Burkhalter Management AG
Hohlstrasse 475, 8048 Zürich
+41 44 432 47 77
www.burkhalter.ch, info@burkhalter.ch

ORDER PROCESSING CONTRACT (OPC)
(Agreement)

between

Customer of the "Declaration of consent regarding the Order Processing Contract"

Controller (Client)

and

Burkhalter Management AG
Hohlstrasse 475, 8048 Zürich as the

Processor (Contractor)

Controller and Data Processor individually **Party** and collectively **Parties**

regarding

Order processing in accordance with Swiss law

1 Purpose

(a) A legal relationship exists between the Parties for the performance of which personal data is transferred from the Controller to the Processor. This Agreement is concluded between the Parties in order to ensure adequate protection when transferring personal data. In the event of any contradictions between this Agreement and other contracts, this Agreement shall take precedence if and insofar as it is connected with the Contractor's processing of personal data under the existing Contract.

1.1 Definitions

(a) Unless otherwise stipulated in this Agreement, all terms shall have the same meaning as in the Swiss Federal Data Protection Act ("**FADP**") of 19 June 1992 and 20 September 2020, once the latter is in force. Any reference to the FADP should always include a reference to the current Ordinance to the FADP ("**OFADP**") and also to any other legal provision of the underlying Swiss data protection law.

(b) This Agreement also supports the Parties in complying with Ordinance (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("EU GDPR"). References to the EU GDPR are only relevant for those data processing operations to which the EU GDPR applies. If references to the EU GDPR lead to a contradiction to Swiss data protection law, the latter shall take precedence.

1.2 Description of data processing

(a) The personal data covered by this order processing and the purposes of the processing are described in Appendix 1 to this Agreement. Appendix 1 forms an integral part of this Agreement and may be amended unilaterally by the Controller from time to time.

2 Responsibilities of the Controller

(a) The Controller shall ensure:

(1) that the transfer of personal data and the processing of such data by the Processor as set out in this Agreement are permissible under applicable law and the Controller ensures that the transfer to the Contractor is carried out in accordance with applicable law; and

(2) that no other statutory provision prohibits the transfer of data processing.

(b) The Controller has verified that the technical and organisational measures implemented by the Processor, described in Appendix 2, are sufficient to ensure adequate data protection for the transferred personal data.

3 Responsibilities of the Processor

3.1 General

(a) With regard to the processing of personal data in accordance with Appendix 1, the Processor ensures that it

(1) will process such personal data in accordance with this Agreement and solely for the purposes pursued by the Controller;

(2) The purposes pursued by the Controller are set out in Appendix 1 or in the Controller's explicit instructions or are defined in another agreement with the Controller.

(3) will provide the Controller with the information necessary to monitor compliance with the obligations set out in this Agreement;

(4) will take into account the principles of data privacy by design and by default in its work equipment, products, applications and services;

(5) will inform the Controller if it is no longer able or is likely to no longer be able to comply with this Agreement;

(6) will inform the Controller of the contact address for data protection requests and communicate any changes in this regard on its own initiative;

(7) will adequately support the Controller in data protection impact assessments (in particular pursuant to Article 35 of the EU GDPR) or prior consultations (in particular pursuant to Article 36 of the EU GDPR), and

(8) will cooperate with the relevant supervisory authorities to the extent permitted by law.

(b) Persons authorised by the Controller to issue instructions shall be notified to the Processor in text form at the start of order processing. In the event of a change or long-term absence of the contact person, the Contractor must be notified of the successor or representative in writing without delay. Verbal instructions are only binding with immediate written confirmation from the Controller. Email is sufficient for compliance with the written form.

(c) The Contractor must inform the Client without delay if it believes that an instruction violates statutory provisions. The Contractor is entitled to suspend the execution of the corresponding instruction until its legality is confirmed by the Controller or the instruction is amended.

3.2 Data security

(a) For the duration of this Agreement, the Processor shall implement appropriate technical and organisational measures as required by the Data Protection Act (FADP) and Article 32 of the EU

GDPR. In so doing, the Processor has taken into account the state of the art, the implementation costs and the nature, scope and purposes of the processing, as well as the probability of occurrence and severity of the risk to the fundamental and personal rights of the data subjects. The measures are described in Appendix 2 and are reviewed periodically. Changes to the measures are permitted provided that the current level of security is not lowered.

