Auftragsverarbeitungsvertrag (AVV) – Ariba-Gateway

Fassung: 1.1 · **Stand:** November 2026 · **Auftragsverarbeiter:** ALTENBRAND Datentechnik GmbH

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 der Datenschutz-Grundverordnung (DSGVO) für das Ariba-Gateway des Ariba-Connectors von merchantCENTRAL.

---

§ 1 Vertragsparteien, Gegenstand und Geltungsbereich

(1) Dieser Vertrag wird geschlossen zwischen dem Lizenznehmer des Ariba-Connectors von merchantCENTRAL als **Verantwortlichem** (im Folgenden „Auftraggeber“) und der **ALTENBRAND Datentechnik GmbH** als **Auftragsverarbeiter** (im Folgenden „Auftragnehmer“). Die Angaben zu den Parteien enthält Anlage 1.

(2) Der Auftragnehmer betreibt das Ariba-Gateway (`ariba.merchantcentral.de`). Es nimmt die cXML-Belege, die SAP Business Network an den Auftraggeber sendet, entgegen, hält sie zum Abruf durch die Business Central-Umgebung des Auftraggebers bereit und sendet die Belege aus dieser Umgebung an SAP Business Network. Grundlage ist die Endbenutzer-Lizenzvereinbarung (EULA) von merchantCENTRAL (im Folgenden „Hauptvertrag“).

(3) Dieser Vertrag gilt für alle personenbezogenen Daten, die der Auftragnehmer beim Betrieb des Ariba-Gateways im Auftrag des Auftraggebers verarbeitet (im Folgenden „Auftraggeber-Daten“). Art, Zweck, Datenkategorien und betroffene Personen beschreibt Anlage 2.

(4) Nicht Gegenstand dieses Vertrags sind die Daten, die der Auftragnehmer als eigener Verantwortlicher verarbeitet: die Registrierung am Ariba-Gateway, der Onboarding-Code, der Nachweis der Annahme nach Abs. 5 Nr. 2 und die Betriebsprotokolle sowie die Daten der Lizenzierung. Dafür gilt die Datenschutzerklärung von merchantCENTRAL, Abschnitt 5 (für das Ariba-Gateway Abschnitt 5 o)).

(5) Der Vertrag kommt auf einem der folgenden Wege zustande:

1. **Registrierung mit Onboarding-Code**, insbesondere für das Produktivkonto: Der Auftraggeber nimmt den Vertrag in Textform an, etwa durch Bestätigung per E-Mail oder durch Unterzeichnung. Der Auftragnehmer stellt den Onboarding-Code für die Registrierung am Ariba-Gateway erst danach aus und stellt dem Auftraggeber den geschlossenen Vertrag als PDF-Datei bereit.
2. **Testregistrierung ohne Onboarding-Code:** Der Auftraggeber nimmt den Vertrag vor der Registrierung im Einrichtungsassistenten des Ariba-Connectors an. Der Assistent verlinkt den Vertrag in der angenommenen Fassung als PDF-Datei unter einer Adresse, die sich nicht ändert; der Auftraggeber kann sie speichern. Dabei gibt der Auftraggeber eine E-Mail-Adresse für Meldungen nach diesem Vertrag an (E-Mail für Datenschutzmeldungen). Als Nachweis speichert das Ariba-Gateway je Annahme Fassung und Zeitpunkt, den Firmennamen aus dem Business Central-Mandanten, Tenant-ID und Kennung (ANID) aus der Registrierung, den Benutzernamen des annehmenden Benutzers sowie die angegebene E-Mail für Datenschutzmeldungen; Fassung, Zeitpunkt und Benutzer stehen außerdem im Business Central-Mandanten des Auftraggebers. Diesen Nachweis bewahrt der Auftragnehmer als eigener Verantwortlicher bis vier Jahre nach dem Ende der Nutzung des Ariba-Gateways auf, also nach der Löschung der letzten Registrierung des Auftraggebers, auch über das Ende dieses Vertrags hinaus; § 10 Abs. 2 gilt für ihn nicht.

