

Data Processing Agreement (DPA)

This Data Processing Agreement (hereinafter "DPA") specifies the data protection obligations arising from the contractual relationship between Z83 AG (hereinafter "Processor") and its clients (hereinafter "Controller"). This DPA applies to all activities arising from the contractual relationship between the parties in which employees of the Processor or third parties commissioned by the Processor process personal data (hereinafter "Data") of the Controller. For any data protection matters, the Controller may contact the Processor's data protection officer at datenschutz@z83.ch.

PREAMBLE

- a. The Controller and the Processor have entered into an agreement (hereinafter "Main Agreement") under which the Processor provides services or other deliverables for the Controller as specified in the Main Agreement.
- b. For the purpose of fulfilling the Main Agreement, the Processor may have access to personal data disclosed to the Processor by the Controller directly or on behalf of the Controller by third parties or made available to the Processor in other ways (hereinafter "Personal Data").
- c. The parties wish to ensure that the processing of Personal Data by the Processor on behalf of the Controller is in accordance with applicable data protection laws. They agree to regulate the terms of such data processing in this DPA (hereinafter the "Agreement").

Having set forth the foregoing, the parties agree as follows:

1. Definitions

1.1. Applicable Data Protection Laws

Refers to 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 and on the free movement of such data (hereinafter "GDPR"), the Swiss Federal Act on Data Protection (FADP), the Swiss Ordinance to the FADP (OFADP), and any other applicable data protection laws.

1.2. Controller

A natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data (Art. 4 para. 7 GDPR; Art. 5 FADP).

1.3. Processor

A natural or legal person who processes personal data on behalf of the Controller (Art. 4 para. 8 GDPR).

1.4. Personal Data

Any information relating to an identified or identifiable natural or legal person (hereinafter "Data Subject"). An identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person (Art. 4 para. 1 GDPR; Art. 5 FADP).

1.5. Processing

Any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, restriction, erasure, or destruction (Art. 4 para. 2 GDPR; Art. 5 FADP).

2. Scope and Subject Matter

2.1. Scope

This Agreement applies to all processing of personal data by the Processor on behalf of the Controller.

2.2. Subject Matter, Duration, Nature, and Purpose

The subject matter, duration, nature, and purpose of the processing are defined in the Main Agreement and in Annex 1, unless already specified in the Main Agreement and its service description.

2.3. Type of Personal Data / Categories of Data Subjects

The types of personal data and categories of data subjects are specified in Annex 1, unless already sufficiently detailed in the Main Agreement and its service description.

3. Obligations of the Processor

3.1. Processing According to Instructions

The Processor shall process the Data exclusively for the purposes of fulfilling the Main Agreement and in accordance with the Controller's documented instructions, including those regarding transfers to a third country or an international

organization. If the Processor is required by EU or Member State law, or the law of a non-EU state to which it is subject, to process data beyond the instructions, it must inform the Controller in advance unless prohibited by law.

The Controller may issue, amend, or supplement instructions at any time, including regarding rectification, deletion, or blocking of personal data. Instructions must be documented in writing by both parties. If the Processor considers any instruction unlawful, it must immediately notify the Controller and may suspend execution until clarified. The Processor may refuse to implement clearly unlawful instructions.

The Processor's obligations under applicable data protection laws remain unaffected, including maintenance of a record of processing activities (Art. 30 para. 2 GDPR).

3.2. Confidentiality

The Processor ensures that all persons authorized to process personal data are bound to confidentiality or are subject to an appropriate statutory obligation of confidentiality, and that these obligations continue after termination of their activities. The Processor is liable for breaches by its personnel or subcontractors as for its own actions.

3.3. Security Measures

The Processor shall implement and maintain appropriate technical and organizational measures (TOMs) to ensure the security of processing as required by Art. 32 GDPR and Art. 7 FADP. The minimum measures are described in Annex 2.

