

Data Processing Agreement (DPA)

Version: April 2026

1. Subject of the contract

- (a) Scope: This data processing agreement (**DPA**) supplements the service agreement between the customer (**Controller**) and the service provider (**Processor**), insofar as a service agreement including applicable general terms and conditions (the **Agreement**) refers to this DPA and the Processor processes personal data of the Controller (the **Processing Data**) in performance of the Agreement and subject to a separately concluded data processing agreement for the relevant services. The Processor is a company of the BKW Group; a directory of the group members can be viewed at <https://www.bkw.ch/en/about-us/the-bkw-group/our-network-of-companies>.
- (b) The DPA applies between the Processor and, on the other hand, the Controller and, if applicable, all other companies affiliated with the Controller in a group that are entitled to receive services under the Agreement, in the provision of which the Processor processes Processing Data. To the extent that the Controller in turn acts as a processor of another controller, the Processor acts as a sub-processor. In this case, the provisions of this DPA apply as a sub-processing agreement, and the Controller assures that the instructions issued by it correspond to the instructions of the controller.
- (c) Subject matter: In this DPA, the parties regulate the requirements applicable to the Processor in connection with the processing of the Processing Data by the Processor. The duration of the processing, its nature and purpose, the categories of data processed, and the categories of data subjects are set out in the Agreement. In the event of a conflict between the Agreement and this DPA, subject to clause 8, the stricter provisions for the protection of personal data shall prevail.
- (d) Definitions: Terms in bold are used in this DPA with the meaning assigned to them. Legal terms such as "personal data," "processing," "personal data breach," etc. have the meaning defined in applicable data protection law. **Applicable data protection law** means the Swiss Federal Act on Data Protection (**FADP**) and the corresponding ordinance, the General Data Protection Regulation (**GDPR**), and other data protection regulations, in each case to the extent they apply to the processing of Processing Data. References in this DPA to provisions of the FADP or the GDPR are to be read as references to corresponding provisions of the applicable data protection law in each case.
- (e) Term: This DPA takes effect upon conclusion of the Agreement, but no later than upon the Processor's first access to Processing Data, and ends upon termination of the Agreement, but no earlier than deletion of all Processing Data processed by the Processor.

2. General obligations of the Contractor

- (a) Compliance with instructions:
- (i) The Contractor is obliged to process order data exclusively for the performance of the contract, this DPA, and the Controller's instructions. Reserved are any deviating obligations under applicable mandatory law, about which the Controller must be informed in advance to the extent permitted.

- (ii) Instructions regarding the processing of personal data by the Contractor are binding insofar as they do not expand the contractual obligations. As a rule, they are issued through direct interaction with the Contractor's systems (where technically possible) or in text form; in urgent cases, they may also be given orally. The Controller is obliged to document instructions appropriately.
- (b) Personnel: The Contractor shall take appropriate measures to ensure that its employees and engaged third parties who may have access to order data processed for the provision of the services are reliable, trustworthy, and adequately trained for the tasks assigned to them in the secure handling of data, and that they process the order data exclusively in accordance with the provisions of this DPA.
- (c) Place of data processing: Data processing shall be carried out exclusively at the Contractor's locations, subject to outsourcing to engaged subcontractors in accordance with the provisions of section 6. If the Contractor intends to transfer personal data to a country that does not provide an adequate level of protection under the applicable data protection law, it shall conclude an agreement for this data transfer that permits the transfer under the applicable data protection law.
- (d) Return and deletion obligation:
 - (i) If the Contractor no longer requires order data to fulfil its obligations to the Controller, it shall ensure that the relevant order data is returned to the Controller and/or that any remaining copies are deleted. Upon termination of the DPA, the Controller shall issue corresponding instructions to the Contractor.
 - (ii) Reserved in each case is longer storage in customary backup systems until the next regular deletion, provided that these systems are secured at least in accordance with the requirements of this DPA and the stored order data is used exclusively for backup purposes.

3. General obligations of the client

- (a) Responsibility for the lawfulness of data processing lies with the client.
- (b) The client warrants the lawfulness of transferring the data processing to the contractor and of its corresponding processing. In the case of special requirements for processing (such as increased security needs), the contractor must be informed accordingly.

4. Data and Information Security

4.1. General Duties

- (a) The Contractor undertakes to implement appropriate technical and organizational measures to protect the order data processed for the provision of the service against impermissible processing, but at a minimum the measures set out in Annex 1 "Technical and organizational measures" (the **TOM**).
- (b) The Client confirms the appropriateness of the TOM, taking into account the need for protection of the order data as assessed by it. The Contractor may adjust the TOM at any time. Changes that impair the security level of the order data must be communicated to the Client in text form in advance. The

Client may object to such changes within a period of two weeks.

