Data Processing Agreement (DSG)
including Technical and Organisational Measures (TOM)

Table of Contents:

This data processing agreement (Agreement) governs the processing of personal data by or on behalf of the service provider within the framework of the underlying master agreement. The scope of the data processing (subject, purpose, categories of data, etc.) results directly from the master agreement, unless otherwise specified and outlined below.
The duration of the data processing is determined by the term of the underlying master agreement and can only be terminated in the ordinary or extraordinary course together with said agreement.

Provisions on Data Processing

The parties have entered into a master agreement under which the service provider processes personal data on behalf of the client. This agreement is intended to govern such data processing for the purposes of the Swiss Data Protection Act (DSG) and, where applicable, the General Data Protection Regulation (DSGVO).
The transfer of personal data to a country without an adequate level of data protection (in accordance with Annex 1 of the Data Protection Ordinance (DSV)) is not permitted.
Any processing of personal data for the service provider's own purposes requires an explicit and separate agreement and is otherwise prohibited.

1) Definitions:

The following defined terms are used in this agreement. In all other respects, terms shall have the meaning defined in the Swiss Data Protection Act (DSG) and, where applicable, the General Data Protection Regulation (DSGVO), in particular "personal data", "processing", "processor", and "controller".

"DSG" refers to the Swiss Federal Act on Data Protection in its current version, including its ordinances.

"DSGVO" 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, on the free movement of such data, and repealing Directive 95/46/EC.

"EWR" refers to the European Economic Area.

"**A country with an adequate level of data protection"** is a country or territory listed in Annex 1 of the Swiss Data Protection Ordinance (DSV).

"**Affiliated company**" means a legal entity which is directly or indirectly controlled by the client, which directly or indirectly controls the client, or which is directly or indirectly under common control with the client.

2) Processinhg on Behalf:

1. Scope and Characteristics of Data Processing on Behalf

This agreement governs, within the scope of fulfilling the main contract**, the processing of personal data** by the service provider as a processor on behalf of the client as the controller.

Alternatively, the service provider may act as a sub-processor of the client, and the client may act as a processor of a third party.

If the client itself is acting as a processor (e.g., of a customer), then, to the extent permitted, only the client shall be responsible for communication with the controller, and the client's instructions shall be deemed those of the controller.

Personal data refers to all data that the service provider receives in the course of processing from the client, an affiliated company, or a third party.

The subject matter, duration, nature, and purpose of the processing, as well as the categories of personal data processed and the categories of data subjects, are defined as specified under section c, clause 5 of this agreement.

2. Processing of Personal Data

Obligations oft he Client

The client confirms to the service provider that:
it has made all notifications, registrations, regulatory approvals, and obtained all consents from data subjects that are required for the lawful processing of personal data by the service provider as processor under the DSG and, where applicable, the DSGVO; and
it responds to all requests from data subjects exercising their rights under the applicable data protection regulations.

Obligations of the Service Provider

The service provider undertakes and warrants to the client:

a) to process personal data solely for the purposes of the client and exclusively for the **performance** of the main contract in accordance with the documented instructions of the client;
b) to process personal data only at the **locations** agreed upon or otherwise approved by the client;
c) not to disclose or transfer personal data abroad, unless the client requests this as part of the commissioned service;
d) to implement and maintain appropriate technical and organizational measures (TOM according to the annex of this DPA) to ensure the confidentiality, integrity, and availability of personal data at all times and to protect personal data from unauthorized processing, access, or disclosure, as well as from accidental or unlawful alteration, destruction, or loss, in particular and at a minimum the data security measures stipulated in the DSG and, where applicable, in Article 32 of the DSGVO and other applicable data protection regulations; the service provider shall regularly review these measures for compliance and effectiveness and propose improvements or adjustments to the client where appropriate;
to rely on employees and other auxiliary persons (including all subprocessors acting under the instruction of the service provider) for the processing of personal data who are contractually or legally bound to confidentiality and obligated not to use or process personal data for any purpose other than to perform the tasks assigned to them by the service provider in accordance with the main contract and this agreement, it being further agreed between the parties that the service provider remains liable for the conduct of its employees and other auxiliary persons as for its own conduct;
to delegate the processing of personal data to subprocessors only if the client has not objected to their engagement. The service provider must inform the client of the engagement of a subprocessor sixty (60) days in advance. The engagement is deemed approved if the client does not object within thirty (30) days. Iomarket may use the subprocessors listed under the title “Subprocessors of io market AG” for the

respective services when processing personal data. The service provider must ensure that the subprocessor is bound to confidentiality and data protection provisions that are at least as stringent as those in the main contract and this agreement, it being further agreed between the parties that the service provider remains liable for the conduct of its subprocessors as for its own conduct, and that it shall immediately and appropriately inform the client of any change in the contact details, location, or other important aspects of its subprocessors. Any changes affecting data protection aspects require renewed approval. Further subprocessing by the subprocessor is not permitted.

