Data Processing Agreement

1 Introduction

This Data Processing Agreement (henceforth the «DPA») supplements the Main Agreement with regard to the processing of personal data, in particular with regard to the requirements of the Swiss Data Protection Act (CH-DPA) and the EU-General Data Protection Regulation (EU-GDPR) concerning the processing of personal data by bbv Software Services AG, Blumenrain 10, 6002 Lucerne (hereinafter ”bbv” or ”Service Provider”). This may concern one or several agreements between bbv as the Service Provider and the Customer or Contracting Entity (henceforth “Controller“), provided that bbv acts as Service Provider vis-à-vis the Controller. Offers and invoices are deemed as contractual documents. In the event of contradictions between the provisions of this DPA and the other contractual provisions between the parties, the provisions of this DPA concerning the processing of personal data shall take precedence over the other agreements. This DPA applies to all processing of personal data which is carried out by bbv in its function as the Authorized Processor (henceforth ”Processor”) of the Customer or Controller.

This DPA uses the terminology of the EU-GDPR, whereby the use of EU-GDPR terminology is merely intended to ensure consistency and simplification. Where applicable, the corresponding terms also include the substantively equivalent or comparable terms of the CH-DPA, even if they are designated differently therein. References to terms of the EU-GDPR are therefore to be interpreted as including the corresponding concepts of the CH-DPA.

2 Subject Matter and Validity

The Controller acts as the controller within the meaning of the data protection laws. The Service Provider acts as the Processor.

The subject matter of the Data Processing is set out in the Main Agreement. The term of this Data Processing Agreement shall correspond to the term of the Main Agreement, unless the provisions set out below give rise to any additional obligations that extend beyond such term.

The categories of personal data which are processed, the categories of Data Subjects and the applicable Technical and Organizational Measures constitute the subject matter of this DPA.

3 Scope and Responsibility

3.1 Lawfulness of Data Processing

The Parties shall process personal data exclusively in a lawful manner and shall comply with all applicable data protection laws and principles.

The Service Provider shall process personal data exclusively for the purpose of completing the contract and/or for the purposes which are stated in the Main Agreement, in accordance with this Data Processing Agreement and the documented directives and instructions of the Controller. The Controller shall be solely responsible for compliance with the statutory requirements of the applicable data protection laws, in particular the lawfulness of the disclosure of personal data and the processing of personal data by bbv, including the permissibility of processing by a processor and/or sub-processor.

The processing shall take place within Switzerland or the EEA. If processing takes place in third countries, the Service Provider shall ensure that an adequate level of data protection exists for this purpose in accordance with the CH-DPA or EU-GDPR.

3.2 Additional Instructions

The Controller has the right to issue additional instructions to the Service Provider in writing at any time in relation to the processing of personal data. The Service Provider shall comply with such instructions to the extent that they can be implemented by the Service Provider within the scope of the contractually agreed services and are objectively reasonable. If such instructions result in additional costs for the Service Provider or a changed scope of services, the contractually agreed contract amendment procedure shall apply.

3.3 Compliance of Instructions

The Service Provider shall inform the Controller without undue delay if it considers that an instruction violates the CH-DPA or the EU-GDPR. In this case, the Service Provider may suspend implementation of the instruction until it has been confirmed or amended by the Controller that it is lawful.

The above does not apply to instructions of the Controller in connection with the granting of access rights or the disclosure of personal data to the Controller itself. The Service Provider may at any time assume that these instructions comply with the law. However, it is entitled to request corresponding written confirmations from the Controller.

4 Type of Data Processed

4.1 General

The Controller provides the Service Provider with personal data for processing in connection with the Main Agreement and its engagement. A distinction is made between data for administrative and commercial cooperation and data for the performance of the agreed service.

The Service Provider classifies systems and data (personal and non-personal data) for the provision of services in order to ensure that the information is given an appropriate level of protection. A distinction is made between three categories of information classification:

- Confidential: Data which relate to individuals and concern their privacy (personal data and particularly sensitive personal data) as well as data which are explicitly classified as confidential.
- Internal: Data that does not constitute personal data but is relevant to the fulfilment of the engagement.
- Public: Information which is accessible for everyone.

Personal data are classified as confidential data and are therefore given the highest level of protection.

4.2 Data Subjects

The processing of personal data by the Service Provider under the Main Agreement concerns the following Data Subjects:

- Potential customers, customers, business partners, suppliers and service providers.
- Employees or other auxiliary personnel of potential customers, customers, business partners, suppliers and service providers.
- Employees or other auxiliary personnel of the customer who have been authorized by the customer to use the Services.

