discover.swiss

Order processing contract

According to Art 9 of the Federal Act on Data Protection (FADP)

Cooperative discover.swiss
Schaffhauserstrasse 14
8042 Zurich
Switzerland

www.discover.swiss | legal@discover.swiss

Preamble

This Order Processing Agreement (hereinafter "OPA") specifies the obligations regarding data protection arising from the contractual relationship between the contractor, cooperative discover.swiss (hereinafter "Processor"), and its service users (hereinafter "Controller"). The contractual data processing is based on the contract for the provision of services by the Controller at discover.swiss according to the General and product-specific Terms and Conditions (hereinafter collectively referred to as "Terms") of discover.swiss. These Terms (https://www.discover.swiss/gtcs) and the Privacy Policy (hereinafter "PP", https://discover.swiss/en/privacy-policy)) of cooperative discover.swiss are thus an integral part of the OPA. The OPA applies to all activities resulting from the main contract for the provision of services between the parties, in which employees of discover.swiss or third parties commissioned by discover.swiss process personal data (hereinafter "Data") of the Controller. For any data protection-related queries, the Controller can contact the data protection officer of discover.swiss at legal@discover.swiss.

1 Subject, duration and specification of order processing

1.1 The subject matter and duration of the contract, as well as the nature and purpose of the processing, generally arise from the contractual relationship for the provision of services by the Controller at the Processor according to the Processor's Terms and Conditions.

1.2 Annex A to the OPA specifies the subject matter, nature, and purpose of the order processing by the Processor when accessing the Software-as-a-Service services.

2 Scope of application and responsibilities

2.1 The Processor processes personal data on behalf of the Controller. This includes activities specified in the Terms and Conditions, the Privacy Policy, Annex A of the OPA, and in the current service description on the Processor's website.

2.2 Within the framework of the contractual relationship, the Controller is solely responsible for compliance with the statutory provisions of data protection laws, for the lawfulness of data transfer to the Processor and for the lawfulness of data processing.

2.3 Upon activation of the Processor's services for the Controller, the Controller provides the Processor with the corresponding instructions for data processing. Thereafter, the Controller may supplement, amend, or withdraw their instructions in written form or in an electronic format ("text form") to the designated contact specified by the Processor. Instructions not provided for in the Terms and Conditions shall be treated as requests for a change in services. Oral instructions must be promptly confirmed in writing or in text form by the Controller.

3 Obligations of the Processor

3.1 The Processor processes data of data subjects only within the scope of the contractual relationship in accordance with the GTC, the Privacy Policy and these OPA, unless there is a legally regulated exception.

3.2 The Processor shall establish the internal organisation within its area of responsibility in a manner that it meets the special requirements of data protection. It shall implement technical and organizational measures to ensure the adequate protection of the Controller's data, which comply with the respective legal requirements of data protection laws. These measures ensure the confidentiality, integrity, availability, and resilience of the systems and services associated with the processing on a continuous basis. The Controller is aware of these technical and organizational measures and is responsible for ensuring that they provide an appropriate level of protection for the risks associated with the data being processed. Any changes to the security measures implemented are at the discretion of the Processor, provided that the contractually agreed-upon level of protection is not undermined.

3.3 The measures taken by the Processor are specified in Annex B. The technical and organizational measures (TOMs) are subject to technological progress and further development. In this respect, the Processor is permitted to implement alternative appropriate measures at any time. However, the agreed-upon level of security established in this OPA must not be compromised.

3.4 As agreed upon, the Processor supports the Controller to the extent possible in fulfilling the requests and claims of data subjects in accordance with Chapters 3 and 5 of the Federal Data Protection Act FDPA ("Rights of Data Subjects") as well as in compliance with the obligations stated in Article 22 ("Data Protection Impact Assessment") and Article 24 ("Notification of Personal Data Breaches") of the FDPA. Unless otherwise agreed, the Processor may request appropriate compensation for this.

3.5 Employees involved in the processing of the Controller's data, as well as other third parties working for the Processor, shall process the data exclusively within the scope of the contractual relationship in accordance with the Terms and Conditions, the Privacy Policy, and this present OPA, and are obligated to maintain confidentiality.

3.6 If the Processor becomes aware of a breach of the protection of personal data, it shall take reasonable measures to secure the data and mitigate any potential adverse consequences for the data subjects. Additionally, the Processor fully complies with the applicable legal provisions regarding the notification of data breaches to the Controller.

3.7 The Processor fully complies with the applicable data protection regulations and regularly evaluates the effectiveness of the technical and organizational measures to ensure the security of the processing.

3.8 The Processor processes and stores personal data for the duration of the contractual relationship between the Processor and the Controller. The Processor corrects or deletes the data subject to the Controller's instructions and within the scope of the instruction framework. This excludes data required for further processing due to legal requirements or mandatory internal purposes. The release of data and the corresponding compensation are regulated in the Terms and Conditions.

3.9 The Processor does not guarantee the storage or provision of data and is particularly entitled to delete data independently of statutory retention obligations.