to notify the client without delay and in any case within 24 hours to the address designated by the client (or in the absence of such, to the contact address on the signature page): (i) of any actual or suspected personal data breach or data security breach (which also includes any violation of this section 2.0 and any other breach of the protection of personal data under the DSGVO, the DSG, and other applicable data protection regulations), together with all information pursuant to Article 33(3) DSGVO, the relevant provisions of the DSG, and other applicable data protection regulations as well as, upon first request, such further information and explanations as required under section 2 (v) (e.g. root cause analysis), (ii) of any actual or threatened deficiency or inadequacy in the service provider's compliance with any provision of this agreement including any reasonably requested **information and explanations** related thereto, (iii) of any request for or actual access to personal data by authorities or other bodies, unless applicable law expressly prohibits notification for important reasons of public interest; in the case of (iii), the service provider shall furthermore attempt to resist and limit any such access to personal data to the extent reasonable and unless instructed otherwise by the client;

to support the client upon request in complying with the DSGVO, the DSG, and other applicable data protection regulations in the manner requested by the client and taking into account the nature of the processing as well as the information available to the service provider, especially in fulfilling its obligations (i) towards data subjects exercising their rights under **applicable data protection regulations** (including Chapter III of the DSGVO and the relevant provisions of the DSG and other applicable regulations), and (ii) under Articles 32 to 36 of the DSGVO and the corresponding provisions of the DSG and other applicable data protection regulations;

to inform the client immediately if, in its opinion, an instruction from the client violates applicable data protection or other relevant regulations; to the extent reasonable, it shall continue processing in the absence of other instructions;

to provide the client with all information necessary to demonstrate the service provider's compliance with its obligations and to allow and cooperate with **audits and inspections** (including on-site) by the client or by audit firms appointed by the client; the service provider shall provide the client with audit reports prepared by its audit firms, which confirm or document compliance with or breaches of the obligations set out in this agreement or legal requirements, without additional costs upon request or on its own initiative; the service provider shall ensure that the client can exercise these audit rights also with respect to subprocessors; the service provider shall also remedy any deficiencies identified without culpable delay and at its own expense and provide evidence thereof; if material deficiencies are identified during an audit or inspection, or if the service provider gives cause for such audit or inspection, it shall bear the related costs and expenses; and

at the client's discretion, subject to applicable legal retention obligations, to return or delete all or certain personal data at the end of the main contract or upon request by the client, without retaining a copy, and to confirm such **deletion** to the client.

Indemnification

The service provider shall indemnify and hold the client harmless from and against any claims by third parties arising from a breach of this agreement or applicable data protection regulations. Such indemnification particularly applies to all damages, costs, administrative sanctions, claims, or expenses incurred by the client because of such breaches. This indemnification, as well as any potential claim for damages by the client and its affiliated companies, shall—unless expressly agreed otherwise in relation to this clause—be subject to double the amount of any liability limitation agreed upon in the main contract. Any exclusion of liability for slight negligence shall not apply.

3) Miscellaneous Provisions:

The parties further agree as follows:

This agreement shall also apply for the benefit of the client's **affiliated companies** for whom the service provider processes personal data in accordance with the main contract. Accordingly, the client's affiliated companies may assert the same rights against the service provider as the client, and the service provider shall have the same obligations towards them under this agreement as towards the client.

Each party shall comply with its **obligations** under the applicable data protection regulations, in particular those under the DSG and, where applicable, the DSGVO.
The currently valid version is published online on the website. Insofar as different linguistic versions exist due to translated versions, the German version shall prevail.

This agreement shall be deemed an independent agreement in addition to the main contract. In the event of any contradictions between the provisions of this agreement and those of the main contract, the provisions of this agreement shall prevail to the extent they relate to the processing of personal data by the service provider under the main contract.

The provisions of this agreement shall remain in effect even after the termination of the main contract and shall continue to apply as long as the service provider is in possession of, or has access to, the personal data covered by this agreement.

The provisions of this agreement are subject to Swiss law. The place of jurisdiction is specified in the main contract.

Annex:
Technical & Organisational Measures (TOM)

In today's digital world, data protection and information security are of the utmost importance. This is especially true for communication and EDI services such as iomarket. To ensure the security and confidentiality of user data, the application of effective technical and organisational measures (TOM) is essential.
The following sections outline the specific data protection measures implemented at iomarket and on the "gate2b platform" to ensure compliance with data protection and information security standards.
The measures are based on the Swiss Federal Act on Data Protection (DSG), which provides a solid foundation for data security. In accordance with the DSG, iomarket undertakes to implement comprehensive technical and organisational measures (TOM) to ensure the confidentiality, integrity, and availability of your data.

Additionally, iomarket follows the Data Protection Ordinance (DPO) in order to cover specific areas of security in detail. These legal requirements serve as a guideline for keeping data safe and protected.

