Data Processing Agreement (DPA)

This DPA outlines the obligations of the contracting parties regarding data protection, which result from the contractual relationship (the "Contract") between Vertec and the customer. The following legal provisions in particular apply: a) For customers in Germany, Austria and other countries of the European Union: the General Data Protection Regulation of the European Union (GDPR); b) For customers in Switzerland: the Swiss Data Protection Act (DSG), the Ordinance on the Data Protection Act (VDSG) and, if applicable, the GDPR; c) For customers in the UK: the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This provision applies to all types of contract-related services where Vertec processes the customer's personal data ("data").

1 Subject matter, duration and specification of the data processing

The subject matter and duration, as well as the nature and purpose of the data processing arises from the Contract.

The duration of this DPA shall be the same as the duration of the Contract, unless the provisions of this DPA give rise to additional obligations.

Vertec processes the customer's personal data as a data processor in the following cases:

- When migrating data from external systems to Vertec in accordance with a customer request. In this case, personal data is only processed to the extent that the customer intends to migrate data to Vertec and provides such data to Vertec (e.g. personal data about the customer's employees);
- When Vertec receives a request to save a copy of the Vertec database for testing or support purposes (this requires a separate request from the customer). In this case, personal data saved by the customer in the Vertec database is processed (e.g. personal data about the customer's employees);
- When using the Vertec Cloud Suite, where Vertec operates the Vertec software on behalf of the customer. In this case, personal data saved by the customer in the Vertec database is processed (e.g. personal data about the customer's employees) The type of personal data processed depends on the use of the software by the customer and may include all categories of personal data. Typically, this concerns the following categories:
  Categories of personal data, e.g.
  - Master data (name, address)
  - Contact details (e-mail, telephone number)
  - Content data (text entries, documents, uploads)

  Categories of data subjects, e.g.
  - Customers of the contracting entity
  - Employees of the customer
  - Interested parties
  - Other third parties whose data are processed by the customer

  The specific personal data processed is the responsibility of the customer who stores this data in Vertec.
- When using the Vertec service for optional receipt recognition of expense and creditor documents. With this service, the customer has the option of extracting commercial data from image or PDF files using an AI-based service in order to process them with Vertec. Although the service does not permanently save the input (expense and creditor documents) nor the extracted output (commercial data), the identity of the customer is transmitted to the service for verification. In addition, in the event of an error, image or PDF files or the extracted output may be saved in log files. However, such data is not permanently linked to the identity of the customer.
- When using the optional AI Know-how Management module. This is an AI-based chat service provided as a cloud service based on Vertec data. Data relevant to the chat, especially activities and documents, but also master data regarding addresses and projects or mandates and potentially also personal data, are stored and saved and indexed in a database operated by Vertec. When a query is submitted using Vertec AI chat, data relevant to the question is retrieved from the index and sent to the pre-configured LLM (pre-configured by the customer) to generate a response.

2 Scope and responsibility

Vertec processes personal data on behalf of the customer and in accordance with its instructions. Within the scope of this Contract, the customer is responsible for compliance with the legal provisions of the data protection laws for the legality of data processing ("controller" as defined in Art. 4 No. 7 GDPR or Art. 5 lit. j. GDPR).

The instructions are stipulated in the Contract. Instructions from the customer that are not provided for in the Contract are treated as a request for a change in services and are subject to an additional fee.

3 Obligations of Vertec

Vertec may only process data within the scope of the Contract and the instructions of the customer, unless there is an exceptional case as defined by Article 28 (3) a) of the GDPR or a justification in accord-

ance with Article 9 (4) of the DSG. Vertec shall inform the customer immediately if Vertec is of the opinion that an instruction violates applicable laws. Vertec may suspend the implementation of the instruction until it has been confirmed or amended by the customer.