3.4. Assistance Obligations

The Processor shall assist the Controller, to the extent possible, in fulfilling its obligations under applicable data protection laws.

a. Data Subject Requests

The Processor shall assist the Controller in responding to data subject requests (under Chapter III of the GDPR and Chapter 4 of the FADP), such as access, rectification, deletion, data portability, objection, and automated decision-making. If a request is made directly to the Processor, it must immediately forward it to the Controller and not respond unless legally obligated. Both parties will coordinate responses.

b. Further Assistance

The Processor shall assist the Controller in complying with obligations under Articles 32 to 36 GDPR and Chapter 4 of the FADP, including data breach notifications, data protection impact assessments (DPIAs), and prior consultations with authorities. The Processor shall promptly notify the Controller of any (i) actual or suspected data breaches, (ii) deficiencies impacting compliance with this Agreement, and (iii) requests or actual access by public authorities (unless prohibited by law).

3.5. Return or Deletion of Data

Upon termination of the Main Agreement, the Processor shall, at the Controller's choice, return or securely delete all personal data unless otherwise required by law, and confirm such deletion to the Controller.

3.6. Audits and Inspections

The Processor shall make available all necessary information to demonstrate compliance and allow for audits or inspections by the Controller, its auditors, or supervisory authorities. Audits shall be conducted without disrupting the Processor's operations.

4. Location of Data Processing

Processing shall only occur at the locations specified in Annex 3 or approved in writing by the Controller. No personal data may be transferred to a third country without prior written consent from the Controller. For processing outside the EU/EEA, appropriate safeguards must be in place in accordance with Art. 45 et seq. GDPR and Art. 16 et seq. FADP, such as:

- Adequacy decisions
- EU standard contractual clauses
- Binding corporate rules
- Approved codes of conduct
- Certification mechanisms
- Exceptions under GDPR/FADP for specific situations.

5. Use of Sub-Processors

The Processor may engage sub-processors listed in Annex 4, which shall be updated regularly. The Controller shall be informed in advance of any intended changes, providing the opportunity to object. The Processor must ensure sub-processors are bound by data protection terms at least as strict as those in this Agreement. The Processor is fully liable for the sub-processors' compliance with their obligations.

6. Additional Agreements

Upon reasonable request by the Controller, the Processor agrees to conclude additional agreements necessary to comply with data protection laws.

7. Extraordinary Termination

The Controller may terminate this Agreement immediately without notice if the Processor commits a serious breach of data protection laws or this Agreement, refuses to follow lawful instructions, or denies audit rights in breach of contract. Material breaches include non-compliance with obligations under Art. 28 GDPR.

8. Relationship with the Main Agreement

- 8.1. Annexes are integral parts of this Agreement.
- 8.2. In case of conflict between this Agreement and the Main Agreement, the provisions of this Agreement shall prevail.
- 8.3. This Agreement shall survive termination of the Main Agreement as long as the Processor retains personal data of the Controller.

9. Final Provisions

- 9.1. Amendments or supplements to this Agreement require written form.
- 9.2. If any provision is invalid, the remaining provisions shall remain in effect. The invalid provision shall be replaced with a valid provision that best reflects its original intent.
- 9.3. This Agreement is governed by Swiss law, excluding conflict of laws rules (IPRG). The exclusive jurisdiction is the Controller's registered office.

Annexes

Annex 1: Specification of Processing

Annex 2: Technical and Organizational Measures (TOMs)

Annex 3: Approved Data Processing Locations

Annex 4: Authorized Sub-Processors

Annex 1: Specification of Processing

1. Subject and Purpose of Processing

The Controller's engagement of the Processor covers the following tasks and/or services:

Processing of personal data on behalf of the Controller by Run My Accounts AG and Z83 AG for accounting and payroll services, including hotline support services and consulting.

2. Types of Personal Data

The following types of personal data are regularly subject to processing or may be accessed by Infoniqa employees during maintenance and/or support activities:

- **Master Data of Individuals** (e.g., name, address, date of birth, marital status, job title, company affiliation, bank details, nationality, passport/ID details, and any other information required for payroll accounting and (withholding) tax purposes, including health data in the event of accident or sick leave notifications)
- **Communication Data** (e.g., telephone numbers, email addresses)
- **Contract, Billing, and Payment Data**

3. Categories of Data Subjects

- Employees of the Controller
- (Potential) Clients of the Controller
- Suppliers of the Controller
- Freelancers of the Controller
- Business Partners of the Controller
- Other Data Subjects

Annex 2: Technical and Organisational Measures

The following technical and organisational measures are based on Article 32 GDPR, Article 7 FADP, and Articles 8 et seq. OFADP. They specify the minimum precautions to be implemented by the Processor in connection with the processing of personal data and the fulfilment of its obligations under the Main Agreement, including this Agreement. These measures are designed to ensure an appropriate level of security in relation to the risk, concerning the protection of personal data and data security.