§ 2 Dauer

(1) Der Vertrag beginnt mit seinem Abschluss und läuft, solange der Auftragnehmer für den Auftraggeber Auftraggeber-Daten im Ariba-Gateway verarbeitet.

(2) Er endet ohne Kündigung, wenn der Hauptvertrag für den Ariba-Connector endet und alle Auftraggeber-Daten nach § 10 gelöscht sind. Besteht nur eine Testregistrierung ohne Onboarding-Code, endet er auch, sobald diese nach ihrem Ablauf gelöscht ist. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

§ 3 Weisungen

(1) Der Auftragnehmer verarbeitet Auftraggeber-Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen ergeben sich aus diesem Vertrag, dem Hauptvertrag und den Einstellungen, die der Auftraggeber im Ariba-Connector und in seinem Lieferantenkonto bei SAP Business Network vornimmt. Einzelweisungen erteilt der Auftraggeber in Textform. Gehen sie über den vereinbarten Leistungsumfang hinaus, gelten sie als Änderungswunsch; der Auftragnehmer kann den Mehraufwand nach Aufwand berechnen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert er den Auftraggeber unverzüglich. Er darf die Ausführung der Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

(4) Eine Übermittlung von Auftraggeber-Daten in ein Drittland außerhalb der EU und des EWR findet nur nach § 12 statt.

§ 4 Zweckbindung

Der Auftragnehmer verarbeitet Auftraggeber-Daten ausschließlich für die in Anlage 2 genannten Zwecke. Er nutzt sie nicht für eigene Zwecke, gibt sie nicht an Dritte weiter, außer an SAP Business Network und die Business Central-Umgebung des Auftraggebers wie in § 1 Abs. 2 beschrieben, und wertet sie nicht aus.

§ 5 Vertraulichkeit

Der Auftragnehmer gewährt nur den Personen Zugang zu Auftraggeber-Daten, die ihn für den Betrieb, die Wartung oder die Fehlerbehebung des Ariba-Gateways benötigen. Er hat sie zur Vertraulichkeit verpflichtet, soweit sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 6 Sicherheit der Verarbeitung

(1) Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 3 beschrieben sind.

(2) Er darf die Maßnahmen dem technischen Fortschritt anpassen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber auf Anfrage mit.

§ 7 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter nennt Anlage 4; sie gelten als genehmigt.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens **30 Tage** vorher in Textform über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann der Änderung innerhalb dieser Frist widersprechen. Finden die Parteien keine Lösung, kann der Auftraggeber die Lizenz für den Ariba-Connector und die Nutzung des Ariba-Gateways zum Zeitpunkt des Wechsels kündigen. Muss ein Unterauftragsverarbeiter aus dringenden Gründen der Sicherheit oder Verfügbarkeit ohne Vorlauf ersetzt werden, informiert der Auftragnehmer unverzüglich; das Widerspruchsrecht gilt dann ab dieser Information.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf die Datenschutzpflichten nach Art. 28 Abs. 3 DSGVO, insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Bei Anbietern standardisierter Cloud-Dienste genügt deren Datenschutzvereinbarung, sofern sie diese Anforderungen erfüllt. Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer dem Auftraggeber dafür nach Art. 28 Abs. 4 DSGVO im Rahmen von § 13.

(4) Keine Unterauftragsverarbeitung im Sinne dieses Vertrags ist die Übermittlung an SAP Business Network. Der Auftraggeber nutzt SAP Business Network aufgrund seines eigenen Vertrags mit SAP; der Auftragnehmer leitet die Belege nur dorthin weiter.

§ 8 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Art. 12 bis 22 DSGVO zu beantworten. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm vorliegenden Informationen bei den Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(3) Unterstützungsleistungen, die über die Pflichten aus diesem Vertrag hinausgehen oder auf ein Verschulden des Auftraggebers zurückgehen, kann der Auftragnehmer nach Aufwand berechnen.

