Data Processing Agreement (DPA)

Seamlesswork AG | Last updated: July 2026

This Data Processing Agreement ("DPA") forms an integral part of the Seamless Terms and Conditions ("Terms") and governs the processing of personal data by Seamlesswork AG on behalf of the Customer in connection with the Seamless product. By accepting the Terms, the Customer also accepts this DPA.

Contents

1. Purpose

1.1 Seamlesswork AG ("Provider") provides Customers with Seamless, a Governance Solution for Microsoft 365 ("Product"). The Product is provided under and in accordance with the Terms.

1.2 The provision of the Product involves the processing of personal data by the Provider on behalf of the Customer. The purpose of this DPA is to define the rights and obligations of the Parties in connection with such processing, in accordance with applicable data protection law.

1.3 This DPA is designed to assist the Parties in complying with the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") and the revised Swiss Federal Act on Data Protection (Bundesgesetz über den Datenschutz, "revFADP", SR 235.1), as well as any other applicable data protection legislation.

2. Scope

2.1 This DPA applies to all activities under the Terms in which the Provider processes personal data on behalf of the Customer. The categories of personal data processed, the purposes of processing, the categories of data subjects, and the applicable retention periods are set out in Annex 1 to this DPA.

2.2 The Provider processes only the personal data strictly necessary for the provision of the Product. The Provider does not process end-user content (documents, files, messages, or other communications) created or stored by the Customer's users within Microsoft 365. Such content remains exclusively within the Customer's Microsoft 365 tenant and is not accessible to the Provider.

3. Definitions

3.1 Unless otherwise defined in this DPA, all terms shall have the meaning ascribed to them in the GDPR, the revFADP, or the Terms, as applicable.

Term	Definition
Controller	The Customer, as the natural or legal person who determines the purposes and means of the processing of personal data.
Processor	The Provider (Seamlesswork AG), processing personal data on behalf of the Customer in accordance with this DPA and the Terms.
Sub-processor	Any third-party service provider engaged by the Provider to process personal data in connection with the Product. A list of current Sub-processors is set out in Annex 3 to this DPA.

Term	Definition
Security Incident	Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data processed under this DPA.
Data Subject	Any identified or identifiable natural person whose personal data is processed under this DPA.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.
revFADP	The revised Swiss Federal Act on Data Protection (Bundesgesetz über den Datenschutz), SR 235.1, in force since 1 September 2023.
Data Act	Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data.
Non-Personal Data	Any data that does not qualify as personal data under applicable Data Protection Laws.
Mixed Dataset	Any dataset that contains both personal data and Non-Personal Data.
Exportable Data	Customer-related data (personal or non-personal) that is generated or stored within the Product environment and which the Provider is required to make available to the Customer or a third party designated by the Customer under the Data Act and this DPA, excluding data that remains exclusively within Microsoft 365, Entra ID or other systems fully controlled by the Customer.
Switching	The migration by the Customer of Exportable Data from the Product to another data processing service or to the Customer's own environment, in accordance with the Data Act and this DPA.

4. Roles and legal responsibility

4.1 Within the scope of this DPA, the Customer acts as Controller and the Provider acts as Processor within the meaning of the GDPR and revFADP. The Customer remains solely responsible for the lawfulness of the processing of personal data instructed by it.

4.2 The Provider shall process personal data only on behalf of and on the documented instructions of the Customer, as set out in this DPA and the Terms, unless the Provider is required to process for another purpose under applicable law. In such a case, the Provider shall inform the Customer of the legal requirement before processing, unless prohibited by law.

4.3 The Customer warrants that the transfer of personal data to the Provider and the processing described in this DPA are permissible under applicable data protection law. The Customer is responsible for fulfilling its own obligations as Controller, including providing any required notices to data subjects and obtaining any necessary consents.

4.4 The Provider makes the technical and organisational measures described in Annex 2 to this DPA available to the Customer. The Customer is responsible for assessing whether these measures are sufficient for its intended use of the Product and for the personal data to be processed.

4.5 The Customer shall inform the Provider without undue delay if it becomes aware of any violation of data protection provisions or any instruction that, in the Customer's view, infringes applicable data protection law.

