

Agreement on Contract and Data Processing

Innov8iveIT Solutions GmbH
Schaanerstrasse 27
9490 Vaduz

If any part is unclear, please reference the German version "ADV German".

1 Introduction

This agreement specifies the obligations of the parties with regard to the requirements of the Swiss Data Protection Act (DSG) and the EU General Data Protection Regulation (GDPR). It supplements the contractual agreements ("Contract") between IITS and the customer in this respect. This may involve a single or multiple contracts between IITS and the customer, in which IITS acts as a service provider to the customer.

This agreement applies only to the extent that the following conditions are met:

1. The customer is either the controller or processor within the scope of the DSG and/or GDPR, and
2. the customer engages IITS as a processor or sub-processor for the processing of personal data or personal-related data that are covered by the scope of the DSG and/or GDPR ("relevant data").

2 Subject, Duration and Type of Data Processing

The subject, duration, as well as the type and purpose of the processing are defined in the contract. The categories of relevant data processed, the categories of affected individuals, and the technical and organizational measures ("TOM") to be implemented are listed in the appendix of this agreement.

3 Scope and Responsibility

IITS processes the relevant data exclusively for the purpose of fulfilling the contract or for the purposes stated in the contract. The customer is responsible for the legality of the data processing itself, including the permissibility of the contract/sub-contract processing.

The customer's instructions are documented in this agreement and the contract. The customer has the right to issue additional written instructions to IITS at any time regarding the processing of the relevant data. IITS will comply with these instructions as long as they are feasible within the scope of the services contractually agreed upon by IITS and are objectively reasonable. If such instructions result in additional costs for IITS or a changed scope of services, the contractually agreed procedure for contract modification applies.

IITS will inform the customer immediately if it believes that an instruction violates the DSG or the EU GDPR. In such cases, IITS may suspend the implementation of the instruction until it has been confirmed or modified by the customer. The above does not apply to customer instructions related to the assignment of access rights or the release of relevant data to the customer themselves, and IITS may at any time assume that these instructions are compliant with the law. However, it is entitled to request corresponding written confirmations from the customer.

4 Duties of IITS

IITS processes the relevant data exclusively according to the provisions of the contract and this agreement. This is subject to the fulfillment of legal, regulatory, or governmental obligations by IITS.

IITS will implement the Technical and Organizational Measures (TOM) defined in the contract and the appendices to this agreement to protect the relevant data. IITS may adjust the agreed TOM at any time,

provided that the agreed level of protection is not reduced. In addition, IITS continuously reviews the agreed TOM against the current state of technology and, if necessary, proposes to the customer the implementation of additional measures, which can be agreed upon in a contractual amendment.

IITS commits to maintaining a directory of processing activities concerning the relevant data in accordance with Art. 12 para. 1 of the DSG or Art. 30 para. 2 of the EU GDPR. IITS will grant the customer access to the parts of this directory affected by its service provision upon request.

IITS ensures that its employees and other assistants involved in processing the customer's relevant data are prohibited from processing the relevant data for purposes other than those stated in the contract and deviating from this agreement. Furthermore, IITS ensures that the persons authorized to process the relevant data have committed to confidentiality and/or are subject to an appropriate statutory duty of secrecy. The duty of confidentiality/secrecy continues even after the contract has ended.

IITS will immediately inform the customer if it becomes aware of any breaches of the protection of the relevant data at IITS or any of its sub-processors (Data Breach). IITS will inform the customer in writing (email is sufficient) in a reasonable manner about the nature and extent of the breach as well as possible remedial measures. In such a case, the parties will take the necessary measures to ensure the protection of the relevant data and to mitigate any potential adverse effects on the affected individuals and the parties and will coordinate immediately.

IITS will provide the customer with a contact person for data protection issues arising under the contract and, where required according to Art. 37 EU GDPR, the data protection officer.

IITS commits to supporting the customer in fulfilling the rights of the affected persons against the customer according to Chapter 4 of the DSG or Chapter III of the EU GDPR, upon request and against a separately agreed remuneration. Furthermore, IITS may offer the customer additional support, for example, in connection with a data protection impact assessment, consultation of the supervisory authority, notifications to the latter, etc., against separate remuneration.