§ 9 Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes von Auftraggeber-Daten unverzüglich, nachdem sie ihm bekannt geworden ist, in Textform an die in Anlage 1 genannte Adresse. Bei Annahme im Einrichtungsassistenten meldet er an die jeweils aktuelle E-Mail für Datenschutzmeldungen (§ 14 Abs. 3), solange kein Vertrag in Textform nach § 1 Abs. 5 Nr. 1 geschlossen ist; danach gilt Anlage 1.

(2) Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung mit Kategorien und ungefährer Zahl der betroffenen Personen und Datensätze, Kontakt für weitere Informationen, wahrscheinliche Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen. Was zunächst nicht bekannt ist, reicht der Auftragnehmer nach, sobald es vorliegt.

(3) Der Auftragnehmer ergreift unverzüglich die Maßnahmen, die zur Eindämmung der Verletzung und zur Minderung möglicher nachteiliger Folgen erforderlich sind.

§ 10 Löschung und Rückgabe

(1) Während der Laufzeit löscht der Auftragnehmer Auftraggeber-Daten nach den Fristen in Anlage 2. Belege, die die Business Central-Umgebung des Auftraggebers abgerufen hat, liegen dem Auftraggeber dort bereits vor; eine gesonderte Rückgabe ist daher nicht erforderlich.

(2) Endet der Hauptvertrag für den Ariba-Connector, sperrt der Auftragnehmer die Registrierung des Auftraggebers unverzüglich, sodass das Ariba-Gateway keine weiteren Belege für ihn annimmt. Innerhalb von **30 Tagen** nach Ende des Hauptvertrags löscht er alle noch vorhandenen Auftraggeber-Daten, einschließlich nicht abgerufener Belege und der zugehörigen Eingangsvermerke. Auf Wunsch, den der Auftraggeber bis zur Löschung äußert, stellt er nicht abgerufene Belege vorher in einem gängigen Format bereit. Innerhalb derselben Frist löscht er auch die Registrierung, den Onboarding-Code und das Shared Secret, die er nach § 1 Abs. 4 als eigener Verantwortlicher verarbeitet. Azure Key Vault hält gelöschte Secrets technisch noch 90 Tage im Zustand „gelöscht" vor; sie sind dann nicht mehr abrufbar, ein vorzeitiges endgültiges Löschen ist technisch ausgeschlossen.

(3) Der Auftragnehmer bestätigt die Löschung auf Anfrage in Textform. Eine Pflicht zur Speicherung nach dem Recht der Union oder eines Mitgliedstaats bleibt unberührt.

§ 11 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO und diesem Vertrag erforderlich sind.

(2) Der Nachweis wird vorrangig durch Unterlagen geführt, etwa durch Auskünfte, Dokumentation der Maßnahmen nach Anlage 3, aktuelle Zertifikate oder Prüfberichte; für die Rechenzentren von Microsoft Azure gelten die von Microsoft veröffentlichten Zertifizierungen und Prüfberichte.

(3) Reichen die Unterlagen nicht aus, kann der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer, der kein Wettbewerber des Auftragnehmers ist, Überprüfungen einschließlich Inspektionen durchführen. Sie finden höchstens einmal im Kalenderjahr statt, sind mit einer Frist von mindestens 30 Tagen anzumelden, finden während der üblichen Geschäftszeiten statt und dürfen den Betrieb nicht unverhältnismäßig stören. Aus konkretem Anlass, insbesondere nach einer Verletzung nach § 9, sind weitere Überprüfungen mit einer Frist von 5 Werktagen zulässig.

(4) Jede Partei trägt ihre eigenen Kosten einer Überprüfung. Für Inspektionen vor Ort kann der Auftragnehmer einen angemessenen Ersatz seines Aufwands verlangen, nicht jedoch, wenn die Überprüfung einen wesentlichen Verstoß des Auftragnehmers ergibt; dann trägt er die angemessenen Kosten der Überprüfung.