(b) The Processor will

(1) only use employees who are contractually or legally bound to confidentiality and who have been made familiar with the data protection provisions relevant to them in advance,

(2) inform and cooperate with the Controller without delay if the Controller believes that it might no longer be able to or is no longer able to comply with this Agreement and, in particular, the data security obligations;

(3) support the Controller with appropriate measures in ensuring a level of data protection appropriate to the risk,

(4) report and document a data security breach (including unauthorised access to personal data in accordance with Appendix 1) to the Controller without delay, so that the Controller can report the breach to a supervisory authority (in particular pursuant to Article 33 of the EU GDPR) or to the data subjects (in particular pursuant to Article 34 of the EU GDPR) within 72 hours. The report shall include at least i) the type of data security breach, ii) the consequences of the breach (in particular for data pursuant to Appendix 1), iii) the measures taken and iv) planned measures.

(c) The Contractor shall make data security reports available to the Controller upon legitimate request. The Controller also has the right to check compliance with the agreed data security at its own expense or to have it checked by a third party that is bound to secrecy. Checks must be reported in good time and agreed with the Contractor.

3.3 Subcontractors

(a) The Processor shall not transfer data processing to subcontractors without the prior consent of the Controller. The Controller may not unreasonably withhold consent. If the Controller consents to a subcontractor, this shall not in any way release the Contractor from its responsibility for outsourced data processing.

(b) The Processor is obliged to conclude agreements with subcontractors that ensure at least a level of data protection equivalent to this Agreement.

(c) As a rule, ancillary services for the Contractor that do not relate to the Controller's data pursuant to Appendix 1 (e.g. telecommunications services, postal/transport services, maintenance and user services or the disposal of data storage media as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software) are not considered to be subcontracting. However, the Contractor is obliged to take appropriate control measures to ensure the data protection and data security of the Client's data, including where ancillary services are concerned.

3.4 Disclosure abroad

(a) The processing of data in accordance with Appendix 1 generally takes place in Switzerland or a member state of the European Union or in another contracting member state party to the Agreement on the European Economic Area. Any relocation to another third country may only take place if the corresponding statutory requirements (Art. 6 FADP or Art. 16 et seq. FADP of 20 September 2020; Art. 44 et seq. EU GDPR) are met.

(b) If the Processor employs subcontractors in countries that do not have an adequate level of data

protection according to the Federal Data Protection and Information Commissioner, the Appendix to the OFADP or the EU Commission, the Processor shall ensure that the disclosure is permissible under data protection law by means of measures appropriate to the respective data transfer. This is usually performed by the Processor agreeing with these subcontractors the standard contractual clauses in accordance with the EU Commission implementing decision (EU) 2021/914 ("modernised standard contractual clauses"). Here, the Contractor shall agree on the correct module (generally Module 3) of the modernised standard contractual clauses and, in particular, make the following adaptations for the processing of data subject to Swiss data protection law:

(1) references to the EU GDPR are to be understood as references to the Swiss FADP,

(2) the Federal Data Protection and Information Commissioner is designated as the supervisory authority,

(3) the place of residence and jurisdiction of data subjects resident in Switzerland should not be ruled out and

(4) until the FADP comes into force on 20 September 2020, the term "personal data" also includes data relating to legal entities.

(c) For the existing cooperation with subcontractors in countries without an adequate level of data protection, which is still based on the standard contractual clauses enacted under Directive 95/46/EC, the modernised standard contractual clauses or another appropriate guarantee will be agreed by 27 December 2022.

4 Rights of data subjects

(a) The Controller is responsible for ensuring that data subjects receive the information to which they are entitled with regard to their right to information (right of access), data disclosure and transmission, rectification, blocking, suppression or erasure pursuant to the FADP or Chapter III of the EU GDPR. The Processor shall:

(1) forward to the Controller any queries relating to data in accordance with Appendix 1 without responding to them themselves,

(2) cooperate with the Controller and provide the necessary support services so that the Controller can fulfil the rights of data subjects in accordance with the FADP or Chapter III of the GDPR; and

(3) respond fully and truthfully to the Controller's enquiries regarding the rights of data subjects within 15 working days or explain within this period why it takes longer to respond. However, under no circumstances may the delay result in the Controller being unable to fulfil its obligations.

5 Duration and termination

(a) Unless otherwise agreed in writing, this Agreement shall automatically end upon termination of the Principal Contract or cancellation of the "Declaration of consent regarding the Order Processing Contract". However, the provisions of this Agreement shall outlast the termination of the Principal Contract and shall remain in force for as long as the Contractor has possession of the personal data.