4.2. Maintaining confidentiality

- (a) All order data must be treated as confidential. The Contractor undertakes to:
- (i) protect the order data appropriately against access by unauthorized persons;
 - (ii) ensure that all persons with access to the confidential information are subject to an appropriate statutory or contractual confidentiality obligation; and
 - (iii) grant access to confidential information only to persons who require it for the performance of their duties, whereby access and authorization are to be limited to the extent objectively and personally necessary for business purposes (compliance with the "need-to-know" principle).
- (b) The Contractor is obliged to inform the Client without undue delay of requests or orders from authorities (e.g. judicial, criminal prosecution, and administrative authorities), insofar as this is permissible under applicable law. It shall refer the requesting authority to the Client in each case. Subject to any contrary instructions from the Client, it shall, at the Client's expense, take the legal remedies available under applicable law that are not obviously futile in order to prevent or restrict disclosure of order data. If it is legally obliged to disclose, it shall disclose only the minimum amount of order data.

4.3. Notification of data security breaches

- (a) The Contractor shall notify the Client in the event of a data security breach without undue delay and no later than within 48 hours after the Contractor becomes aware of the data security breach.
- (b) The notification to the client contains at least the following information (which must be provided in stages insofar as it is not yet fully known at the time of notification):
- (i) Type of data security breach;
 - (ii) affected persons (category and approximate number of affected persons);
 - (iii) type and scope of the client's personal data affected by the data security breach (categories and approximate number of affected data records);
 - (iv) contact person of the client from whom additional information can be obtained;
 - (v) expected consequences of the data security breach for the affected persons;
 - (vi) measures taken or planned to investigate and address the data security breach.

5. Subcontractor

- (a) Permissibility: The Contractor is authorized to engage subcontractors, provided they are engaged in accordance with the Agreement and this DPA and the Contractor has concluded with them an agreement in text form that imposes on the subcontractor essentially the same obligations to which the Contractor is subject under this DPA. When engaging subcontractors from third countries, Section 2(c) shall apply. The Contractor shall be liable to the Client for compliance with the obligations of the

subcontractors as for its own conduct.

(b) Approval:

- (i) If the Contractor intends to engage an additional sub-processor, this must be notified to the Client as early as possible by express notice in text form. If the Client objects to the engagement of the sub-processor by notice in text form within 20 days of receipt of the corresponding notice and the Contractor is not prepared to refrain from engaging the respective sub-processor, each party shall have the right to terminate the Agreement and this DPA extraordinarily.
- (ii) The following shall be deemed sub-processors approved hereby: (i) any sub-service providers provided for in the Agreement, if applicable, (ii) the subcontractors notified to the Client in text form before conclusion of the Agreement, and (iii) the companies of the BKW Group.

6. Data protection control rights

- (a) In cases of urgency or suspicion of a breach, the Client is entitled to review and inspect the processing of commissioned data transferred to the Contractor with regard to compliance with the applicable data protection regulations. This also includes reviewing the security of the IT infrastructure provided for services.
- (b) In the context of such audits, the principle of proportionality must be observed and the Contractor's legitimate interests worthy of protection (in particular confidentiality) must be appropriately taken into account. Subject to any differing arrangement, the Customer shall bear all costs of such audits (including the Contractor's proven internal costs incurred in assisting with the audit).
- (c) Any audit rights defined in the contract as well as any legally mandatory inspection rights of the Client or its supervisory authorities remain reserved.

7. Further support obligations

- (a) The Contractor shall reasonably assist the Client in complying with its obligations to ensure appropriate data security, to report data breaches, and to carry out data protection impact assessments.
- (b) If a data subject contacts the Contractor in connection with data protection claims (e.g. with a request for access or deletion), the Contractor shall promptly forward the relevant request to the Client. It shall not respond to such requests. It shall reasonably assist the Client in handling such requests, as well as in fulfilling obligations to cooperate with authorities.

8. Transfer abroad

- (a) To the extent that the permissibility of the transfer of personal data by the Contractor to the Client is justified by the inclusion of approved standard contractual clauses, the parties hereby agree, for this transfer, as an integral part of the DPA, to the European Standard Contractual Clauses (SCC; <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914>), general provisions and Module 4. In the event of any conflict, the SCC shall prevail over the Agreement and this DPA.

- (b) Clause 7 SCC shall apply; (ii) Clause 11 SCC shall apply without the option; (iii) for Clause 17 SCC, the law agreed in the Agreement shall apply, or Swiss law if the applicable law does not provide otherwise; (iv) for Clause 18 SCC, the place of jurisdiction under the Agreement shall apply; (v) Annex I of the SCC shall be governed by the Agreement and Annex II by Annex 1 of this DPA. (v) If the transfer subject to the SCC is subject to Swiss data protection law, references in the SCC to the GDPR shall also be read as references to the Swiss FADP, references to EU Member States shall also include Switzerland, and the FDPIC shall be a competent supervisory authority.

9. Contact persons

- (a) The Client shall designate to the Contractor one or more contact persons for questions in connection with this DPA.
- (b) The Contractor shall be deemed authorized, until revoked, to communicate with this person on all matters of processing on behalf, including notifications of data security incidents.