4.3 Types of Personal Data

The processing of personal data under the Main Agreement may involve the following types of personal data:

- Contact details such as email address, telephone number or address.
- Other data such as contract, billing or payment data.
- Personal information such as first name, last name, date of birth, gender or nationality.
- Information about professional life such as job title or function.
- User information such as login data, customer number, personal number or personnel number.
- Technical information such as IP address or device information.
- Other personal data which the Controller provides in the context of the provision of services.

4.4 Exceptions

If the data have been encrypted by the Controller and are therefore not accessible to the Service Provider, they do not constitute data which are processed on behalf of the Controller by the Service Provider. Furthermore, processing on behalf of the Controller does not apply if the personal data have been transferred directly by the Controller to a Sub-processor and are not accessible to the Service Provider. In these cases, this DPA does not apply.

The Service Provider may anonymize the Controller's personal data (henceforth «Controller Data») for its own purposes, e.g. by aggregating the data so that individual Data Subjects can no longer be identified. The parties agree that anonymized Controller Data is no longer subject to this DPA.

If the data is provided by the Customer or the Controller for the provision of services (e.g. test data), or if employees of the Service Provider gain access to this data on the Controller's infrastructure, the handling of this data is governed by the Main Agreement. If this is not the case, this DPA shall apply subsidiarily.

5 Security Measures of the Service Provider

5.1 Compliance with Legal Provisions

The Service Provider undertakes to comply with the statutory provisions on data protection and not to disclose Controller Data to third parties.

5.2 Technical and Organizational Measures (TOMs)

The Service Provider maintains appropriate Technical and Organizational Measures (henceforth ″TOM″) and a quality-management system. The Information Security Management System (henceforth ″ISMS″) is an integral part of the quality-management system, which is certified in accordance with the ISO 9001 and ISO 13485 standards. The ISMS defines the TOMs. The certificate is publicly available on the Service Provider's website. bbv continuously develops its ISMS and aligns it with recognized standards.

The measures which are described in Appendix 1 are to be understood as generic and apply to cases in which the Service Provider itself processes personal data. They shall apply in each case unless otherwise defined in the Main Agreement. bbv reserves the right to change security measures which are implemented, provided that the contractually agreed level of protection is not reduced. bbv shall require everyone who is processing Controller Data to maintain confidentiality.

If data processing is carried out by third parties who are engaged by the Service Provider, the Service Provider shall ensure by means of appropriate contractual agreements that such third parties comply with measures which are comparable to those which are set out in this DPA.

The Controller shall verify whether the TOMs which are described in Appendix 1 meet its statutory and contractual requirements.

6 Obligations of the Service Provider

6.1 Data Processing

The Service Provider processes the relevant data exclusively in accordance with the provisions of the Main Agreement and this DPA. This is subject to the fulfilment by the Service Provider of statutory, regulatory or official obligations.

6.2 Review of Technical and Organizational Measures

The Service Provider periodically reviews the agreed Technical and Organizational Measures with regard to state-of-the-industry technology and adjusts them as necessary in order to ensure that the security level which is defined in this DPA is not reduced.

6.3 Record of Processing Activities

The Service Provider undertakes to maintain a record of processing activities with regard to personal data in accordance with Art. 12 para. 1 CH-DPA and Art. 30 para. 2 EU-GDPR. The Service Provider shall grant the Controller access, upon request at any time, to the parts of this record that concern the Controller.

6.4 Confidentiality Obligation

The Service Provider shall ensure that its employees and other auxiliary personnel who are involved in processing the Controller's personal data are prohibited from processing the personal data for purposes other than those stated in the Main Agreement or for purposes which are in deviation from this DPA.

The Service Provider shall further ensure that people who are authorized to process personal data have committed themselves to maintaining confidentiality. The confidentiality obligation shall continue after termination of the Main Agreement.

6.5 Duty to Inform

The Service Provider shall inform the Controller without undue delay if it becomes aware of any personal data breach or other irregularities in the processing of Controller Data by bbv or one of its Sub-Processors.

The Service Provider shall inform the Controller in writing (email being sufficient) in an appropriate manner about the nature and extent of the breach and possible remedial measures. In such a case, the parties shall take the necessary measures to ensure the protection of personal data and to mitigate possible adverse consequences for the Data Subjects and the parties themselves, and they shall coordinate with each other without undue delay.

