigung. Eine Storage Box in Helsinki ist erst nach einer Änderung dieser Liste nach § 8 Abs. 2 zulässig (Ort „Deutschland, Finnland“).

Anlage 4 · Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand: 03.11.2026

Geltungsbereich. Diese Anlage beschreibt den Dienst auf dem Server bei Hetzner, den Betrieb durch DEKObyte und die Teile beim Kunden, die der Dienst vorgibt (Connector).

Stand je Maßnahme. Die Maßnahmen in den Abschnitten A bis F und Maßnahme M42 sind ab dem ersten Kundenzugang in Betrieb; Abschnitt H beschreibt die Grenzen in diesem Stand. „Ab Folge-Update“ kennzeichnet Maßnahmen, die mit einem späteren Update des Dienstes kommen; die Frist steht dabei. Abschnitt H nennt die Grenzen der Maßnahmen.

A. Zugang zu den Systemen

Nr.	Maßnahme
M1	Server bei Hetzner in Deutschland (Nürnberg). Die Firewall von Hetzner lässt nur die Ports 22, 80, 443 und 8443 zu; ihre Wirkung ist von außen gemessen.
M2	Zugang zum Server per SSH haben nur Personen bei DEKObyte, und nur mit Schlüssel; die Anmeldung mit Passwort ist abgeschaltet.
M3	Die Datenbank hat keinen veröffentlichten Port und ist nur im internen Netz der Container erreichbar.
M4	Der Dienst läuft im Container nicht als root, sondern als eigener Benutzer; der Schlüssel des Serverzertifikats ist nur für diesen Benutzer lesbar.
M5	Geheimnisse (Signierschlüssel der Links, Zugangsdaten) stehen in einer Datei auf dem Server, die nur root lesen kann, nicht im Quelltext und nicht in der Compose-Datei; die Container erhalten sie beim Start als Umgebungsvariablen.
M6	Die Betriebssicht `/ops/status` öffnet nur ein Geheimnis. Die Sonde `/ops/bereit` hat ein eigenes, schwächeres Geheimnis; ihre Antwort trägt keine Kundendaten. Geheimnisse werden in konstanter Zeit verglichen.
M7	Der unauthentifizierte Gesundheitsendpunkt ist über nginx (Port 443) gesperrt. Auf Port 8443 beantwortet derselbe Dienst auch Pfade außerhalb von /v1/* ohne Client-Zertifikat, darunter /healthz und die Seiten für Tauschpartner (Grenze G8).
M50	KI-Werkzeuge erhalten bei Prüfungen auf dem Produktionsserver nur Angaben ohne Personenbezug: Zählungen, Versionen, Konfiguration ohne Geheimnisse und die Antwort von `/ops/bereit`. `/ops/status`, das Entscheidungsprotokoll, Tabellen mit Daten der Tauschpartner und Protokolle mit Adressen liest nur ein Mensch bei DEKObyte; solche Ausgaben werden auch nicht in ein KI-Werkzeug kopiert.

B. Zugriff auf Daten, Trennung der Mandanten

Nr.	Maßnahme
M8	Row-Level-Security in allen Mandantentabellen (ENABLE und FORCE). Sie bindet die Anwendungsrolle im Mandantenpfad. Für den Dienstprozess, der sich als Eigentümer und Superuser anmeldet, und für den Systempfad greift sie nicht (G1). Alles mit Kundendaten läuft unter der Anwendungsrolle mit gesetztem Mandanten; der Systempfad wird nur an einer abgeschlossenen, durch eine automatische Prüfung gezählten Liste von Stellen benutzt.
M9	Tabellen ohne Mandantenbezug (Konfiguration, Laufprotokoll, Ratenbremse) sind für die Anwendungsrolle gesperrt.
M10	Connector: Der Mandant ergibt sich nur aus dem Client-Zertifikat (mTLS), nie aus der Anfrage. Eine Identität aus einer Kopfzeile wird nicht angenommen. Widerrufene Zertifikate und gesperrte Mandanten werden abgewiesen.
M11	Tauschpartner: Zugang nur über einen persönlichen Link aus 144 Bit Zufall mit HMAC-SHA-256-Prüfwert. Gespeichert wird nur ein Hash. Ein Link gilt 14 Tage. Je Aufstellung und Tauschpartner zählt genau eine Entscheidung.
M12	Eine Ratenbremse verhindert massenhaftes Ausprobieren von Links; sie ist über beide Instanzen geteilt.
M13	Beim Kunden: Der Connector verbindet nur ausgehend; die Datenbank des Kunden wird nie von außen erreichbar. Die Datenbankrolle des Connectors hat nur die nötigsten Rechte und schreibt nur in den Staging-Bereich.
M14	Dateien des Connectors, auch die Warteschlange mit Partnerdaten, sind unter Windows nur für System, Administratoren und den Eigentümer lesbar; eine automatische Prüfung hält die Liste der Stellen fest.
M15	Der private Schlüssel der CA der Web-Bestätigung liegt nicht auf dem Server und nicht in der Datenbank. Client-Zertifikate stellt ein Mensch bei DEKObyte von Hand aus. Die Connector-Schnittstelle hat keinen Endpunkt ohne mTLS. Verwahrung des Schlüssels: Grenze G3.
M16	Ein Zertifikat wird erst ausgestellt, wenn DEKObyte den Antrag in Textform angenommen hat und die Pflichtangaben vollständig sind.
M17	Ohne die Pflichtangaben des Kunden verschickt der Dienst keinen Link zur Bestätigung per Mail (eigener Sperrgrund).
M18	Je nach Einstellung des Kunden gibt ein Mensch bei DEKObyte jede neue Empfängeradresse vor der ersten E-Mail frei; der Dienst zeigt dabei Hinweise auf auffällige Adressen. Das Kürzel des freigebenden Menschen kommt ins Protokoll.

