

Data Processing Agreement pursuant to Art. 28 GDPR

Version date: 2026-04-13

between

Vent.Net Web-Software Andreas Vent-Schmidt

Kieselbach 7c

04746 Hartha

Germany

Phone: +49 34321 63 59 77

Email: xrechnung@vent.net

- hereinafter referred to as the “Processor” -

and

the respective customer using the XInvoice API

- hereinafter referred to as the “Controller” -

the following agreement is concluded:

1. Subject matter of the agreement

1. The Processor provides services to the Controller in connection with `xInvoice`, in particular for the processing, validation, generation, provision, and management of electronic invoice data via the web portal and API.
2. Where the Processor processes personal data on behalf of the Controller, such processing is carried out exclusively in accordance with this agreement.

2. Term

1. This agreement becomes effective upon acceptance by the Controller.
2. It remains in force for the duration of API usage or any other service requiring processing on behalf.
3. The right to extraordinary termination for cause remains unaffected.
4. Upon termination of the main contract, this agreement also ends unless statutory retention obligations require continued storage.

3. Nature and purpose of processing

1. Processing is carried out for the technical provision of `xInvoice` and includes in particular:
 - receipt of structured invoice data
 - validation of invoice data and invoice documents
 - generation of structured invoice documents
 - technical storage and provision of results
 - download and retrieval functions
 - error analysis, logging, and technical support
 - security and abuse prevention
2. Processing serves exclusively the purposes initiated by the Controller within the scope of using the service.

4. Type of personal data and categories of data subjects

4.1 Categories of personal data

Depending on use of the service, the following categories may be processed in particular:

- master data

- contact data
- address data
- email addresses
- telephone numbers
- invoice and order data
- service and line item data
- payment and billing data
- tax and identification data
- communication content
- technical usage and log data

4.2 Categories of data subjects

The following categories of data subjects may in particular be affected:

- contacts of the Controller
- employees of the Controller
- customers, suppliers, or business partners of the Controller
- invoice recipients
- other natural persons whose data is contained in transmitted invoice or business data

5. Obligations of the Controller

1. The Controller is responsible for the lawfulness of processing and for safeguarding the rights of data subjects.
2. The Controller shall promptly inform the Processor if the Controller identifies errors or irregularities in connection with data protection requirements.
3. The Controller shall only transmit data whose processing is permissible under applicable data protection law.

4. Instructions of the Controller shall in principle be issued in documented form.

6. Right to issue instructions

1. The Processor shall process personal data only on documented instructions from the Controller unless required to do so by Union or Member State law.
2. Oral instructions shall be confirmed in text form without undue delay.
3. If the Processor believes an instruction infringes applicable data protection law, the Processor shall inform the Controller without undue delay.

7. Confidentiality

1. The Processor shall ensure that all persons authorized to process personal data are bound to confidentiality or are subject to an appropriate statutory duty of confidentiality.
2. Access to personal data is granted only to the extent necessary under the need-to-know principle.

8. Technical and organizational measures

1. The Processor shall implement appropriate technical and organizational measures within the meaning of Art. 32 GDPR to ensure a level of security appropriate to the risk.
2. This includes in particular measures relating to:
 - physical access control
 - system access control
 - data access control
 - disclosure control

- input control
 - availability control
 - resilience and recoverability of systems
 - separation of data of different customers
 - procedures for regular review, assessment, and evaluation of the effectiveness of measures
3. The Processor may further develop technical and organizational measures provided that the overall level of protection is not reduced.

9. Assistance to the Controller

1. Taking into account the nature of processing and the information available, the Processor shall support the Controller in fulfilling obligations relating to:
- data subject rights
 - security of processing
 - notification of personal data breaches
 - data protection impact assessments
 - consultations with supervisory authorities
2. To the extent such support is not already covered by the contractual service, it may be invoiced separately.

10. Notification of personal data breaches

1. The Processor shall notify the Controller without undue delay if it becomes aware of a personal data breach affecting the Controller's data.

2. The notification shall include the available information required by the Controller to meet legal obligations.

11. Sub-processors

1. The Controller grants the Processor a general authorization to engage sub-processors where this is necessary for service provision.
2. The Processor shall inform the Controller of intended material changes regarding the addition or replacement of sub-processors.
3. The Controller may object to such a change for an important data protection related reason.
4. The Processor shall conclude agreements with sub-processors that meet the requirements of Art. 28 GDPR.

12. Evidence and audits

1. Upon request, the Processor shall make available suitable information to demonstrate compliance with the obligations laid down in this agreement.
2. Where necessary and proportionate, the Controller may conduct audits or have them conducted by a third party bound to confidentiality after giving reasonable prior notice.
3. Audits must not unreasonably impair the Processor's operations and shall be limited to the necessary scope.
4. The Processor may make audits subject to reasonable security and confidentiality requirements.

13. Return and deletion

1. After termination of the services, the Processor shall, at the Controller's choice, delete or return the Controller's personal data unless statutory obligations require continued storage.

2. Statutory retention obligations remain unaffected.
3. The Controller may request proof of proper deletion or return.

14. Third-country processing

1. Processing in a third country shall only take place if the legal requirements of the GDPR are met.
2. Where sub-processors or technical services in third countries are used, the Processor shall ensure that suitable safeguards are in place.

15. Liability

1. Liability of the parties is governed by statutory law and the provisions of the main contract insofar as compatible with data protection law.
2. Mandatory statutory liability provisions, in particular under the GDPR, remain unaffected.

16. Final provisions

1. Amendments and supplements to this agreement must be made in text form unless stricter form requirements apply by law.
 2. If individual provisions of this agreement are or become invalid, the validity of the remaining provisions remains unaffected.
 3. In all other respects, the provisions of the main contract shall apply.
-

Annex 1: Description of processing

1. Subject matter

Provision and operation of xInvoice for the processing, validation, generation, and provision of electronic invoice data and structured invoice documents.

2. Purpose

Technical execution of invoice processing initiated by the Controller and provision of the agreed functions.

3. Type of processing

- collection
- recording
- structuring
- storage
- adaptation
- retrieval
- use
- internal transmission within the agreed system environment
- provision for retrieval
- deletion

4. Categories of data

- names
- contact data
- address data
- invoice data
- service data
- payment data
- tax data

- communication data
- technical metadata

5. Categories of data subjects

- contacts
 - employees
 - customers
 - invoice recipients
 - other natural persons contained in invoice data
-

Annex 2: Technical and organizational measures

The Processor implements appropriate technical and organizational measures, in particular:

- role-based access restrictions
- authentication protection
- secure password processing
- logging of security-relevant events
- separation of customer data
- secured interfaces
- measures to ensure availability and recoverability
- procedures for detecting and handling security incidents
- regular maintenance and updating of systems