6.6 Contact Person

For questions in connection with this DPA, the Controller may contact datenschutz@bbv.ch, unless a different contact is defined in the Main Agreement.

6.7 Data Deletion

Relevant personal data shall be returned or deleted after the ending of the Main Agreement in accordance with the provisions of the Main Agreement, unless applicable law requires the retention of the personal data for a longer period. The Service Provider applies procedures which are established in the IT industry for the deletion of personal data.

7 Controller's Duty to Inform

The Controller shall inform the Service Provider without undue delay if, in the provision of services by the Service Provider, it identifies breaches of data protection regulations.

The Controller shall provide the Service Provider with the name of the contact person for data protection matters which arise in relation to the Main Agreement and, in cases where this is required pursuant to Art. 37 EU GDPR, the name of the data protection officer also.

8 Requests from Third Parties

If a third party directly approaches the Service Provider with requests for rectification, deletion, access or other claims relating to personal data, the Service Provider shall refer the third party to the Controller, provided that the request can be attributed to the Controller.

9 Evidence, Reports and Audits

In principle, evidence of appropriate Technical and Organizational Measures is provided by the Service Provider's ISO/IEC 9001:2015 certification. Audit rights which are defined in the Main Agreement and audit rights of the Controller or its supervisory authorities which are mandatory under applicable law remain reserved. In the context of such audits, the principle of proportionality shall expressly be observed, and the Service Provider's legitimate interests (e.g. confidentiality obligations) shall be taken into account appropriately. The Controller shall bear all costs of such audits (including documented internal costs of the Service Provider at its usual hourly rates and as were incurred in participating in the audit).

If breaches of this DPA or deficiencies in the implementation of the Service Provider's obligations are identified after evidence or reports have been provided or in the course of an audit, the Service Provider shall implement appropriate corrective measures.

10 Sub-processing Relationships

To the extent that the Main Agreement does not contain restrictive provisions regarding the engagement of third parties, the Service Provider is entitled to engage Sub-Processors. The Service Provider shall ensure that, to the extent possible, the Sub-processor is subject to the same obligations as those incumbent upon bbv under this DPA. The parties agree that this requirement is fulfilled if the contract provides for a level of protection which corresponds with this DPA.

The Sub-Processors which are engaged are categorized according to their type of service and listed in Appendix 2. The Sub-Processors which are listed there apply at the time when the Main Agreement is concluded.

The Service Provider shall inform the Controller of significant changes concerning the engagement of additional or replacement Service Providers which concern the processing of personal data.

11 Liability

The Controller and the Processor shall be liable towards Data Subjects in accordance with the provisions of the applicable data protection law. The Processor shall coordinate any fulfilment of liability claims with the Controller.

Each party shall be released from liability if a party proves that it is in no way responsible for the circumstance which caused the damage to a Data Subject.

Unless otherwise accounted for above, liability under this Agreement shall correspond to that which is contained in the Main Agreement.

12 Final Provisions

If individual provisions of this DPA are or become invalid or contain a gap, the remaining provisions shall remain unaffected. The parties undertake the replacement of the invalid provision with a legally permissible provision which comes as close as possible to the purpose of the invalid provision and best meets the requirements of applicable data protection law.

Amendments to this DPA, subject to the exceptions expressly excluded in this DPA, must be made in writing to be valid.

Applicable law and the place of jurisdiction shall be determined by the Main Agreement, unless this Agreement contains deviating provisions.

In the event of any discrepancies between the English and German versions of this DPA, the German version shall prevail.

bbv
MAKING VISIONS WORK.

Appendix 1 – Technical and Organizational Measures (TOMs)

The Service Provider implements appropriate Technical and Organizational Measures to protect personal data in accordance with the applicable data protection laws and state-of-the-industry technology.

These measures form part of the Service Provider's Information Security Management System (ISMS) and are subject to continuous review and further development.

1. Confidentiality

The measures listed below describe the procedures which are implemented within the company to ensure the confidentiality of personal data. They serve to restrict access to systems and personal data to authorized personnel and to ensure that the data is used exclusively in an authorized manner.

ID	Existing	Measure
1.1	☒	Access rights are established according to the Principle of Least Privilege (POLP).
1.2	☒	Access to the Service Provider's systems is exclusively via dedicated infrastructure with strong authentication. Two-factor authentication applies.
1.3	☒	Access via the Internet to relevant data is generally made via an encrypted connection. The Service Provider uses current protocols and protection mechanisms for this purpose.
1.4	☒	Separate communication channels are used when transmitting access credentials.
1.5	☒	No removable media are used to store sensitive information.
1.6	☒	The Service Provider ensures that the personal data of Controllers is not mutually accessible. The separation of customer data is ensured at the logical level using current security procedures.
1.7	☒	When employees leave, access rights are withdrawn and company equipment is returned or deactivated.

