Data Processing Agreement (DPA) – Ariba Gateway

Version: 1.0 · **Last updated:** November 2026 · **Processor:** ALTENBRAND Datentechnik GmbH

Agreement on the processing of personal data on behalf of a controller pursuant to Art. 28 of the General Data Protection Regulation (GDPR) for the Ariba gateway of the merchantCENTRAL Ariba connector.

This English version is provided for convenience. In case of discrepancies, the German version prevails.

---

§ 1 Parties, Subject Matter and Scope

(1) This agreement is concluded between the licensee of the merchantCENTRAL Ariba connector as **controller** (hereinafter "Controller") and **ALTENBRAND Datentechnik GmbH** as **processor** (hereinafter "Processor"). Annex 1 contains the details of the parties.

(2) The Processor operates the Ariba gateway (`ariba.merchantcentral.de`). It receives the cXML documents that SAP Business Network sends to the Controller, holds them for retrieval by the Controller's Business Central environment, and sends the documents from that environment to SAP Business Network. The basis is the merchantCENTRAL End User License Agreement (EULA) (hereinafter "Main Agreement").

(3) This agreement applies to all personal data that the Processor processes on behalf of the Controller when operating the Ariba gateway (hereinafter "Controller Data"). Annex 2 describes the nature, purpose, data categories and data subjects.

(4) This agreement does not cover the data the Processor processes as a controller in its own right: the registration at the Ariba gateway, the onboarding code, the proof of acceptance under paragraph 5 no. 2 and the operational logs, as well as licensing data. The merchantCENTRAL privacy policy, section 5 (for the Ariba gateway, section 5 o)), applies to these.

(5) The agreement is concluded in one of the following ways:

1. **Registration with an onboarding code**, in particular for the production account: the Controller accepts the agreement in text form, for example by confirmation by email or by signature. Only then does the Processor issue the onboarding code for registration at the Ariba gateway, and it provides the Controller with the concluded agreement as a PDF file.
2. **Test registration without an onboarding code:** the Controller accepts the agreement in the setup wizard of the Ariba connector before registering. The wizard links the agreement in the accepted version as a PDF file at an address that does not change; the Controller can save it. As proof, the Ariba gateway stores for each acceptance the version and time, the company name from the Business Central company, the tenant ID and identifier (ANID) from the registration and the user name of the accepting user; version, time and user are also kept in the Controller's Business Central company. The Processor keeps this proof as a controller in its own right until four years after the end of use of the Ariba gateway, i.e. after the deletion of the Controller's last registration, also beyond the end of this agreement; § 10(2) does not apply to it.

§ 2 Term

(1) The agreement begins when it is concluded and runs as long as the Processor processes Controller Data in the Ariba gateway for the Controller.

(2) It ends without notice when the Main Agreement for the Ariba connector ends and all Controller Data has been deleted in accordance with § 10. If only a test registration without an onboarding code exists, it

also ends as soon as that registration has been deleted after its expiry. The right to terminate for good cause remains unaffected.

§ 3 Instructions

(1) The Processor processes Controller Data only on documented instructions from the Controller, unless it is required to do so by Union or Member State law. In that case, it informs the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(2) The instructions result from this agreement, the Main Agreement and the settings the Controller makes in the Ariba connector and in its supplier account on SAP Business Network. The Controller issues individual instructions in text form. If they go beyond the agreed scope of services, they are deemed a change request; the Processor may charge for the additional effort.

(3) If the Processor considers that an instruction infringes the GDPR or other data protection provisions, it informs the Controller without delay. It may suspend the execution of the instruction until the Controller confirms or changes it.

(4) Controller Data is transferred to a third country outside the EU and the EEA only in accordance with § 12.

§ 4 Purpose Limitation

The Processor processes Controller Data exclusively for the purposes stated in Annex 2. It does not use it for its own purposes, does not disclose it to third parties other than SAP Business Network and the Controller's Business Central environment as described in § 1(2), and does not analyse it.

§ 5 Confidentiality

The Processor grants access to Controller Data only to persons who need it to operate, maintain or troubleshoot the Ariba gateway. It has committed them to confidentiality, unless they are under an appropriate statutory obligation of confidentiality.