§ 12 Ort der Verarbeitung

(1) Der Auftragnehmer verarbeitet Auftraggeber-Daten ausschließlich in der Europäischen Union, derzeit in Rechenzentren von Microsoft Azure in der Region Germany West Central (Frankfurt am Main, Deutschland).

(2) Greift ein Unterauftragsverarbeiter im Einzelfall, etwa im Rahmen des technischen Supports, aus einem Drittland auf Auftraggeber-Daten zu, ist dies nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere durch einen Angemessenheitsbeschluss der EU-Kommission oder durch Standardvertragsklauseln.

§ 13 Haftung

Für die Haftung der Parteien gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien zueinander gelten die Haftungsregelungen des Hauptvertrags, soweit dieser Vertrag nichts anderes bestimmt.

§ 14 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage und die Information der betroffenen Personen.

(2) Er informiert den Auftragnehmer unverzüglich, wenn er bei der Prüfung der Ergebnisse oder des Betriebs Fehler oder Unregelmäßigkeiten in Bezug auf den Datenschutz feststellt.

(3) Er teilt dem Auftragnehmer Änderungen der Angaben in Anlage 1, insbesondere der Adresse für Meldungen, in Textform mit. Bei Annahme im Einrichtungsassistenten hält er die E-Mail für Datenschutzmeldungen auf der Ariba-Marktplatzkarte in Business Central aktuell, solange kein Vertrag in Textform nach § 1 Abs. 5 Nr. 1 geschlossen ist; eine Änderung dort überträgt der Ariba-Connector an das Ariba-Gateway.

§ 15 Schlussbestimmungen

(1) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag geht dieser Vertrag in allen Fragen des Datenschutzes vor.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Änderungen der Anlagen 3 und 4 nach § 6 Abs. 2 und § 7 Abs. 2 bleiben davon unberührt.

(3) Ist eine Bestimmung dieses Vertrags unwirksam, bleiben die übrigen Bestimmungen wirksam. An die Stelle der unwirksamen Bestimmung tritt eine Regelung, die den Anforderungen des Art. 28 DSGVO entspricht und dem Gewollten am nächsten kommt.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Der Gerichtsstand richtet sich nach dem Hauptvertrag.

Anlage 1 – Parteien und Ansprechpartner

Auftragnehmer

ALTENBRAND Datentechnik GmbH, vertreten durch den Geschäftsführer Frank Altenbrand
Am Gelicht 5, 35279 Neustadt, Deutschland
Handelsregister: Amtsgericht Marburg, HRB 3649
Kontakt für den Datenschutz und für Meldungen nach § 9: info@altenbrand.de, Telefon +49 6692 202290

Auftraggeber (bei Vertragsschluss auszufüllen; bei Annahme im Einrichtungsassistenten ergeben sich Firma, Tenant-ID und Kennung (ANID) aus der Registrierung und dem Business Central-Mandanten, siehe § 1 Abs. 5)

Angabe	
Firma und Anschrift	
Vertreten durch	
Microsoft Entra Tenant-ID der Business Central-Umgebung	
Kennung (ANID) des Produktivkontos bei SAP Business Network	
Kennung (ANID) des Testkontos bei SAP Business Network, falls genutzt	
Ansprechpartner für den Datenschutz (Name, E-Mail)	
Adresse für Meldungen nach § 7 und § 9 (bei Annahme im Einrichtungsassistenten: die dort angegebene oder zuletzt nach § 14 Abs. 3 geänderte E-Mail für Datenschutzmeldungen)	

Anlage 2 – Beschreibung der Verarbeitung

Kategorien betroffener Personen

- Mitarbeitende der Einkäufer (Kunden) des Auftraggebers, etwa Besteller, Ansprechpartner und Rechnungsempfänger
- Empfänger von Lieferungen an den in Bestellungen genannten Lieferanschriften
- Mitarbeitende des Auftraggebers, soweit sie in Belegen genannt sind (etwa als Ansprechpartner)