2. Availability

The measures listed below describe the procedures which are implemented within the company to ensure the availability and resilience of personal data and the systems used. They serve to protect data media and stored data, to securely transmit personal data, to restore availability after disruptions or failures, and to continuously update and secure the systems which are used.

ID	Existing	Measure
2.1	☒	The Service Provider stores data in data centers which fulfil the required level of protection.
2.2	☒	To ensure data availability, the Service Provider's storage systems are configured such that, whilst one or more components can fail, the data will nevertheless remain available.
2.3	☒	The Service Provider backs up the data in accordance with the service description. The backup is always performed on separate storage systems in different data centers with a sufficient geographical distance between the two locations.
2.4	☒	The Service Provider implements the necessary processes to identify and assess notifications concerning software vulnerabilities and patches and to derive the necessary further steps. The standard patch management process ensures that notifications of patches for systems are assessed and, following a review, installed on the relevant systems. The installation of patches may require the cooperation and approval of the Controller. This is taken into account in the Service Provider's standardized processes. If a patch must be installed urgently, a so-called Emergency Patch Process is available depending on the service involved.

3. Integrity

The measures listed below document the procedures which are implemented within the company to ensure the integrity of personal data. They serve to protect personal data during transmission and storage and to ensure traceability of entries, changes and deletions.

ID	Existing	Measure
3.1	☒	Permanent storage in the data centers is protected against loss by physical protection measures.
3.2	☒	In the event of a defect, data media are physically rendered unusable by the Service Provider in order to completely prevent possible access.
3.3	☒	Functional data media are erased using industry-standard deletion procedures so that reconstruction of the data contained therein is almost impossible. If such a procedure is not possible, the data media are physically rendered unusable or destroyed.
3.4	☒	Where the Service Provider is responsible for the entry and processing of personal data, the Service Provider ensures with the necessary Technical and Organizational Measures that such data is correctly recorded and processed.
3.5	☒	The Service Provider records additional personal data of the Controller for the provision of services. This data is used, for example, to record incident reports, change requests or for invoicing. The Service Provider ensures through appropriate quality measures that this data is also correctly recorded and processed.

4. Traceability

The measures listed below describe the procedures which are implemented within the company for reviewing, assessing, evaluating and continuously improving data protection and information security. They serve to ensure and continuously improve the Technical and Organizational Measures.

ID	Existing	Measure
4.1	☒	The information security policy is documented (ISMS).
4.2	☒	Roles and responsibilities in the area of information security are defined and documented in writing. Employees are informed where they can report security incidents.
4.3	☒	A documented process exists for handling information security incidents. Security incidents are handled and documented according to a defined procedure.

5. Review, Assessment, Evaluation and Training

The measures listed below document the procedures which are implemented within the company for review, assessment, evaluation and training in the areas of data protection and information security.

ID	Existing	Measure
5.1	☒	The Service Provider periodically reviews the internal processes and the Technical and Organizational Measures in order to ensure that processing within its area of responsibility is carried out in accordance with the requirements of applicable data protection law and that the protection of the rights of Data Subjects is ensured.
5.2	☒	Based on a risk analysis, new services and offerings are subjected to a technical review. Identified deficiencies are remedied by the responsible bodies of the Service Provider. Depending on the severity of the deficiencies, an additional review is carried out to demonstrate the effectiveness of the remediation.
5.3	☒	The Service Provider periodically conducts internal and external audits to review and optimize information security. Identified deficiencies are remedied within the defined timeframe and, depending on their severity, reviewed again by the internal audit function.
5.4	☒	The Service Provider periodically conducts a risk assessment. The purpose of the risk assessment is to identify potential information security risks, their impact and the likelihood of any occurrence. A periodically recurring risk assessment report describes the measures taken by the Service Provider to reduce the risk potential and its impacts.
5.5	☒	New employees of the Service Provider are subject to screening before commencing employment. A confidentiality clause and the data protection policies are signed.

ID	Existing	Measure
5.6	☒	New employees are familiarized with the relevant rules concerning their own security and data security when they commence work.
5.7	☒	Existing employees of the Service Provider receive periodic awareness training.

MAKING VISIONS WORK.