C. Verschlüsselung und Übertragung

Nr.	Maßnahme
M19	Seiten für Menschen über nginx (Port 443) nur über HTTPS (TLS 1.2 und 1.3) mit HSTS und Schutzkopfzeilen (nosniff, keine Einbettung in fremde Seiten, keine Weitergabe der Adresse); HTTP leitet nur um. Auf Port 8443 fehlen die Kopfzeilen von nginx (G8).
M20	Der Connector spricht nur mit einem eigenen Listener mit mTLS gegen die eigene CA; ein fremdes Client-Zertifikat wird im Handshake abgewiesen (gemessen).
M21	E-Mails gehen über das Relay mit STARTTLS; für die Absenderdomain sind SPF, DKIM und DMARC eingerichtet.
M22	Sicherungen werden verschlüsselt geschrieben (gpg mit Integritätsschutz). Verwahrung der Passphrase: Grenze G4.

D. Datenminimierung im Betrieb

Nr.	Maßnahme
M23	Weder der Dienst noch nginx auf Port 443 schreiben Zugriffsprotokolle. Im Protokoll des Dienstes steht statt des Link-Tokens ein Platzhalter.
M24	nginx schreibt auch auf Port 80 kein Zugriffsprotokoll; Fehlerzeilen nur ab Stufe „crit“.
M25	Containerprotokolle sind nach Größe begrenzt (3 × 10 MB). Zusätzlich gilt eine zeitliche Grenze von höchstens 14 Tagen.
M26	Je Link hält der Dienst nur das erste Öffnen mit IP-Adresse und Browserkennung fest; weitere Aufrufe zählt er ohne IP-Adresse.
M27	Der Kunde erhält keine IP-Adresse und keine Browserkennung, sondern nur Entscheidung, Zahl, Kommentar, Adresse und Zeitpunkt.
M28	Die Seiten für Tauschpartner setzen keine Cookies, speichern nichts im Browser und laden nichts von fremden Servern. Links zur Website tragen nur feste Kampagnenwerte ohne Kennung.
M29	E-Mails an Tauschpartner enthalten keine Bilder und keine Werbung.

E. Integrität der Beweismittel

Nr.	Maßnahme
M30	Entscheidungsprotokoll und Belege sind für die Anwendungsrolle nur anhängbar. Entscheidungen und Aufstellungen kann sie nicht als Ganzes löschen; ihre einzelnen Zeilen sind dagegen nicht gesperrt.
M31	Die Anwendungsrolle kann keinen Mandanten löschen; sonst nähme die Kaskade Belege und Protokoll mit. Eine automatische Prüfung hält das fest.
M32	Ein Beleg wird einmal erzeugt und danach unverändert ausgeliefert, mit SHA-256-Prüfsumme; je Aufstellung und Tauschpartner gibt es genau einen.
M33	Der Beleg druckt die Erklärungstexte, die der Tauschpartner gesehen hat, aus dem Protokoll.
M34	Die IP-Adresse im Protokoll ist die echte Herkunft: nginx überschreibt die weitergereichte Kopfzeile, und der Dienst glaubt sie nur von der festen Adresse des Proxys.
M35	Neue Fassungen des Dienstes werden nur mit bestandenen automatischen Testsuiten freigegeben und von DEKObyte eingespielt. Ein technisches Tor vor dem Einspielen gibt es nicht. Die Schutzregeln in M6, M8, M15, M28 und M31 sind durch automatische Prüfungen festgehalten.

F. Verfügbarkeit, Belastbarkeit, Wiederherstellung

Nr.	Maßnahme
M36	Tägliche Sicherung der Datenbank um 02:15 UTC. Nach dem Schreiben wird geprüft, dass Belege, Entscheidungsprotokoll und die Konfigurationstabelle im Dump stehen. Der Signierschlüssel der Links liegt auf dem Produktionsserver nicht in der Datenbank, sondern nur in der Geheimnisdatei (M5), und ist nicht Teil dieser Sicherung. Sicherungen werden ab 29 vollen Tagen nach ihrem Alter gelöscht, auch wenn ein Sicherungslauf fehlschlägt; eine Sicherung liegt damit höchstens knapp 30 Tage. Ein fehlgeschlagener Lauf löst einen Alarm aus.
M37	Server-Backups von Hetzner sind nur eingeschaltet, wenn keine dieser Sicherungen länger als 30 Tage aufbewahrt wird.
M38	Werkzeuge für Rücksicherung und Rückspielprobe liegen vor. Probe auf dem Produktionsserver: Grenze G5.
M39	Container starten nach einem Ausfall selbst neu; Gesundheitsprüfungen für die Datenbank und beide Instanzen des Dienstes.