4.6 On request, the Customer shall provide the Provider with all information necessary to maintain a record of all processing activities carried out on the Customer's behalf, insofar as such information is not otherwise available to the Provider.

4.7 If the Provider is required to provide information to a governmental authority or other body in connection with the processing of personal data under this DPA, or to cooperate with such bodies, the Customer shall, upon first request, assist the Provider in providing such information and fulfilling any cooperation obligations.

5. Data processing and obligation to follow instructions

5.1 The Provider shall process personal data only in accordance with the documented instructions of the Customer as set out in this DPA, unless required to do otherwise by applicable law. The Customer's instructions are, in principle, exhaustively set out in this DPA. Individual instructions that deviate from or impose additional requirements beyond this DPA require the Provider's prior written consent and may result in additional costs to be borne by the Customer.

5.2 The Provider shall ensure that all persons authorised to process personal data on behalf of the Customer are bound by appropriate confidentiality obligations, whether contractual or statutory.

5.3 The Provider shall process personal data within the European Economic Area (EEA) or Switzerland. Any transfer of personal data to a country outside the EEA or Switzerland shall only be made where the requirements of Chapter V GDPR and the applicable provisions of the revFADP are satisfied, and the Customer is informed in advance.

5.4 The Provider may anonymise or aggregate personal data in a manner that makes it impossible to identify individual data subjects, and may use such anonymised or aggregated data for the purposes of improving the security and quality of the Product. The Provider shall not use such

data to train AI models without the Customer's prior written consent (see Section 7.2.1 of the Terms). Anonymised data does not constitute personal data for the purposes of this DPA.

6. Technical and organisational measures

6.1 The Provider shall implement appropriate technical and organisational measures ("TOMs") to ensure a level of security appropriate to the risk, in accordance with Art. 32 GDPR and Art. 8 revFADP. The TOMs currently implemented are described in Annex 2 to this DPA. The Provider is entitled to modify the TOMs over time, provided that the overall level of protection is not reduced.

6.2 The Provider shall ensure that all persons engaged in processing personal data on behalf of the Customer are subject to an appropriate duty of confidentiality with regard to such processing.

7. Support, information, and cooperation

7.1 The Provider shall assist the Customer, to the extent technically feasible and legally required, in fulfilling the Customer's obligations under the GDPR and revFADP, including data subject rights, breach notification, security obligations, and data protection impact assessments. The Customer shall reimburse the Provider for documented costs incurred in providing such assistance, unless the need arose from the Provider's own breach.

7.2 If a data subject submits a request directly to the Provider concerning the exercise of their rights under data protection law, the Provider shall forward the request to the Customer without undue delay. The Provider shall not respond to such requests directly without the Customer's prior authorisation, except as required by law.

7.3 The Provider shall provide the Customer with all information reasonably necessary to demonstrate compliance with the obligations set out in this DPA.

7.4 The Customer shall have the right to audit the Provider's compliance with this DPA upon at least thirty (30) days' prior written notice, at the Customer's expense. The Provider may, at its discretion, provide equivalent assurance through a current audit report or relevant certification (e.g. ISO 27001). If the Customer has reasonable grounds to believe such documentation is insufficient, it may request an on-site inspection. If the audit reveals a material breach by the Provider, the Provider shall bear the reasonable costs of the audit.

7.5 Upon becoming aware of a Security Incident, the Provider shall notify the Customer without undue delay, providing available information on the nature, scope, and likely consequences of the incident and the measures taken to address it.

8. Sub-processors

8.1 The Customer grants the Provider general authorisation to engage Sub-processors for the processing of personal data under this DPA. A list of Sub-processors currently engaged by the Provider is set out in Annex 3 to this DPA, which is updated from time to time.

8.2 The Provider shall inform the Customer in advance of any intended change to the list of Sub-processors, including the addition of new Sub-processors or the replacement of existing ones. The Customer may object to such a change on reasonable data protection grounds within thirty

(30) days of notification. If the Customer raises a valid objection and the Provider is unable to accommodate it, either Party may terminate the Terms in accordance with its terms.