Appendix 2 – Sub-Processors of the Service Provider in the context of service provision

Services in relation to the bbv AI Hub

The Sub-Processors listed below are engaged by bbv if the services are provided as part of the AI Hub offering. bbv is furthermore entitled to engage or use additional Sub-Processors for other services or offerings. In these cases, a corresponding Data Processing Agreement shall apply to such service provision.

Name of Sub-Processor	Address	Function	Measures to ensure appropriate data protection
stepping stone AG	Wasserwerkgasse 7, CH-3011 Bern, Switzerland	Cloud Infrastructure as a Service, GPU/server infrastructure for LLM services, LLM as a Service	Data Processing Agreement, ISO/IEC 27001 certified, Technical and Organizational Measures (TOMs), data processing in Swiss data centers
Phoenix Technologies AG	Christmases 54, 8808 Pfäffikon SZ, Switzerland 8808 Pfefferkorn SZ, Schweiz	LLM as a Service	Data Processing Agreement, ISO/IEC 27001 (where applicable), TOM pursuant to Art. 32 GDPR/DPA, Confidential Computing, data storage in Swiss Sovereign Cloud
Infomania Network SA	Rue Eugène-Marziano 25, 1227 Les Acacias (Geneva), Switzerland	LLM as a Service	Data Processing Agreement, ISO/IEC 27001, Technical and Organizational Measures (TOMs), data processing in Switzerland
iCloud SAS	2 Rue Kellermann, 59100 Roubaix, France	LLM as a Service	DPA (iCloud Data Processing Agreement), ISO/IEC 27001, ISO/IEC 27701 (for selected services), ISO/IEC 27017, ISO/IEC 27018, Technical and Organizational Measures (TOMs), Standard Contractual Clauses (SCC)

bbv
MAKING VISIONS WORK.

Services in relation to the Swiss LCDM Hub

The Sub-Processors listed below are engaged by bbv if the services are provided as part of the Swiss LCDM Hub offering. bbv is furthermore entitled to engage or use additional Sub-Processors for other services or offerings. In these cases, a corresponding Data Processing Agreement shall apply to such service provision.

Name of Sub-Processor	Address	Function	Measures to ensure appropriate data protection
Microsoft Schweiz GmbH	Microsoft Schweiz GmbH, The Circle, Postface, 8058 Zürich-Flughafen, Switzerland	Cloud Services (e.g. Microsoft Azure, Microsoft 365)	DPA (Microsoft DPA), ISO/IEC 27001, ISO/IEC 27701, SOC 1/2, Technical and Organizational Measures (TOMs)

Services in relation to service provision

Name of Sub-Processor	Address	Function	Measures to ensure appropriate data protection
Microsoft Schweiz GmbH	Microsoft Schweiz GmbH, The Circle, Postface, 8058 Zürich-Flughafen, Switzerland	Cloud Services (e.g. Microsoft Azure, Microsoft 365)	DPA (Microsoft DPA), ISO/IEC 27001, ISO/IEC 27701, SOC 1/2, Technical and Organizational Measures (TOMs)
Kudelski Security SA	Route de Genève 22–24, 1033 Cheneaux-sur-Lausanne, Switzerland	Security Monitoring (SOC), Managed Detection & Response (MDR), Security Operations	DPA, ISO/IEC 27001, Technical and Organizational Measures (TOMs), confidentiality obligations
Open Systems AG	Räffelstrasse 29, 8045 Zürich, Switzerland	Managed Security Services, IT Monitoring, Firewalls, Secure Access Service Edge (SASE)	DPA, ISO/IEC 27001, Technical and Organizational Measures (TOMs), data processing in accordance with contractual instructions
Slack Technologies Limited (Salesforce Group)	Salesforce Tower, 60 R801, North Dock, Dublin 1, D01 W028, Ireland	Collaboration and communication platform (team chat, file and document exchange, audio/video conferences)	DPA (Slack Data Processing Addendum), EU Standard Contractual Clauses (SCC), Technical and Organizational Measures (TOMs), ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 Type II
Net Solutions AG	Früebergstrasse 47, 6340 Baar, Switzerland	Managed IT Services, system operation, support	DPA, Technical and Organizational Measures (TOMs), confidentiality obligations

Acronis International GmbH	Rheinweg 9, 8200 Schaffhausen, Switzerland	Backup	DPA (Acronis Data Processing Addendum), ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 Type II, Technical and Organizational Measures (TOMs), encryption of data in transit and at rest