Kategorien personenbezogener Daten

- Namen, Firmen, Abteilungen, Liefer- und Rechnungsanschriften
- E-Mail-Adressen und Telefonnummern
- Inhalte von Kommentaren und Zusatzfeldern der Belege, soweit sie personenbezogene Angaben enthalten
- Bestell-, Liefer- und Rechnungsdaten mit Bezug zu diesen Personen (Artikel, Mengen, Preise, Termine, Sendungsnummern)
- Status, Kommentare und Zahlungsangaben aus Statusmeldungen der Einkäufer zu Rechnungen und Gutschriften
- die E-Mail-Adresse, die der Auftraggeber für Statusmeldungen zu Katalogen angibt

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht vorgesehen.

Art und Zweck der Verarbeitung

Vorgang	Art der Verarbeitung
Eingehende Bestellungen und Statusmeldungen von SAP Business Network	Empfang, Prüfung der Absenderkennung, Speicherung bis zum Abruf, Übermittlung an die Business Central-Umgebung des Auftraggebers, Löschung
Ausgehende Auftragsbestätigungen, Lieferavise, Rechnungen, Gutschriften (gegebenenfalls mit E-Rechnungsdatei) und Kataloge	Entgegennahme aus der Business Central-Umgebung, Umwandlung in cXML, Weiterleitung an SAP Business Network, Rückmeldung des Ergebnisses; keine Speicherung der Inhalte

Zweck ist der elektronische Austausch von Geschäftsbelegen zwischen dem Auftraggeber und seinen Einkäufern über SAP Business Network.

Speicherfristen

Daten	Frist
Inhalte eingehender Bestellungen und Statusmeldungen	7 Tage nach dem Abruf durch die Business Central-Umgebung; nicht abgerufene spätestens nach 180 Tagen
Inhalte ausgehender Belege	keine Speicherung
Eingangsvermerk ohne personenbezogene Daten (Kennung, Zeitpunkte, Belegnummer)	90 Tage nach Eingang; bei nie abgerufenen Belegen 180 Tage nach Eingang, spätestens mit der Löschung der Registrierung

Anlage 3 – Technische und organisatorische Maßnahmen

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

- **Zutrittskontrolle:** Das Ariba-Gateway läuft ausschließlich in Rechenzentren von Microsoft Azure; der physische Schutz richtet sich nach den Maßnahmen und Zertifizierungen von Microsoft (unter anderem ISO/IEC 27001). Der Auftragnehmer betreibt keine eigenen Server für das Gateway.

- **Zugangskontrolle:** Verwaltungszugriff auf die Azure-Ressourcen nur für namentlich benannte Administratoren des Auftragnehmers mit persönlichem Konto und Mehr-Faktor-Authentifizierung; Onboarding-Codes stellt nur dieser Personenkreis über einen geschützten Verwaltungszugang aus. *[Vom Auftragnehmer zu bestätigen, einschließlich des Umgangs mit dem Hauptschlüssel der Function App.]* Der Lizenz-Manager des Auftragnehmers sperrt, entsperrt und löscht Registrierungen über einen eigenen, nur dafür freigeschalteten Schlüssel; Belegdaten kann er nicht abrufen.
- **Zugriffskontrolle der Anwendung:**
- Die Anwendung greift über eine verwaltete Identität (Managed Identity) mit rollenbasierten Rechten auf Speicher und Key Vault zu; Kontoschlüssel des Speichers sind abgeschaltet.
- Shared Secrets liegen in Azure Key Vault mit rollenbasierter Zugriffssteuerung.
- Dienstschlüssel und Onboarding-Codes werden nur als SHA-256-Hashwert gespeichert; Dienstschlüssel und Shared Secrets werden in konstanter Zeit verglichen. Ein Onboarding-Code gilt 14 Tage und nur einmal.
- Jedes eingehende Dokument wird gegen das Shared Secret geprüft, Bestellungen zusätzlich gegen die Kennung des Lieferantenkontos; jeder Aufruf aus Business Central braucht den Dienstschlüssel der jeweiligen Registrierung.
- **Trennungskontrolle:** Belege sind der Registrierung eines Auftraggebers zugeordnet und nur mit deren Dienstschlüssel abrufbar. Test- und Produktivkonto sind getrennte Registrierungen.
- **Datenminimierung:** Gespeichertes cXML wird ohne Shared Secret und Signaturen abgelegt. Betriebsprotokolle enthalten Belegnummern und technische Kennungen, aber keine Belegdaten wie Anschriften oder Namen und keine Secrets.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle:** Alle Verbindungen sind mit TLS 1.2 oder höher verschlüsselt; HTTP-Anfragen werden nicht verarbeitet, sondern auf HTTPS umgeleitet, FTP ist abgeschaltet. Das Shared Secret sendet das Gateway nur über HTTPS an Adressen von SAP Ariba (`ariba.com`, `sapariba.com`).
- **Eingabekontrolle:** Jeder Aufruf der Anwendung wird mit Zeitpunkt, Vorgang und Ergebnis protokolliert. Lese-, Schreib- und Löschzugriffe auf den Speicher werden mit Aufrufer, IP-Adresse und Objektname protokolliert, Zugriffe auf Key Vault ebenso. Alle Protokolle werden 12 Monate aufbewahrt.
- **Verschlüsselung ruhender Daten:** Speicher und Key Vault von Microsoft Azure verschlüsseln gespeicherte Daten.