Relevant data must be handed over or deleted according to the contractual provisions after the contract ends. IITS uses established procedures in the IT industry for the deletion of relevant data.

5 Duties and Obligations of the Customer

The customer independently takes appropriate technical and organizational measures to protect the relevant data within their area of responsibility (e.g., on their own systems, buildings, applications/environments under their operational control).

The customer must inform IITS immediately if they detect any violations of data protection regulations in the performance provided by IITS.

The customer provides IITS with a contact person for data protection issues arising under the contract and, where required according to Art. 37 EU GDPR, the data protection officer.

6 Inquiries from Data Subjects

If a data subject approaches IITS with requests for correction, deletion, information, or other claims concerning relevant data directly, IITS will refer the data subject to the customer, provided that the data subject can be associated with the customer according to their information. The support provided by IITS to the customer regarding inquiries from data subjects is governed by clause 4.

7 Evidence, Reports, and Audits

IITS is obliged to provide the customer with information upon request to document compliance with the obligations according to this agreement.

The parties acknowledge that compliance with this obligation is generally evidenced by IITS being certified according to ISO 27001, or by IITS providing the customer with reports or similar audit reports or confirmations created by an independent third party concerning certain areas, or certifications specifically mentioned in the contract, etc. Any audit rights defined in the contract, as well as legally mandatory inspection rights of the customer or their supervisory authorities, are reserved. In any case, such audits must adhere to the principle of proportionality and adequately consider the legitimate interests of IITS (notably confidentiality). Unless otherwise agreed, the customer bears all costs of such audits (including proven internal costs of IITS incurred during participation in the audit).

If violations of this agreement or deficiencies in the implementation of IITS's obligations are identified after the presentation of evidence or reports or during an audit, IITS must immediately and at no cost implement appropriate corrective measures.

8 Involvement of Sub-Processors

To the extent that the contract does not contain restrictive provisions regarding the involvement of third parties, IITS is entitled to engage sub-processors but must inform the customer in advance if it engages new sub-processors or replaces existing sub-processors after this agreement comes into effect. The customer may object in writing to the engagement of a new or the replacement of an existing sub-processor for significant data protection reasons within a period of 30 days. If there is a significant data protection reason and if a mutually agreeable solution is not possible between the parties, the customer will be granted the right to terminate the service affected by this. IITS will make agreements with its sub-processors to the extent necessary to ensure the obligations according to this agreement are met.

9 Disclosure Abroad

Any disclosure of relevant data by IITS abroad or to an international organization is only permissible if IITS complies with the provisions of Art. 16 et seq. of the DSG or Chapter V of the EU GDPR. However, if such disclosure of relevant data is desired by the customer or occurs on their behalf, compliance with the relevant provisions is exclusively the responsibility of the customer.

10 Final Provisions

The article numbers of the DSG refer to the revised DSG (BBl 2020 7639). Before its entry into force, the provisions agreed herein apply correspondingly. The term of this agreement is aligned with the term of all contracts between IITS and the customer under which IITS processes relevant data for the customer, unless the provisions of this agreement result in longer-lasting obligations.

Notwithstanding any written form requirements specified in the contract, this agreement may also be agreed upon or amended electronically between the parties.

The obligations from this agreement are in addition to the obligations set out in the contract and do not restrict the latter. In the event of a conflict regarding the TOM generically set out in an annex to this agreement, the provisions of the contract shall prevail. Otherwise, the provisions of the contract remain unchanged.

Attachment

1 Data Elements Used

1.1 General

The Customer provides IITS with personal data for processing under the terms of the agreements, at its own discretion and on its behalf.