(b) The Controller is entitled at any time to terminate this Agreement for good cause without notice if the Processor fails to remedy the cause within a reasonable period of time despite a reminder. Good cause shall be deemed to exist if the Contractor

(1) seriously breaches its obligations under this Agreement,

(2) violates provisions of the Swiss Data Protection Act or the EU GDPR intentionally or through

gross negligence, or

(3) does not carry out the Controller's instructions.

(c) Upon termination of this Agreement, for any reason, the Processor shall:

(1) destroy or irretrievably delete any personal data and copies thereof transferred under this Agreement, arrange for subcontractors to destroy or delete it, and confirm to the Controller that this has been carried out;

(2) or, at the discretion of the Controller, immediately return any personal data transferred under this Agreement and arrange for subcontractors to return it,

(d) If the law to which the Processor is subject prohibits it from returning or destroying the personal data or parts thereof, the Processor shall inform the Controller of this, shall treat such personal data confidentially and shall not actively process it.

6 Miscellaneous

6.1 Supplements

(a) Amendments, supplements or revocation of provisions in this Agreement must be made in writing in order to be valid. Any amendment to this obligation must be agreed in writing in order to be valid. Changes of address must be communicated to the other Party without delay in the manner agreed above.

6.2 Processing record

(a) Each Party is responsible for maintaining a record of data processing unless a statutory exception exists.

6.3 Costs

(a) The costs associated with the execution of this Agreement and the fulfilment of the obligations set forth therein shall be included in the compensation agreed between the Parties in the Principal Contract.

6.4 Liability

(a) If the Contractor's grossly negligent or intentional non-compliance with this Agreement results in damage to the Controller or third-party claims against the Controller, the Contractor shall indemnify the Controller.

6.5 Severability clause

(a) Should any provision of this Agreement be unenforceable or invalid, it shall only lapse to the extent of its unenforceability or invalidity and shall otherwise be replaced by a valid and enforceable provision that corresponds as closely as possible to the legal and economic significance of the invalid provision. The remaining provisions of this Contract shall remain binding and in force.

6.6 Assignment prohibition

(a) The admissibility of the assignment of rights and obligations arising from this Agreement shall be assessed in accordance with the rules of the Principal Contract. If there is no provision in the Principal Contract, the Parties shall be prohibited from assigning or transferring this Contract or rights and obligations under this Contract to third parties in whole or in part without the prior written consent of the other Party and any assignment or transfer without the prior written consent shall be null and void.

6.7 Applicable law

(a) This Agreement is subject to substantive Swiss law, to the exclusion of the provisions of the conflict of laws and the Vienna Convention on Contracts for the International Sale of Goods.

6.8 Place of jurisdiction

(a) The ordinary courts at the registered office of the Controller shall have exclusive jurisdiction over all disputes arising from or in connection with this Agreement.

Appendix 1

Purpose of processing	The purpose of the processing of personal data by the Processor is to provide the maintenance and support services for the Controller described in the Principal Contract.
Duration of processing	Personal data will only be processed for the term of the Principal Contract or for the duration of the "Declaration of consent regarding the Order Processing Contract".
Categories of data subjects	Employees, customers and partners.
Categories of personal data	Name, email, telephone number, address, date of birth, occupation or other information and statements relating to a specific person or person that can be identified using the information.
Place of storage and processing	To the business address of the Controller and its approved sub-processors.
On-site inspections	No
Sub-data processor	Sub-data processors approved to provide the maintenance and support services for the Controller described in the Principal Contract.
Transfer outside the EU/EEA Switzerland	Not allowed.
Specific instructions or other special provisions	No further.

Appendix 2: Technical and organisational measures

Description of the technical and organisational security measures implemented by the Processor(s):

1 Organisational security measures

1.1 Security management

(a) Security concept and procedure: The Processor must have a documented security concept for processing personal data.

(b) Roles and responsibilities:

(1) Roles and responsibilities related to the processing of personal data are clearly defined and assigned in accordance with the security concept.

(2) In the case of internal restructuring or redundancies and when changing jobs, the revocation of rights and responsibilities is clearly defined with corresponding transfer procedures.

(c) Access control policy: Each role involved in the processing of personal data is assigned specific access control rights in accordance with the need-to-know principle.

(d) Management of resources/assets: The Processor shall maintain a register of the IT resources (hardware, software and network) used to process personal data. One specific person is responsible for maintaining and updating the register.