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

- Speicher mit lokal redundanter Ablage (drei Kopien innerhalb des Rechenzentrums).
- Key Vault mit vorläufigem Löschen und Löschschutz (90 Tage).
- Nicht abgerufene Bestellungen und Statusmeldungen meldet das Gateway nach 24 Stunden täglich als Warnung und löst einen Alarm an den Betrieb aus; sie bleiben bis zum Abruf erhalten, längstens 180 Tage.

Löschung

- Tägliche automatische Löschung nach den Fristen in Anlage 2; zusätzlich löscht eine Regel des Speichers Belege spätestens nach 180 Tagen.
- Bei Vertragsende wird die Registrierung gesperrt und spätestens 28 Tage nach der Sperre mit allen Belegen, Eingangsvermerken, Onboarding-Codes und dem Shared Secret automatisch gelöscht. Ein

Alarm meldet eine gescheiterte Löschung.

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

- Änderungen am Gateway durchlaufen eine Code-Prüfung und automatisierte Tests; bereitgestellt wird nur der geprüfte Hauptzweig. *[Vom Auftragnehmer zu bestätigen.]*
- Die Zugriffsberechtigungen auf die Azure-Ressourcen werden regelmäßig überprüft. *[Vom Auftragnehmer zu bestätigen: Turnus.]*
- Ein Verfahren zur Behandlung von Sicherheitsvorfällen legt fest, wer Vorfälle bewertet und Meldungen nach § 9 auslöst. *[Vom Auftragnehmer zu bestätigen.]*

Anlage 4 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Rechenzentrumsbetrieb und Cloud-Dienste (Microsoft Azure: Azure Functions, Azure Storage, Azure Key Vault, Azure Application Insights)	Region Germany West Central (Frankfurt am Main, Deutschland)

Grundlage ist das Microsoft Products and Services Data Protection Addendum, das Bestandteil des Azure-Vertrags des Auftragnehmers ist. Microsoft setzt seinerseits Unterauftragsverarbeiter nach der von Microsoft veröffentlichten Liste ein.

Nicht als Unterauftragsverarbeiter eingesetzt wird Cloudflare: Cloudflare dient für die Adresse des Gateways nur der Namensauflösung (DNS) und verarbeitet keine Auftraggeber-Daten.

© 2026 ALTENBRAND Datentechnik GmbH. Alle Rechte vorbehalten.

Diese PDF-Datei gibt den Auftragsverarbeitungsvertrag in der Fassung 1.1 wieder. Abrufbar unter https://www.merchantcentral.de/assets/downloads/avv-ariba-1.1-de.pdf. Maßgeblich ist die deutsche Fassung.