4 Obligations of the Controller

4.1 The Controller shall promptly and fully inform the Processor in writing or by email if they detect errors or irregularities concerning data protection regulations in the results of the contract.

4.2 The Controller shall provide the Processor with the contact person for data protection issues arising within the framework of the contractual relationship, provided that this differs from the contact person mentioned in the main contract.

4.3 The Controller declares that they bear sole responsibility for informing the data subjects regarding the possible storage, use, processing, and disclosure of data by the Processor in accordance with the provisions of the Terms and Conditions, the Privacy Policy, and this OPA. If individual data subjects do not consent to the intended data processing, the Controller is responsible for deleting the respective data accordingly.

5 Enquiries from affected persons

5.1 If an affected person makes claims for rectification, deletion, or information to the Processor, the Processor will refer the affected person to the Controller, if the affected person's identity can be determined. The Processor will forward the affected person's request to the Controller within a reasonable period. The Processor may assist the Controller in addressing data protection claims of an affected person to the extent possible. In this case, the Processor is entitled to reimbursement of expenses. The Processor shall not be liable if the Controller fails to respond to the affected person's request, or if the response is incorrect or not timely.

6 Verification Options

6.1 The Processor shall demonstrate compliance with the obligations laid down in this OPA by appropriate means to the Controller. Unless otherwise agreed, the Controller and Processor agree that proof shall be provided by submitting a list of the "technical and organizational measures" taken pursuant to Article 3 of the Swiss Data Protection Act (DPA).

6.2 If inspections by the Controller or an auditor appointed by the Controller are necessary in individual cases (e.g., due to GDPR compliance), they shall be conducted during regular business hours without disrupting operations, subject to prior notification and a reasonable lead time. The Processor may require prior notification with a reasonable lead time and the signing of a confidentiality agreement regarding the data of other customers and the implemented technical and organizational measures. If the auditor appointed by the Controller is in a competitive relationship with the Controller, the Processor may refuse and propose a neutral person. The Processor may invoice the Controller for any costs associated with the audit, especially if no irregularities are found.

6.3 If a data protection authority or other governmental supervisory authority of the Controller conducts an inspection, the provisions of Clause 6.2 shall generally apply. Signing a confidentiality agreement is not required if this supervisory authority is subject to professional or legal confidentiality obligations punishable under criminal law for violations.

7 Subcontractors (Other Processors)

7.1 The Processor may engage subcontractors to fulfill the contractual services. The engagement of subcontractors as data processors by the Processor is permissible, provided that they meet the requirements of this OPA to the extent of the subcontract. The Processor shall enter into

agreements with subcontractors to ensure appropriate data protection and information security measures to the extent necessary. Subcontractors who do not have access to customer data or do not process personal data as data processors are exempt from this chapter. A list of current subcontractors as data processors (hereinafter simply referred to as "subcontractors") is attached to this document as Appendix 3.

7.2 The Controller agrees that the Processor may engage subcontractors listed on the Processor's website. Before engaging additional subcontractors, the Controller informs the Controller by updating its website. The overview on the website must be updated at least 14 days before engagement. The Controller will regularly check the overview. The Controller may object to the change within 14 days of publication on the website for good reason. If no objection is made within the deadline, consent to the change is deemed to have been given. In the event of a significant data protection reason, and if an amicable solution cannot be found between the parties, the Processor shall be granted a special termination right.

8 Information Obligations

If the Controller's data at the Processor is threatened by seizure or confiscation, insolvency or composition proceedings, or other events or measures by third parties, the Processor shall immediately inform the Controller thereof. The Processor shall promptly inform all parties involved in this matter that ownership and control of the data exclusively belong to the Controller.

9 Liability

Liability is governed by the respective provisions in the Terms and Conditions.

10 Final Provisions

10.1 The provisions of the Terms and Conditions and the Privacy Policy shall apply in all other respects. In the event of any inconsistencies between this OPA and the Terms and Conditions, the provisions of the Terms and Conditions shall prevail.

10.2 discover.swiss reserves the right to amend or change these OPA at a later date. Changes will be exclusively announced on the URL under which these OPA is stored at the relevant time. It is the responsibility of the Platform User to check this page regularly for changes. The changes will become part of the contract unless the Platform User objects within 14 days of notification of the change. Your continued use of the product after expiry of the aforementioned period constitutes your acceptance of the changes to the GTC.

10.3 The contractual relationship is subject to Swiss law, to the exclusion of the Vienna Sales Convention. The courts of Zurich shall have exclusive jurisdiction for all legal disputes arising from the contract.

10.4 Should any provision of these OPA be or become invalid or void, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by an appropriate provision that comes as close as possible to what the contracting parties intended or to the meaning and purpose of this contract.10.3 Annexes A and B are part of this OPA.

10.5 In case of discrepancies or interpretation issues between the German and the English version of this GTC, the German version shall prevail.

APPENDIX 1 - SUBJECT MATTER, NATURE AND PURPOSE

A. Object of the order

Processing of personal data of the Controller in the context of its use of the Processor's services as software-as-a-service in connection with the use of the platform.