1.2 Data Subjects

The personal data may pertain to the following categories of data subjects:

- Potential customers, customers, business partners, vendors, and merchants of the customer—who are natural persons
- Employees or other agents of potential customers, customers, business partners, vendors, or merchants
- Employees or other agents of the customer, who have been authorized by the customer to use the services

1.3 Types of Personal Data

This may include, but is not limited to, the following types of personal data:

- Personal information such as first name, last name, date of birth, age, gender, nationality, etc.
- Business contact details such as email address, phone number, address
- Private contact details such as email address, phone number, address
- Employment-related information such as job title, function, etc.
- User information such as login details, customer number, employee number, etc.
- Technical information such as IP address, device information, etc.

1.4 Special Categories of Personal Data

These data categories include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data or biometric data for the unique identification of a natural person, health data, or data related to sexual life or sexual orientation.

1.5 Confidential Data

This data may include, for example, information subject to professional secrecy, banking secrecy, official secrecy, or confidentiality obligations under social security law.

2 Technical and Organizational Measures

The following chapters describe the measures taken by IITS regarding the protection of personal data within the scope of data processing. The measures listed below are to be understood as generic and shall apply unless otherwise defined in the contract.

IITS has taken (among other things) the following measures to prevent unauthorized access to data processing systems:

- Assignment of user rights
- Access based on a permission concept according to the Need-to-Know principle
- Password assignment with minimum requirements for password complexity
- Authentication with username/password and multi-factor authentication
- Use of intrusion prevention systems and firewalls
- Use of multiple network zones
- Use of personalized user profiles
- Deployment of web application firewalls
- Regular external vulnerability scans
- Patch management
- Use of antivirus software
- Use of VPN technology
- Use of mobile device management
- Reduction of the number of administrators to a necessary minimum
- Encryption of transmitted data using TLS
- Encryption of stored data according to FIPS 140-2
- Control of permissions upon employee onboarding and offboarding

2.1 Access Control (Data)

IITS has (among other things) implemented the following measures to ensure that users only have access to the data they are authorized to access and to prevent personal data from being read without authorization:

- Use of a role-based authorization concept according to the Need-to-Know principle
- Reduction of the number of administrators to the necessary minimum
- Logging of application access
- Secure media cleaning before reuse
- Use of shredders
- Encryption of transmitted data using TLS
- Rights management by system administrators
- Password policy with applicable minimum requirements for password complexity
- Compliant destruction of storage media
- Control of permissions upon employee onboarding and offboarding

2.2 Transmission Control

IITS has taken (among other) measures to ensure that personal data cannot be read, copied, or modified during electronic transmission, transport, or storage:

- Use of Dedicated Line and/or VPN Connections
- Encryption of Transferred Data with TLS
- Documentation of Data Recipients and Transfer Times
- Careful Selection of Transport Personnel and Vehicles for Physical Transport, and Encryption of Storage Media

- Data Disclosure Only in Anonymized or Pseudonymized Form

2.3 Input Control

IITS has (among others) implemented the following measures to ensure that it is possible to trace and control whether and by whom personal data is entered, modified, or deleted from data processing systems:

- Logging of Data Entry, Modification, and Deletion
- Traceability of Data Entry, Modification, and Deletion through Individual User Profiles
- Authorization for Data Entry, Modification, and Deletion Based on a Defined Authorization Concept

2.4 Order Control

IITS has taken the following measures to ensure that, under its direction and in agreement with the data controller, the processed data is only processed according to the controller's instructions:

- Careful Selection of Subcontractors: Subcontractors are selected based on their track record, particularly in terms of information security.
- **Written Instructions to Subcontractors:** Subcontractors are provided with written instructions in accordance with the Data Processing Agreement.
- **Ensure Appointment of Data Protection Officers:** Subcontractors must appoint Data Protection Officers (DPOs) to ensure data protection compliance.
- Effective Control Rights by Data Processor
- Prior Review of Documentation and Security Measures
- Confidentiality Obligations for Data Processor Staff
- Secure Deletion of Data after Contract Termination
- Ongoing Monitoring of Subcontractors and Their Activities

2.5 Separation Control

IITS has (among other things) implemented the following measures to ensure that data collected for different purposes can be processed separately:

- Ensuring that customer data is not accessible to other customers through logical or physical separation.
- For pseudonymized data: separating the mapping file and storing it on a separately secured IT system.
- Separation of production and test systems.