§ 6 Security of Processing

(1) The Processor implements the technical and organisational measures pursuant to Art. 32 GDPR described in Annex 3.

(2) It may adapt the measures to technical progress provided that the level of protection is not reduced. It documents material changes and informs the Controller of them on request.

§ 7 Sub-processors

(1) The Controller grants general authorisation to engage sub-processors. The sub-processors engaged when the agreement is concluded are listed in Annex 4 and are deemed approved.

(2) The Processor informs the Controller in text form at least **30 days** in advance of any intended addition or replacement of a sub-processor. The Controller may object to the change within this period. If the parties do not find a solution, the Controller may terminate the license for the Ariba connector and the use of the Ariba gateway with effect from the date of the change. If a sub-processor has to be replaced without notice for urgent reasons of security or availability, the Processor informs the Controller without delay; the right to object then applies from this information.

(3) The Processor contractually imposes on each sub-processor the data protection obligations under Art. 28(3) GDPR, in particular sufficient guarantees for appropriate technical and organisational measures. For

providers of standardised cloud services, their data protection agreement suffices provided that it meets these requirements. If a sub-processor fails to fulfil its obligations, the Processor is liable to the Controller pursuant to Art. 28(4) GDPR within the scope of § 13.

(4) The transfer to SAP Business Network is not sub-processing within the meaning of this agreement. The Controller uses SAP Business Network under its own contract with SAP; the Processor merely forwards the documents there.

§ 8 Assistance to the Controller

(1) The Processor assists the Controller with appropriate technical and organisational measures in responding to requests from data subjects under Art. 12 to 22 GDPR. If a data subject contacts the Processor directly, the Processor forwards the request to the Controller without delay and does not answer it itself.

(2) Taking into account the nature of processing and the information available to it, the Processor assists the Controller with its obligations under Art. 32 to 36 GDPR (security, notification of breaches, data protection impact assessment, prior consultation).

(3) The Processor may charge for assistance that goes beyond the obligations under this agreement or results from the Controller's fault, based on the effort involved.

§ 9 Personal Data Breaches

(1) The Processor notifies the Controller of a personal data breach affecting Controller Data without undue delay after becoming aware of it, in text form to the address stated in Annex 1.

(2) As far as known, the notification contains the information pursuant to Art. 33(3) GDPR: the nature of the breach including the categories and approximate number of data subjects and records concerned, a contact point for more information, the likely consequences, and the measures taken or proposed. Information not initially available is provided as soon as it is.

(3) The Processor takes without delay the measures necessary to contain the breach and mitigate its possible adverse effects.

§ 10 Deletion and Return

(1) During the term, the Processor deletes Controller Data in accordance with the periods in Annex 2. Documents retrieved by the Controller's Business Central environment are already available to the Controller there; a separate return is therefore not required.

(2) When the Main Agreement for the Ariba connector ends, the Processor suspends the Controller's registration without delay so that the Ariba gateway accepts no further documents for it. Within **30 days** after the end of the Main Agreement, it deletes all remaining Controller Data, including documents not retrieved and the related receipt records. On request, made by the Controller before the deletion, it first provides documents not retrieved in a common format. Within the same period, it also deletes the registration, the onboarding code and the shared secret, which it processes as a controller in its own right under § 1(4). Azure Key Vault technically keeps deleted secrets for another 90 days in a "deleted" state; they can no longer be retrieved, and early permanent deletion is technically excluded.

(3) The Processor confirms the deletion in text form on request. Any obligation to store data under Union or Member State law remains unaffected.

§ 11 Evidence and Audits

(1) The Processor makes available to the Controller on request all information necessary to demonstrate compliance with the obligations under Art. 28 GDPR and this agreement.

(2) Evidence is primarily provided by documents, such as information, documentation of the measures in Annex 3, current certificates or audit reports; for the Microsoft Azure data centers, the certifications and audit reports published by Microsoft apply.

(3) If the documents are not sufficient, the Controller, or an auditor mandated by it who is bound to confidentiality and is not a competitor of the Processor, may conduct audits, including inspections. They take place at most once per calendar year, must be announced at least 30 days in advance, take place during normal business hours and must not disrupt operations disproportionately. For a specific reason, in particular after a breach under § 9, further audits are permitted with 5 working days' notice.