B. Nature and purpose of the intended processing

The personal data processed by the Controller is transferred to the Processor as part of the Software-as-a-Service services for the purpose of providing and authorising the use of the Software-as-a-Service services by discover.swiss in accordance with the contract. This includes the following processing in connection with the creation of a user account:

- "Creation of user account"
- "Login user account"
- "Forgotten user account password"
- "Change user account password"

via Microsoft Azure B2C or via social logins. The subject of this processing, the legal basis of which is the processing of the contractual relationship, are the following data types: e-mail, password, surname, first name, display name, user name.

The following processing operations are associated with the use of the user account:

- User account management"
- "Profile data management support portal"
- "Platform API profile data management"
- "Customer Service B2C"

The subject of the processing, the legal basis of which is the processing of the contractual relationship, are the data types salutation, e-mail, password, surname, first name, mobile phone, street, postcode, city, country, nationality, passport number, nickname, correspondence language, contact details, order history, travel group information, display name, user name.

The following processing operations are associated with the use of the Marketplace service (shopping basket and payment processing):

- Processing of orders entered in the Controller's application, including payment transactions

The subject of the processing, the legal basis of which is the processing of the contractual relationship, is the surname, first name, date of birth, product, means of payment, validity, and price. The personal data processed via the platform will only be passed on to the service providers and, if necessary, to the service providers. Payment is made directly via the payment service provider. The Controller is responsible for processing the data recorded on its application as long as it is not transmitted to discover.swiss via the interface. "Behind" the interface or for the data transmitted via API calls, discover.swiss is responsible.

Depending on the subscription model selected, individual aforementioned data processing operations may be omitted and/or additional ones may be added. The details of the respective data processing are recorded in the API documentation in the developer portal (https://developer.discover.swiss/apis).

C. Categories of data subjects:

The categories of data subjects depend on the data transmitted by the Controller. These are (depending on the order):

- Employees (including applicants and former employees) of the Controller
- Customers of the Controller
- Interested parties of the Controller
- Service provider of the Controller
- Contact details for contact persons

D. Deletion, blocking and correction of data

Requests for deletion, blocking and correction must be addressed to the Controller; otherwise, the provisions of the GTC, the DSE and these GTC apply.

APPENDIX 2 - TECHNICAL AND ORGANISATIONAL MEASURES (TOMS)

The following measures are fundamental for data processing.

A. System and data security in general

Measures to ensure the comprehensive security of the systems used and the correct handling of data security breaches:

- Regular installation of system and software updates
- Process for recognising security vulnerabilities (vulnerability management)
- Process for eliminating critical vulnerabilities (patch management)

B. Access control

Measures to prevent unauthorised persons from gaining access to data processing systems with which personal data is processed or used:

- Data is stored in the Azure Cloud in Europe. The physical access controls are guaranteed by Microsoft Inc.

C. Access control

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

- Assignment of user rights
- Minimum requirements for password complexity and forced password change
- Authentication with user name / password
- Use of user profiles
- Additional measures: Web application firewalls, regular vulnerability scans, regular penetration testing, patch management, use of virus scanners.
- Assignment of user profiles to IT systems

D. Access control

Measures that ensure that persons authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage:

- Creation of an authorisation concept (Identity Access Management)
- Number of administrators reduced to the "absolute minimum"
- Logging of application access, in particular for input, modification and data deletion
- Rights management by system administrators
- Blocking access rights for personnel changes
- Password policy with specifications on password length, password change management
- Secure storage of data carriers

E. Disclosure control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data carriers and that it is possible to verify and establish to which bodies the transmission of personal data by data transmission equipment is intended:

- TLS encryption for all communication (web Controller, APIs, mobile apps)

F. Input control

Measures that ensure that it is possible to subsequently check whether and by whom personal data can be entered, changed or removed in data processing systems:

- Logging the entry, modification, and deletion of data
- Traceability of the entry, modification, and deletion of data by individual users (not user groups)
- Assignment of rights for entering, modifying and deleting data based on an authorisation concept
- Creation of an overview of the authorised applications for entering, modifying, or deleting data
- Storage of forms used to collect data by means of automated processing

G. Availability control

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

- Creation of backup & recovery concepts
- Creating data backups
- Testing the data recovery

H. Commandment of separation

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

- Creation of an authorisation concept
- Data records with purpose attribute / data fields
- Authorised and documented database rights
- Logical Controller separation (at software level)
- Separation of productive and test systems

APPENDIX 3 – SUBCONTRACTORS (OTHER PROCESSORS)

In addition to Section 7, Clause 7.1 of this order processing contract, the subcontractors who may be called in by the Contractor to fulfil the contractual service are listed here.

Name	Adress	Processing purpose
MOBIDEV	3855 Holcomb Bridge Rd. Suite 300, Norcross, GA 30092, USA	MOBIDEV development team from Ukraine. Can see the data during implementation. However, no data is stored or processed on the MOBIDEV systems.