8.3 The Provider shall impose on all Sub-processors data protection obligations at least equivalent to those set out in this DPA, by means of a written contract. The Provider remains liable to the Customer for the performance of Sub-processors' obligations under this DPA to the extent that the Provider would itself be liable.

8.4 Where a Sub-processor is located outside Switzerland or the EEA, the Provider shall ensure that an appropriate data transfer mechanism is in place, including where applicable the EU Standard Contractual Clauses (Implementing Decision (EU) 2021/914) and the Swiss Standard Contractual Clauses recognised by the Swiss Federal Data Protection and Information Commissioner (FDPIC), or equivalent safeguards under the revFADP.

9. Duration and termination

9.1 This DPA enters into force on the same date as the Terms and remains in force for as long as the Provider processes personal data on behalf of the Customer under the Terms.

9.2 Upon termination of the Terms for any reason, the Provider shall, at the Customer's choice and within a reasonable period: (a) return all personal data processed under this DPA to the Customer in a structured, commonly used, and machine-readable format; or (b) securely delete or destroy all such personal data and confirm in writing that this has been done. The Customer may permanently delete its Seamless configuration data at any time via the Seamless Admin Center; such deletion is irreversible.

9.3 The Provider may retain personal data beyond the period referred to in Section 9.2 to the extent required by applicable law, or as necessary to establish, exercise, or defend legal claims. Such retained data remains subject to the confidentiality and security obligations of this DPA.

10. Liability and indemnification

10.1 The Provider's liability under this DPA is governed by the limitations and disclaimers set out in the Terms (Chapter 11). Nothing in this DPA shall limit the Provider's liability where such limitation is not permitted by applicable data protection law (in particular, Art. 82 GDPR).

10.2 Where a third party asserts claims against the Provider arising from the Customer's breach of this DPA, the Customer's breach of applicable data protection law, or the Customer's instructions to the Provider, the Customer shall indemnify and hold the Provider harmless against such claims, including reasonable legal costs.

10.3 The Customer shall indemnify the Provider against any administrative fines or penalties imposed on the Provider by a supervisory authority to the extent that such fines are attributable to the Customer's conduct or instructions.

11. Data Act provisions

11.1 To the extent applicable, the Parties acknowledge that the Provider may qualify as a provider of data processing services and/or as a data holder under the Data Act in relation to Exportable Data stored within the Product environment. Data that remains solely within Microsoft 365, Entra ID or other systems controlled by the Customer is outside the scope of this Section 11.

11.2 The Provider shall make Exportable Data available to the Customer in a commonly used, machine-readable and structured format through self-service interfaces, including the export functionality available via the Seamless Admin Center and the Seamless API. Standard exports are provided free of charge. Additional efforts beyond standard export functionality that are expressly requested by the Customer may be charged at the Provider's standard hourly rate.

11.3 The Provider shall not impose unjustified contractual, technical or commercial obstacles to Switching. In particular, the Provider: (a) shall not charge specific fees for Switching, other than for additional services expressly requested by the Customer that exceed standard export capabilities; (b) shall enable the Customer, where technically feasible, to run the Product in parallel with another service during a reasonable transition period; and (c) shall provide reasonable cooperation and information necessary to enable the effective migration of Exportable Data to another service or to the Customer's own environment.

11.4 The Provider shall make available to the Customer documentation on the export formats, relevant data structures and interfaces, including APIs, used to access Exportable Data within the Product. Such documentation is available via https://sml-api.io/docs/ or on request from the Provider.

11.5 If the Provider receives a legally binding request from a third-country authority for access to Non-Personal Data or Mixed Datasets covered by the Data Act and stored within the EEA or Switzerland, the Provider shall, to the extent permitted by law: (a) notify the Customer of the request without undue delay; (b) assess the legality and scope of the request and challenge any request that appears manifestly unlawful; (c) provide access only to the extent strictly required to comply; and (d) document the request and response appropriately.

12. Governing law and jurisdiction

12.1 This DPA is governed by Swiss law, with the exception of its conflict-of-law rules, and the application of the United Nations Convention on Contracts for the International Sale of Goods (CISG) is excluded. To the extent the GDPR applies, the mandatory provisions of the GDPR shall take precedence where required.