(4) Each party bears its own costs of an audit. For on-site inspections, the Processor may claim reasonable compensation for its effort, except where the audit reveals a material breach by the Processor; in that case the Processor bears the reasonable costs of the audit.

§ 12 Location of Processing

(1) The Processor processes Controller Data exclusively in the European Union, currently in Microsoft Azure data centers in the Germany West Central region (Frankfurt am Main, Germany).

(2) If a sub-processor accesses Controller Data from a third country in individual cases, for example as part of technical support, this is only permitted if the requirements of Art. 44 et seq. GDPR are met, in particular by an adequacy decision of the EU Commission or by standard contractual clauses.

§ 13 Liability

Art. 82 GDPR applies to the liability of the parties towards data subjects. Between the parties, the liability provisions of the Main Agreement apply unless this agreement provides otherwise.

§ 14 Obligations of the Controller

(1) The Controller is responsible for the lawfulness of the processing, in particular for the legal basis and for informing the data subjects.

(2) It informs the Processor without delay if it discovers errors or irregularities relating to data protection when checking the results or the operation.

(3) It notifies the Processor in text form of changes to the details in Annex 1, in particular the address for notifications.

§ 15 Final Provisions

(1) In the event of conflicts between this agreement and the Main Agreement, this agreement takes precedence in all matters of data protection.

(2) Amendments and additions to this agreement require text form. Changes to Annexes 3 and 4 in accordance with § 6(2) and § 7(2) remain unaffected.

(3) If any provision of this agreement is invalid, the remaining provisions remain valid. The invalid provision is replaced by a provision that meets the requirements of Art. 28 GDPR and comes closest to what was intended.

(4) The law of the Federal Republic of Germany applies. The place of jurisdiction is determined by the Main Agreement.

Annex 1 – Parties and Contacts

Processor

ALTENBRAND Datentechnik GmbH, represented by its managing director Frank Altenbrand
Am Gelicht 5, 35279 Neustadt, Germany
Commercial register: Amtsgericht Marburg, HRB 3649
Contact for data protection and for notifications under § 9: info@altenbrand.de, phone +49 6692 202290

Controller (to be completed when the agreement is concluded; on acceptance in the setup wizard, company, tenant ID and identifier (ANID) result from the registration and the Business Central company, see § 1(5))

Detail	
Company name and address	
Represented by	
Microsoft Entra tenant ID of the Business Central environment	
ID (ANID) of the production account on SAP Business Network	
ID (ANID) of the test account on SAP Business Network, if used	
Data protection contact (name, email)	
Address for notifications under § 7 and § 9	

Annex 2 – Description of Processing

Categories of data subjects

- Staff of the Controller's buyers (customers), such as requesters, contact persons and invoice recipients
- Recipients of deliveries at the shipping addresses stated in purchase orders
- Staff of the Controller, insofar as they are named in documents (for example as contact persons)

Categories of personal data

- Names, companies, departments, shipping and billing addresses
- Email addresses and phone numbers
- Content of comments and additional fields of the documents, insofar as it contains personal data
- Order, delivery and invoice data relating to these persons (items, quantities, prices, dates, tracking numbers)
- Status, comments and payment details from buyers' status updates on invoices and credit memos
- The email address the Controller provides for status notifications on catalogs

Special categories of personal data pursuant to Art. 9 GDPR are not intended.

Nature and purpose of processing

Operation	Nature of processing
Incoming purchase orders and status updates from SAP Business Network	Receipt, check of the sender credentials, storage until retrieval, transfer to the Controller's Business Central environment, deletion
Outgoing order confirmations, ship notices, invoices, credit memos (where applicable with an e-invoice file) and catalogs	Receipt from the Business Central environment, conversion to cXML, forwarding to SAP Business Network, return of the result; content is not stored

The purpose is the electronic exchange of business documents between the Controller and its buyers via SAP Business Network.