10. Final provisions

- (a) Amendments: Amendments or additions to this agreement require an express agreement in text form.
- (b) Liability: Liability arising from breaches is governed by the contract and, subsidiarily, by the liability provisions applicable by law.
- (c) Notices: Notices provided for in this AV agreement must in each case be made expressly and in text form (e.g. by E-Mail), unless otherwise agreed.
- (d) Dispute resolution: The applicable law and the place of jurisdiction are governed by the contract.

Annex 1: Technical and organizational measures

Status: April 2026

1. Introduction

- (a) The following technical and organizational measures describe the specific steps to be taken by the Contractor in connection with the processing of personal data and the fulfillment of obligations under the main contract and the data processing agreement in order to ensure a level of protection appropriate to the risk.
- (b) If the data processing is carried out by a subcontractor engaged by the Contractor, the Contractor shall ensure by means of suitable contractual arrangements that the subcontractors comply with comparable measures. The assessment of whether the technical and organizational measures described below are appropriate for protecting the data entrusted to the Contractor is the responsibility of the Client.

2. Physical access control

- (a) Measures suitable for preventing unauthorized persons from gaining access to data processing facilities with which personal data are processed or used.
- (b) Access control may include the following measures: Alarm systems, automatic notification to a security service, electronic access systems using magnetic cards, authorizations and locking systems for sensitive rooms, data protection-compliant video surveillance, authorization process, visitor policy, reception staff, careful selection of cleaning and security personnel.

3. Access control

- (a) Measures that are suitable for preventing data processing systems from being used by unauthorized persons.
- (b) Access control may include the following measures: IT systems in independent, secured networks, protection by user ID and password, secure passwords in accordance with the password policy, two-factor authentication, encryption of mobile devices, anti-virus software, trustworthy personnel for the security and cleaning areas, access on a need-to-know basis after prior approval, blocking of access after departure, regular review of all access authorizations.

4. Logical access control

- (a) Measures that ensure that persons authorized to use a data processing system can access only the data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use, and after storage.
- (b) Access control may include the following measures: Only approved devices (PCs, laptops, etc.) may

use the network, access to computers and applications only by means of user ID and password. Secure passwords in accordance with the password policy, logging of access, authorization concept, granting of access according to the need-to-know principle and prior approval, periodic review of authorizations, especially of administrative user accounts, limited number of administrators who have full access authorization, four-eyes principle for special applications, all employees take part in annual data protection training, disposal of confidential data via certified specialist disposal companies.

5. Separation control

- (a) Measures that guarantee separate processing of data collected for different purposes.
- (b) Separation control can include the following measures: access-controlled secure areas, data-processing applications on virtualized application servers, access according to the need-to-know principle, separation of systems in development, testing, integration and production, use of firewalls, tenant separation, database rights and authorization concepts tailored to the respective data records, authorization concept, separation of data stored for different purposes.

6. Input control

- (a) Measures that ensure that it can be subsequently verified and determined whether personal data have been entered into, modified in, or removed from data processing systems, and by whom.
- (b) Input control may include the following measures: storage of confidential documents, traceability of access, access to logs by IT administration, logs are integrated into data backup procedures, retention periods, setup and use of individual usernames, assignment of access authorizations.

7. Transfer control

- (a) Measures that ensure that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or during its transport or storage on data carriers, and that it can be verified and determined to which entities the transmission of personal data by data transmission facilities is intended.
- (b) Transfer control may include the following measures: access to dedicated network zones exclusively via company-owned devices and VPN access with two-factor authentication, data on mobile devices is encrypted, data exchange via SFTP, email encryption, disposal of confidential documents and electronic data carriers through a certified disposal company.

8. Order control

- (a) Measures that ensure that the processing of personal data by subcontractors is carried out only in accordance with the instructions of the controller.
- (b) Order control may include the following measures: confidentiality obligation, reporting of security incidents, data protection impact assessments, careful selection of subcontractors, conclusion of data

processing agreements.

9. Availability check

- (a) Measures that ensure that personal data are protected against accidental destruction or loss.
- (b) Availability control may include the following measures: Monitoring and securing server systems, data backup procedures and archiving, redundant systems, anti-theft protections, virus protection, fire-wall/IDS, alarm systems, fire protection measures in the server room and office premises, tests for data recovery, fire extinguishers, emergency management, standard processes when employees change roles/leave the company.

10. Recoverability

- (a) Measures that ensure the rapid restoration of data availability after their temporary loss or damage.
- (b) Restorability may include the following measures: virtualized systems, data backups, redundant servers with reserve capacity, emergency plans, exercise plans, emergency concept/emergency plan, audits, exercises, emergency documentation.

11. Review, assessment and evaluation (organizational control)

- (a) Measures for the regular review, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of processing.
- (b) Organizational control may include the following measures: data protection management or data protection organization, incident response management, privacy-friendly default settings, documented record of processing activities, training of employees, central instruction management.