(e) Change management: The Processor must ensure that all changes to the IT system are registered and monitored by a specific person (such as the IT or security officer). This process is monitored on a regular basis**.**

1.2 Incident response and business continuity

(a) Handling incidents/breaches of personal data:

(1) An incident response plan with detailed procedures shall be established to ensure an effective and proper response to incidents involving personal data.

(2) The Processor shall promptly report to the Controller any security incident that has resulted in the loss, misuse or unauthorised access to the Controller's personal data.

(b) Business continuity: The Processor has defined the key procedures and controls to be followed to ensure the necessary level of continuity and availability of the IT system for processing personal data (in the event of an incident/a violation of the protection of personal data).

1.3 Human resources

(a) Confidentiality of staff: The Processor shall ensure that all employees are aware of their responsibilities and obligations in connection with the processing of personal data. Roles and responsibilities will be clearly communicated during the process prior to recruitment and/or during induction.

(b) Training: The Processor must ensure that all employees are adequately informed about the security controls of the IT system that relate to their day-to-day work. The employees involved in processing personal data will also be appropriately informed about the relevant data protection requirements and legal obligations through regular awareness-raising campaigns.

2 Technical security measures

2.1 Access control and authentication

(a) An access control system applicable to all users accessing the IT system has been introduced. The system enables user accounts to be created, approved, reviewed and deleted.

(b) The use of shared user accounts is avoided. In cases where this is necessary, it shall be ensured that all users of the shared account have the same roles and responsibilities.

(c) When granting access or assigning user roles, the “need to know” principle shall be observed in order to limit the number of users who have access to personal data to those who need such access to fulfil the processing purposes of the Processor.

(d) If the authentication mechanisms are password-based, the Processor will require the password to be at least eight characters long and comply with very strict password control parameters, including length, character complexity and non-repeatability.

(e) Authentication data (such as user ID and password) must never be transmitted unprotected over the network.

(f) The authentication data and access controls to the Controller’s systems are beyond the control of the Processor.

2.2 Logging and monitoring:

(a) Log files are enabled for each system/application used to process personal data. They include all types of access to data (displaying, changing, deletion).

(b) Authentication/access is logged by the Controller.

2.3 Data security in standby mode

(a) Server/database security

(1) Database and application servers are configured to run under a separate account with minimum operating system privileges to function correctly.

(2) Database and application servers only process personal data for which processing is actually necessary to achieve the processing purpose.

(3) The security of the productive servers and databases is guaranteed by the Controller and is beyond the control of the Processor.

(b) Safety in the workplace:

(1) Users cannot deactivate or circumvent security settings.

(2) The anti-virus applications and recognition signatures are configured regularly.

(3) Users are not authorised to install or deactivate unauthorised software applications.

(4) The system will time out sessions if the user has been inactive for a certain period of time.

(5) Critical security updates published by the developer of the operating system are installed on a regular basis.

2.4 Network/communication security:

(a) Every time the Internet is accessed, communication is encrypted using cryptographic protocols.

(b) Traffic to and from the IT system is monitored and controlled by firewalls and intrusion detection

systems.

2.5 Backups:

(a) Backup and data recovery procedures will be defined, documented and clearly linked to roles and responsibilities.

(b) Backups will be adequately protected both physically and ecologically in accordance with the standards that apply to the original data.

(c) Backup execution is monitored for completeness.

(d) The backup strategy of the systems will be determined by the Controller and is beyond the control of the Processor.

2.6 Mobile/portable devices:

(a) Procedures for managing mobile and portable equipment are to be established and documented with clear rules for their proper use.

(b) Mobile devices that are allowed to access the information system will be registered and authorised in advance.

(c) Management and authentication/access via mobile devices will be ensured by the Controller.

2.7 Application life cycle security

During the development cycle, best practices, state-of-the-art technology and recognised safe development procedures or standards will be followed.

2.8 Deletion/disposal of data:

(a) The data carriers will be overwritten with software before they are disposed of. If this is not possible (CDs, DVDs, etc.), they will be physically destroyed.

(b) Paper and portable data carriers on which personal data is stored will be destroyed.

2.9 Physical security:

(a) The physical environment of the IT system infrastructure is not accessible to unauthorised personnel. Appropriate technical measures (such as intrusion detection system, chip card-controlled turnstile, one-person security access system, locking system) or organisational measures (such as security duty) must be used to protect the security areas and their entrances against unauthorised entry.

(b) The physical security of the IT system infrastructure will be ensured by the Controller and is beyond the control of the Processor.