Storage periods

Data	Period
Content of incoming purchase orders and status updates	7 days after retrieval by the Business Central environment; if not retrieved, 180 days at the latest
Content of outgoing documents	not stored
Receipt record without personal data (identifier, times, document number)	90 days after receipt; for documents never retrieved, 180 days after receipt, at the latest when the registration is deleted

Annex 3 – Technical and Organisational Measures

Confidentiality (Art. 32(1)(b) GDPR)

- **Physical access control:** The Ariba gateway runs exclusively in Microsoft Azure data centers; physical protection follows Microsoft's measures and certifications (including ISO/IEC 27001). The Processor operates no servers of its own for the gateway.
- **System access control:** Administrative access to the Azure resources only for named administrators of the Processor with a personal account and multi-factor authentication; only this group of people issues onboarding codes, via a protected administrative access. *[To be confirmed by the Processor, including the handling of the Function App's master key.]* The Processor's license manager suspends, resumes and deletes registrations using a separate key enabled only for this purpose; it cannot retrieve document data.
- **Application access control:**
- The application accesses storage and Key Vault through a managed identity with role-based permissions; storage account keys are disabled.
- Shared secrets are stored in Azure Key Vault with role-based access control.
- Service keys and onboarding codes are stored only as SHA-256 hash values; service keys and shared secrets are compared in constant time. An onboarding code is valid for 14 days and only once.
- Every incoming document is checked against the shared secret, purchase orders additionally against the ID of the supplier account; every call from Business Central requires the service key of the respective registration.
- **Separation control:** Documents are assigned to the registration of a Controller and can only be retrieved with its service key. Test and production accounts are separate registrations.
- **Data minimisation:** Stored cXML is kept without the shared secret and signatures. Operational logs contain document numbers and technical identifiers, but no document data such as addresses or names, and no secrets.

Integrity (Art. 32(1)(b) GDPR)

- **Transfer control:** All connections are encrypted with TLS 1.2 or higher; HTTP requests are not processed but redirected to HTTPS, and FTP is disabled. The gateway sends the shared secret only via HTTPS to SAP Ariba addresses (`ariba.com`, `sapariba.com`).
- **Input control:** Every call to the application is logged with time, operation and outcome. Read, write and delete access to storage is logged with caller, IP address and object name, and so is access to Key Vault. All logs are kept for 12 months.
- **Encryption at rest:** Microsoft Azure storage and Key Vault encrypt stored data.

Availability and resilience (Art. 32(1)(b) and (c) GDPR)

- Storage with locally redundant replication (three copies within the data center).
- Key Vault with soft delete and purge protection (90 days).
- The gateway reports purchase orders and status updates not retrieved after 24 hours as a warning every day and triggers an alert to operations; they are kept until retrieval, for 180 days at most.

Deletion

- Daily automatic deletion in accordance with the periods in Annex 2; in addition, a storage rule deletes documents after 180 days at the latest.
- When the agreement ends, the registration is suspended and automatically deleted, with all documents, receipt records, onboarding codes and the shared secret, no later than 28 days after the suspension. An alert reports a failed deletion.

Process for regular testing (Art. 32(1)(d) GDPR)

- Changes to the gateway undergo code review and automated tests; only the reviewed main branch is deployed. *[To be confirmed by the Processor.]*
- Access permissions to the Azure resources are reviewed regularly. *[To be confirmed by the Processor: interval.]*
- An incident handling process defines who assesses incidents and triggers notifications under § 9. *[To be confirmed by the Processor.]*

Annex 4 – Sub-processors

Sub-processor	Service	Location of processing
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Data center operation and cloud services (Microsoft Azure: Azure Functions, Azure Storage, Azure Key Vault, Azure Application Insights)	Germany West Central region (Frankfurt am Main, Germany)

The basis is the Microsoft Products and Services Data Protection Addendum, which forms part of the Processor's Azure agreement. Microsoft in turn engages sub-processors according to the list published by Microsoft.

Cloudflare is not engaged as a sub-processor: for the gateway's address, Cloudflare is used for name resolution (DNS) only and does not process Controller Data.

© 2026 ALTENBRAND Datentechnik GmbH. All rights reserved.

This PDF file reproduces version 1.0 of the data processing agreement. Available at https://www.merchantcentral.de/assets/downloads/avv-ariba-1.0-en.pdf. This English text is a translation; the German version is binding.