1. General Security Measures

Access Control

Regulates physical access permissions within the organisation

- Doorbell system with intercom / reception
- Access is controlled via electronic security locks and two security doors
- Access rights are managed by the administration and logged
- User rights are managed by the administrators and logged
- Visitors may only enter business premises when accompanied by employees
- Careful selection of cleaning personnel
- Key management
- Visitor registration

System Access Control

Ensures that only authorised persons can access systems

- Data privacy safe
- Password assignment
- Assignment of user rights
- Authorisation / authentication concepts with access regulations restricted to what is strictly necessary (''need to know'')
- Automatic desktop lock
- Two-factor authentication
- Use of hardware firewalls
- Use of software firewalls
- Use of user profiles

Data Access Control

Ensures that data processing is carried out according to granted permissions

- User authorisations
- Clean desk policy
- Hardware encryption
- Rights management for system administrators
- Blocking of access rights upon staff changes
- Password policies
- Awareness training to prevent phishing

2. Specific Measures

Transmission Control

Measures to ensure that personal data cannot be read, copied, altered, or removed without authorisation during transmission

- Encryption (e.g. TLS)
- Securing communication channels
- Hardware encryption

Order Control

Ensures that data is processed on behalf of the controller strictly according to instructions

- Conclusion of data processing agreements (AVV)
- Regular audits of processors

3. Data Integrity

Integrity Control

Protection of data from accidental or unauthorised modification. Ensures data completeness and immutability.

- Operation of an ISMS that ensures data integrity and is regularly updated.
- Prompt and documented response to security incidents by our CSIRT to trace and resolve integrity violations.
- Continuous monitoring of all data changes through a monitoring system.
- Comprehensive identity and access management that strictly regulates access to data.
- Regular penetration tests and an active bug bounty programme to test and enhance the robustness of our systems.
- OWASP Top 10-compliant secure software development training, ensuring the quality and security of our products.
- Effective contingency plans for integrity violations to ensure prompt resolution.

Availability Control

Ensures continuous accessibility and functionality of systems and data:

- Use of various security tools, such as malware scanners and web application security tools
- Redundant cloud operation of iomarket applications to ensure high availability
- Regular backups to ensure data availability and recoverability
- Fire and smoke detection systems
- Backup and recovery concepts

- Preparedness with an emergency response plan
- Server room with air conditioning

4. Organisational Measures (Art. 26 DSG)

Includes structures and processes within an organisation.

- Appropriate organisational structure for information security, integrated into organisation-wide processes and workflows: Organisational embedding of information security
- Consistent involvement of the ISO (Information Security Officer): Responsibility assignment and expert involvement
- Training of all personnel in information security and data protection: Knowledge transfer and awareness building
- Regular updates on data protection and IT security: Information and communication policy
- Our information security principles are firmly embedded in our business processes and are reinforced through regular training and competency testing of employees

5. Type and Purpose of Processing

As part of fulfilling the service contract, the processor gains access to the following categories of personal data:

Types of Personal Data

- Customer master data: first and last name, date of birth, address, nationality, etc.
- Customer's customer data
- Customer's data subjects
- Employee master data
- Address data: street, house number, postal code, city, country, etc.
- Meta and communication data (e.g., telephone, email)
- Delivery data: goods and quantities, delivery locations and times, recipients, etc.
- Billing data: customer invoices, supplier invoices, etc.
- Customer content data

Categories of Data Subjects

Personal data relates to the following groups of individuals:

- Customer data
- Supplier data
- Customer employees
- External employees of the customer
- Customer's end users

- Customer’s data subjects
- Customer’s service providers

Purpose of Data Processing

The nature of processing includes all types of processing within the meaning of the Swiss Federal Act on Data Protection (DSG). The "purposes" refer to the measures required for providing the agreed services.
Processing includes storing, retrieving, writing, and evaluating activity logs. Processing takes place exclusively in a protected user environment with appropriate access permissions. The processor is authorised to process personal data on its systems as required to fulfil its tasks.

The processing of personal data serves the following purpose:

- Automation of the creditor and debtor processes of the controller

The scope and purpose of processing are also defined in the service contract.
The parties expressly agree that the obligations regulated in this agreement regarding the handling of personal data apply at all times whenever and as long as the processor processes personal data of the controller.

Location of Data Processing

Processing takes place exclusively in Switzerland. The processor is prohibited from processing personal data outside Switzerland

Return and Deletion

Upon completion of the agreed services, the processor undertakes to either delete or return all personal data at the controller's discretion, unless data retention is required under data protection or other applicable law.
Deletion will take place within 30 days after the service provision ends.

6. Awareness and Training

Employee Training

Regular training and awareness-raising on data protection.
Examples:

- E-learning programmes
- In-person training on DSG-relevant topics

7. Continuous Improvement

Auditing and Review

Regular evaluation of the effectiveness of implemented measures.
Examples:

- Internal and external audits
- Data protection impact assessments

The applicable version will be published online on the website. Insofar as different language versions are available due to translated versions, the German version is relevant.