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

1.1. Physical Access Control

Unauthorised access to data processing facilities is prevented through the following measures at each location:

- Alarm systems
- Reception personnel controlling visitor access
- Visitor logging and registration
- Careful selection and supervision of cleaning personnel
- Secure, locked server rooms

1.2. System Access Control

Unauthorised use of IT systems is prevented at all locations through:

- Regulations on the use of data carriers and workstations/mobile devices
- Authentication by user ID and password
- Use of screensavers and manual locking of workstations
- Access by external service providers is restricted to business hours
- Policies for securing documents and locking offices and cabinets

1.3. Data Access Control

Unauthorised reading, copying, modification, or removal of data within IT systems is prevented at all locations by:

- Role-based access rights managed by the system administrator
- Minimisation of the number of system administrators
- Secure storage of administrator passwords
- Password policies including minimum length and regular password changes
- Logging of access to applications, particularly when entering, changing, or deleting data (in preparation)
- Physical erasure of data storage devices prior to reuse
- Proper destruction of data storage media
- Encryption of notebooks and mobile device management
- Use of document shredders for the destruction of paper-based data

1.4. Data Separation Control

Separation of data belonging to different clients is ensured at all locations through:

- Physical separation via dedicated systems or data carriers
- Logical separation of client data (software-based multi-tenancy)
- Implementation of an authorisation concept
- Definition of database access rights
- Separation of production and test environments
- Provision of guest Wi-Fi at all locations
- Secure data rooms for data exchange

1.5. Pseudonymisation (Article 32(1)(a) GDPR; Article 25(1) GDPR)

Personal data is processed in such a way that, without additional information, it can no longer be attributed to a specific data subject. Such additional information is stored separately and protected by appropriate technical and organisational measures. Pseudonymisation is implemented in certain applications.

2. Integrity (Article 32(1)(b) GDPR)

2.1. Data Transfer Control

Unauthorised reading, copying, modification, or removal of data during electronic transmission or transport is prevented at all locations through:

- No physical transport of data carriers
- Use of secure data rooms for data exchange

3. Regular Review, Assessment, and Evaluation Procedures (Article 32(1)(d) GDPR; Article 25(1) GDPR)

- All employees of the Processor and its service providers are immediately obligated, upon commencing work, to maintain confidentiality with respect to personal data and postal secrecy.
- A data protection management system is maintained.
- An incident response management process is in place.
- Data protection-friendly default settings are applied in the planning and development of systems (Article 25(2) GDPR; Article 7 nFADP).
- The execution of processing activities is monitored in accordance with the contractual agreement. No processing under Article 28 GDPR or Article 9 nFADP is performed without specific instructions from the Controller:
 - a. Formalised contract management
 - b. Strict selection criteria for service providers
 - c. Monitoring and auditing of service providers

Annex 3: Approved Data Processing Locations

- Switzerland
- EU Member States (e.g., Austria, Germany, Czech Republic, Poland)
- Countries with an adequacy decision by the European Commission (e.g., the United Kingdom)
- United States (companies certified under the Data Privacy Framework or with agreements based on Standard Contractual Clauses)
- Canada (with agreements based on Standard Contractual Clauses)

Annex 4: Authorized Sub-Processors

The Processor is authorized to engage the following companies as sub-processors:

- Accosense AG
- Advokatur Notariat Verwaltungen - LIC. IUR. Brigitte Sterki Lang
- Barandun AG
- Detof GmbH
- INNOSTA AG
- KSCP Simmen Cattin AG
- Ostschweizerische Treuhand Zürich AG
- Personaltreuhand Gnägi
- Prof. Dr. iur. Peter Ruf AG
- Rohner & Erni Tax AG
- Run my Accounts AG
- TaxWare AG
- Thomas Schneider Treuhand & Unternehmens-Entwicklung GmbH
- Varsity Lakes AG
- ZeedOne GmbH