Nr.	Maßnahme
M40	Überwachung: täglicher Lauf mit Alarmbericht per Mail; `/ops/bereit` meldet auch das Ausbleiben des Laufs; ein Wächter auf dem Server fragt regelmäßig nach.
M41	Automatische Läufe laufen nur in einer Instanz; doppelten Versand verhindert die Datenbank.

G. Löschung, Export und Ende eines Mandanten

Nr.	Maßnahme	Stand
M42	„Mandant beenden“, Schritte 1–4: Deaktivieren, Sperre der Seite für Tauschpartner, Abholen trotz Deaktivierung, Widerruf erst danach; jeder Schritt protokolliert (§ 12). Die Seite für Tauschpartner lässt sich auch ohne Vertragsende sperren, etwa bevor der Kunde den Connector entfernt.	ab dem ersten Kundenzugang
M43	Eigene Löschrolle ohne Anmeldung, protokollierter Löschlauf, kurze Fristen; Löschlauf nach jeder Rücksicherung (Anlage 2, 2.4).	ab Folge-Update, spätestens 90 Tage nachdem der Dienst die ersten Kundendaten verarbeitet hat
M44	Schwärzen von IP-Adresse und Browserkennung bei Links ohne Antwort.	ab Folge-Update, spätestens 6 Monate und 14 Tage nach dem ersten Link zur Bestätigung per Mail
M45	Exporte: Abruf je Zeitraum, Auskunft je Tauschpartner, Export zum Vertragsende.	bis zum Folge-Update von Hand nach festgelegtem Ablauf; Befehle ab Folge-Update, spätestens zur ersten Anforderung
M46	Abrufgrenze von zwölf Monaten, Sperre in der Archivphase, Schritt 5 von „Mandant beenden“.	ab Folge-Update: Sperre in der Archivphase vor dem ersten Vertragsende, Zwölf-Monats-Grenze vor Ablauf von zwölf Monaten nach der ersten Antwort
M47	Lange Fristen im Löschlauf.	ab Folge-Update, vor dem 01.01.2030, 01.01.2031, 01.01.2033 bzw. 01.01.2035
M48	Eigene Anmelderolle des Webdienstes ohne Eigentum und ohne Superuser (behebt Grenze G1).	ab Folge-Update; bis dahin gilt G1
M49	Herstellerhinweis je Kunde abschaltbar; bis dahin nur für alle Kunden zugleich.	ab Folge-Update, bevor ein zweiter Kunde den Dienst nutzt

H. Grenzen der Maßnahmen

Nr.	Grenze
G1	Der Dienst meldet sich als Eigentümer und Superuser der Datenbank an und wechselt nur je Transaktion in die Anwendungsrolle. Die Rechtebeschränkungen (M8, M9, M30, M31) binden die App-Rolle im Mandantenpfad, nicht den Dienstprozess selbst; eingeschleustes SQL wäre nicht gebremst. Bis M48 gilt diese Beschreibung.
G2	Wer Shell-Zugang zum Server, die Eigentümerrolle der Datenbank oder eine entschlüsselte Sicherung hat, ist durch die Rechtebeschränkungen nicht gebunden. Die eigentliche Grenze um die Beweismittel ist der SSH-Zugang (M2).
G3	Der private CA-Schlüssel liegt passwortverschlüsselt auf einem Arbeitsgerät von DEKObyte, das am Netz hängt; die Passphrase verwahrt DEKObyte getrennt vom Schlüssel. Ein Gerät ohne Netz oder ein Hardware-Sicherheitsmodul ist nicht im Einsatz.
G4	Die eigenen Sicherungen liegen auf demselben Server, die Passphrase dafür ebenfalls; der Server kann seine Sicherungen also selbst entschlüsseln. Eine Auslagerung an einen zweiten Ort gibt es nicht.

Nr.	Grenze
G5	Eine Rückspielprobe auf dem Produktionsserver ist bis zum Stand dieser Anlage nicht gefahren.
G6	Die Datenträger des Servers sind nicht zusätzlich verschlüsselt.
G7	Die Freigabe von Adressen (M18) prüft Auffälligkeiten, nicht, ob eine Adresse zum Tauschpartner gehört.
G8	Port 8443 ist aus dem ganzen Internet erreichbar (M1). Dort läuft dieselbe Anwendung mit allen Routen, und der TLS-Handshake gelingt auch ohne Client-Zertifikat. Ohne Client-Zertifikat beantwortet der Dienst dort /healthz (mit Versionsangabe) und die Seiten für Tauschpartner, ohne die Schutzkopfzeilen von nginx (M19); das Client-Zertifikat verlangt nur /v1/*.