Within its area of responsibility, Vertec will design the internal organization in such a way that it meets the specific requirements of data protection. Vertec implements and maintains technical and organizational measures to adequately protect the customer's data, which meet the requirements of the General Data Protection Regulation (Art. 32 GDPR) and the DSG (Art. 8 DSG). Such measures must permanently ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing. The relevant processes as well as the technical and organizational measures introduced in relation to data protection are assessed and verified by external auditors within the framework of ISO 27001 (information security) and ISO 9001 (quality management) certification. Of the technical and organizational measures provided for by ISO 27001 in normative annex A ("controls") and applied in the context of section 6.1.3, Vertec confirms in the "Statement of Applicability" the applicability of all controls provided for. The application of the controls within the framework of the ISO 27001 standard is also assessed and certified by external auditors. Vertec will inform the customer in an appropriate form if the certificates are withdrawn in the future and will provide copies of them upon request.

To the extent agreed and against separate remuneration, Vertec shall support the customer, if possible, in fulfilling the requests and claims of data subjects pursuant to Section III of the GDPR or pursuant to Section 4 of the DSG as well as in compliance with the obligations referred to in Articles 33 to 36 of the GDPR or Articles 24 of the DSG and 25 of the DSG.

Vertec guarantees that the employees involved in the processing of the customer's data and other persons working for Vertec are not allowed to process the data in other ways than instructed. Vertec further guarantees that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality. The duty of confidentiality/non-disclosure shall continue after termination of the Contract.

Vertec shall inform the customer immediately if it becomes aware of any breaches of the protection of the customer's personal data. Vertec shall take the necessary measures to secure the data and to mitigate any possible negative consequences for the persons concerned, and shall inform the customer immediately.

Vertec shall give the customer the name of a contact person for data protection issues arising within the scope of the Contract.

Vertec ensures that it complies with its obligations pursuant to Art. 32 (1) (d) GDPR or Art. 1 et seq. VDSG, to use a procedure to regularly review the effectiveness of the technical and organizational measures to ensure the security of processing.

Vertec corrects or deletes the contractual data if the customer instructs to do so and if this is covered by the instructions. If it is not possible to delete data or restrict its processing compliant with data protection laws, Vertec shall assume the task of destroying any data, data carriers and other materials in a manner compliant with data protection laws and return them to the customer. These services require a separate request from the customer and are to be remunerated separately.

After the end of the Contract, data, data carriers and all other materials shall be either handed over or deleted at the customer's request.

In the event of a claim against the customer by a data subject with regard to any claims pursuant to Art. 82 GDPR or in accordance with the applicable provisions of Swiss law, Vertec undertakes to support the customer in defending the claim within its means. These services are to be remunerated separately.

4 Obligations of the customer

The customer must immediately and fully inform Vertec if it discovers errors or irregularities with regard to data protection regulations.

In the event of a claim against the customer by a data subject with regard to any claims pursuant to Art. 82 GDPR or pursuant to the applicable provisions of Swiss law, Section 3 (10) of this document shall apply mutatis mutandis.

The customer shall give Vertec the name of a contact person for data protection issues arising within the scope of the Contract.

5 Requests from data subjects

If a data subject contacts Vertec with requests for correction, deletion or information, Vertec refers the data subject to the customer. Vertec forwards the data subject's request to the customer without delay. Vertec is not liable if the customer does not respond to the data subject's request correctly or in a timely manner.

6 Audit rights

Vertec shall prove to the customer, upon request, compliance with the obligations stipulated in this Contract by appropriate means.

If audits by the customer are required in individual cases, the customer must engage a recognized data protection expert for this purpose. The audit by the data protection expert must be carried out during normal business hours, taking into account a reasonable lead time. Vertec may make this subject to the signing of a non-disclosure agreement with respect to the data of other customers and the technical and organizational measures in place. If the auditor commissioned by the customer is in a competitive relationship with Vertec, Vertec shall have the right to object. Vertec may demand payment for assistance in carrying out an audit.

Should a data protection authority or another supervisory authority carry out an audit regarding the customer, the preceding paragraph shall in principle apply mutatis mutandis. It is not necessary to sign an obligation of confidentiality if this supervisory authority is subject to professional or statutory secrecy.

7 Subcontractors (other data processors)

The use of subcontractors, with the exception of Vertec Group companies, as additional processors is only permitted if the customer has given their prior consent.

Excluded from this is the processing of data within the scope of the Vertec Cloud Suite and other optional cloud services for which the customer agrees to the use of subcontractors with the conclusion of a Contract.