12.2 Any dispute arising out of or in connection with this DPA shall be submitted to the exclusive jurisdiction of the courts of the Canton of Zurich, Switzerland (Bezirksgericht Zürich as first instance), unless mandatory law requires otherwise. This provision is without prejudice to the right of supervisory authorities to investigate complaints and enforce data protection law.

Annex 1 — Personal Data Processed

The following table sets out the personal data processed by the Provider on behalf of the Customer in connection with the Seamless product.

Category	Details
Categories of personal data	Company name; name of contact persons; business address; telephone number; email address; contractual data (contractual relationship, product, contractual interests); customer history, contract implementation, and payment data; Microsoft Entra ID Tenant ID; Microsoft Entra ID User Object IDs (for telemetry and licence management); primary contact name and email address of the Seamless Admin; Global Admin display name and consent date; audit logs (authentication against Seamless services); data related to the implementation and use of the Product; activity logs for troubleshooting purposes (retained for a maximum of 90 days for security and diagnostic purposes); Seamless configuration data (governance policies, templates, naming conventions, approval workflows).
Categories of data subjects	Employees (internal); contact persons; employees of external companies; interested parties; administrators and users of the Customer's Microsoft 365 environment who use or are managed via Seamless.
Purposes of processing	Provision, operation, and maintenance of the Seamless product and complementary services under the Terms (including collection, processing, analysis, transfer, and storage); licence management and usage tracking; support and troubleshooting; security monitoring; AI-assisted processing of personal data (in particular email addresses) via Microsoft Azure AI Foundry to enable AI-supported features of the Product; fulfilment of contractual obligations under the Terms; where applicable, the provision of Exportable Data and support for Switching and interoperability in accordance with the Data Act.
Legal basis	Processing is necessary for the performance of the Terms (Art. 6 para. 1 lit. b GDPR; Art. 31 para. 2 lit. a revFADP).
Retention period	Audit logs (authentication): 30 days. Activity logs for troubleshooting: 90 days. Entra ID User Object IDs for telemetry: 90 days. Tenant ID and admin contact data: for the duration of the Terms plus any legally required retention period. Seamless configuration data: until deleted by the Customer via the Seamless Admin Center or upon termination of the Terms.

Category	Details
Location of processing	Personal data is primarily stored in Switzerland (Microsoft Azure Switzerland North). AI-assisted features process personal data (in particular email addresses) via Microsoft Azure AI Foundry hosted in Sweden, within the European Economic Area. Static, non-personal assets are delivered globally via Microsoft Azure CDN. All personal data processing takes place within the EEA or Switzerland.

Annex 2 — Technical and Organisational Measures

The following summarises the key technical and organisational measures implemented by the Provider to ensure the security of personal data processed under this DPA.

A2.1 Entry Control

Measures to prevent unauthorised persons from accessing data processing systems with which personal data are processed.

The Product is a PaaS service hosted on Microsoft Azure and governed by Microsoft 365. There is no physical access to such environments.

A2.2 Access Control

Measures to prevent the use of data processing systems by unauthorised persons:

- Assignment of user rights and role-based access controls
- Authentication with username/password and second factor (multi-factor authentication)
- Access control governed by Conditional Access and Privileged Identity Management (PIM)
- Use of intrusion prevention systems
- Additional measures: web-application firewalls, regular vulnerability scans, regular penetration testing, patch management, minimum requirements for password complexity
- Encryption of storage accounts (AES-256)
- Hardware encryption for notebooks
- Use of a software firewall (office clients)

A2.3 Access Rights Control

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access rights and that personal data cannot be processed, used, or stored without authorisation:

- Creation of an authorisation concept
- Number of administrators reduced to the absolute minimum
- Logging of application access, especially for entry, modification, and data deletion
- Rights management by system administrators
- Password policy with guidelines on password length and password change management
- Entra ID User Object IDs are used as pseudonymous identifiers rather than names or email addresses

A2.4 Transfer Control

Measures to ensure that personal data cannot be read, copied, altered, or removed without authorisation during electronic transmission or while being transported or stored on data carriers:

- Documentation of data recipients and transmission times, including agreed deletion times
- Data disclosure (only) in anonymised or coded form
- TLS encryption (1.2 or higher) for all communications (web client, APIs)

A2.5 Input Control

Measures to ensure that it is possible to verify at a later date whether and by whom personal data can be entered, modified, or removed in data processing systems:

- Logging of entry, modification, and deletion of data
- Traceability of data entry, modification, and deletion by individual users
- Assignment of rights for entry, modification, and deletion of data based on an authorisation concept

A2.6 Instruction Control

Measures to ensure that data processed on behalf and in agreement with the data controller are only processed on its instructions:

- Selection of sub-processors taking into account their history (especially about information security)
- Written instructions to sub-processors
- Effective control rights assured by sub-processors
- Prior review of documentation and security measures taken by sub-processors
- Obligation of sub-processor's employees to maintain confidentiality
- Secure deletion of data at the end of the contract
- Continuous monitoring of sub-processors and their activities

A2.7 Availability Check

Measures to ensure that personal data is protected against accidental destruction or loss:

- The Product is hosted on Microsoft Azure with built-in redundancy and disaster recovery
- Testing of data recovery
- Creation of backup and recovery concepts
- Preparation of an emergency response plan
- Several data centres in the active configuration
- Uptime commitments are set out in the Terms (Section 10.2)

A2.8 Principle of Separation

Measures to ensure that personal data collected for different purposes are processed separately:

- Creation of an authorisation concept
- The Provider processes only the personal data strictly necessary for the provision of the Product (data minimisation). End-user content (documents, files, communications) is not processed or stored by the Provider; it remains within the Customer's Microsoft 365 tenant.

Annex 3 — Sub-processor List

Sub-processor	**Microsoft Ireland Operations Limited**
Registered office	Blackthorn Road, Dublin 18, Ireland
Data location	Switzerland (Azure Switzerland North); Sweden (Azure AI Foundry); global Azure CDN for static, non-personal assets
Purpose of processing	Cloud infrastructure and hosting (Microsoft Azure); identity management and authentication (Microsoft Entra ID); Microsoft 365 platform integration (Microsoft Teams, SharePoint Online, Graph API); AI-assisted processing of personal data (in particular email addresses) via Microsoft Azure AI Foundry in Sweden; Commercial Marketplace transaction processing, subscription management, and billing (Azure Marketplace / Microsoft Marketplace), including disclosure of customer contact information and transaction details to the Provider as publisher in accordance with Microsoft's Commercial Marketplace Terms of Use.
Transfer mechanism	EU entity (GDPR applies directly); processing locations Switzerland and Sweden, both recognised as adequate / within the EEA

Sub-processor	**HubSpot Ireland Limited**
Registered office	1 Sir John Rogerson's Quay, Dublin 2, Ireland
Data location	EU / USA
Purpose of processing	Customer relationship management (CRM); customer communication and support tracking; marketing automation.
Transfer mechanism	EU entity; Standard Contractual Clauses (EU) and Swiss SCCs for transfers to USA

Sub-processor	**Resend Inc.**
Registered office	375 Beale St Ste 300, San Francisco, CA 94105, USA
Data location	USA / EU
Purpose of processing	Transactional email delivery (e.g. onboarding notifications, system alerts, product communications sent to Customers and Users).

Sub-processor	**Resend Inc.**
Transfer mechanism	Standard Contractual Clauses (EU); Swiss SCCs

Sub-processor	**Harvest**
Registered office	99 Wall Street Suite 1310, New York, NY 10005, USA
Data location	USA
Purpose of processing	Time tracking and invoicing for direct billing outside the Marketplace (applicable to Scale Plans billed via direct invoice).
Transfer mechanism	Standard Contractual Clauses (EU); Swiss SCCs

Sub-processor	**Google Ireland Limited**
Registered office	Gordon House, Barrow Street, Dublin 4, Ireland
Data location	EU / USA
Purpose of processing	Website analytics (Google Analytics) to analyse usage of our websites. IP anonymisation is activated. Data is collected in pseudonymous form.
Transfer mechanism	EU entity; Standard Contractual Clauses (EU) and Swiss SCCs for transfers to USA