Vertec works with subcontractors in this regard, which are listed here:

https://www.vertec.com/en-ch/terms-and-conditions/subcontractors/

The consent to use subcontractors is required when Vertec engages other contractors to perform all or part of the contracted service. Vertec will enter into agreements with these third parties to the extent necessary to ensure appropriate data protection and information security measures.

If Vertec appoints subcontractors, Vertec shall assign its data protection obligations under this DPA to the subcontractor.

Vertec shall be authorized to replace subcontractors without the explicit consent of the customer if the new subcontractors ensure the same or higher level of data protection. Vertec shall inform of such changes on its website (see link above) and via the e-mail newsletter (registration required). If the customer objects to such a change, he has an extraordinary right of termination regarding the affected cloud services.

8 Information obligations, written form clause, choice of law

Should Vertec's customer data be endangered by legal seizure or confiscation, by insolvency proceedings or by other events or actions of third parties, Vertec shall immediately inform the customer. Vertec shall immediately inform all persons responsible in this context that the ownership of the data rests with the customer.

Amendments and additions to this DPA and all its components – including any representations by Vertec – require a written agreement, which may also be made in electronic format (text form), and the express indication that it is a change or addition to this DPA. This also applies to the waiver of this formal requirement.

In the event of any contradictions, the provisions of the Contract shall have precedence over this DPA. Should parts of this DPA be ineffective, this shall not affect the effectiveness of the rest of the DPA.

The law applicable to the Contract shall also apply to this DPA.

9 Liability and damages

The customer and Vertec shall be liable to the data subjects in accordance with the provisions stipulated in Article 82 of the GDPR and in accordance with the applicable provisions of Swiss law.

Overview of technical and organizational measures

10 Principles, IT basic protection

Vertec's information security management system places great emphasis on IT infrastructure protection and the training and awareness of employees regarding threats to information security.

Increased importance is given to the following topics:

- Client infrastructure protection. Employee workstations and laptops pose a major threat to information security. Vertec places great priority on protecting this infrastructure. Protection measures include: virus scanners, hard disk encryption, patch management systems, hardening systems against attacks via unnecessarily open ports. Client infrastructure protection also includes raising employee awareness of the risks associated with malware and social engineering.
- Separation of networks: Vertec's internal networks are separated from networks with customer services. Individual customer-related services are also interconnected only where absolutely necessary (e.g. the Forum uses the Customer Portal so that customers can log into the Forum).
- Administrative access to server resources is severely limited to a small team of IT administrators.
- All existing passwords are available according to the "need to know" principle only to those users who participate in the relevant process.
- Physical security at Vertec locations. Offices are permanently locked. Access to internal server rooms is secured via armored door and code lock.
- Handling of customer data (data in the possession of customers, not only, but also personal data). In an established monthly process, customer data (e.g. from support requests) is identified and deleted if it is no longer needed for an order and if there is no order to store a Vertec database.
- Access to the Vertec LAN is restricted to devices protected according to section 10. External devices are not allowed to access the internal LAN by hardware (no "BYOD").

11 Processing of personal data in the internal Vertec network

In the case of an order to migrate data or a request to store a Vertec database, processing takes place on a server with restricted access. Alternatively, data migration can also take place on the customer's infrastructure.

After completion of the request, Vertec deletes the customer data.

12 Vertec Cloud Suite

With the Vertec Cloud Suite, Vertec software is operated by Vertec. Which (and if at all) personal data is processed by Vertec depends on the specific application of the customer. Vertec usually processes the customer's personal data completely automatically, there is no manual processing or even enrichment.

Exceptions are:

- Verification of the functioning of the Vertec database backup system by means of a random restore.
- An order from the customer to supply the Vertec database or an order from the customer to restore.
- Disaster recovery.
- For testing purposes

The Cloud Suite infrastructure consists of several connected Linux and Windows servers at the Cloud Suite locations in Switzerland, Germany and Austria. Administrative access to these servers is severely restricted by the circle of people. Communication between the locations and the servers themselves, is encrypted, from the Cloud Suite infrastructure to the customers' client applications, as well as administrative access.

Vertec creates a backup of all customers' Vertec Cloud Suite instances every night, and also saves them with backup service providers (see section 7).

Vertec checks the availability of the infrastructure via an external service, which does not have access to customer data.