Contract for order processing in accordance with Art. 28 GDPR

Version: June 2026

PREAMBLE

There is a contractual relationship between the controller and the processor within the meaning of Art. 28 of Regulation (EU) 2016/679 (General Data Protection Regulation), EU GDPR.
The controller and the processor are aware that the requirements for commissioned data processing are based on the GDPR in its currently valid form.
The controller and the processor agree on the following standard contractual clauses to fulfill the requirements of Art. 28 EU GDPR in order to provide appropriate safeguards (with regard to the protection of privacy and fundamental rights and freedoms of natural persons) for the processing described in Annex 2 of the clauses.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1 Purpose and scope of application

a) These standard contractual clauses (hereinafter referred to as "clauses") are intended to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
b) The controllers and processors listed in Annex I have agreed to these clauses to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725
c) These clauses apply to the processing of personal data in accordance with Annex II.
d) Annexes I to IV are an integral part of the clauses.
e) These clauses are without prejudice to the obligations to which the controller is subject under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725
f) These clauses do not in themselves ensure that the obligations relating to international data transfers under Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 are fulfilled.

Clause 2 Unalterability of the clauses

a) The parties undertake not to amend the clauses except to supplement or update the information provided in the annexes.
b) This does not prevent the parties from including the standard contractual clauses set out in these clauses in a more comprehensive contract and adding further clauses or additional safeguards, provided that these do not directly or indirectly contradict the clauses or restrict the fundamental rights or freedoms of the data subjects.

Clause 3 Interpretation

a) Where terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 are used in these clauses, those terms shall have the same meaning as in that Regulation.
b) These clauses shall be interpreted in the light of the provisions of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.
c) These clauses shall not be interpreted in a manner contrary to the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 or in a manner that restricts the fundamental rights or freedoms of data subjects.

Clause 4 Priority

In the event of any conflict between these clauses and the provisions of any related agreements existing or subsequently entered into or concluded between the parties, these clauses shall prevail.

Clause 5 Tying clause

Not used.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 6 Description of the processing

The details of the processing operations, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the controller, are set out in Annex II.

Clause 7 Obligations of the parties

7.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless it is required to do so under Union law or the law of a Member State to which it is subject. In such a case, the processor shall inform the controller of these legal requirements prior to processing, unless the law in question prohibits this due to an important public interest. The controller may issue further instructions for the entire duration of the processing of personal data. These instructions must always be documented.
b) The processor shall inform the controller immediately if it believes that instructions issued by the controller violate Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or applicable Union or national data protection provisions.

7.2 Earmarking

The processor shall process the personal data only for the specific purpose(s) set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

The data shall only be processed by the processor for the duration specified in Annex II.

7.4 Security of processing

a) The processor shall implement at least the technical and organizational measures listed in Annex III to ensure the security of the Personal Data. This shall include the protection of data against a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of or access to the data, whether accidental or unlawful (hereinafter "Personal Data Breach"). In assessing the appropriate level

of protection, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing and the risks presented to the data subjects.

b) The processor shall grant its personnel access to the personal data subject to processing only to the extent strictly necessary for the performance, management and monitoring of the Contract. The processor shall ensure that the persons authorized to process the personal data received have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.

7.5 Sensitive data

If the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or containing genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning an individual's health, sex life or sexual orientation, or data relating to criminal convictions and offenses (hereinafter "sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance with the clauses

a) The parties must be able to prove compliance with these clauses.

b) The processor shall deal promptly and appropriately with requests from the Controller regarding the processing of data under these Clauses.

c) The processor shall provide the controller with all information necessary to demonstrate compliance with the obligations laid down in these Clauses and arising directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the request of the Controller, the processor shall also allow and contribute to an audit of the processing activities covered by these Clauses at appropriate intervals or where there are indications of non-compliance. When deciding on an inspection or audit, the controller may take into account relevant certifications of the processor.

d) The controller may carry out the audit itself or commission an independent auditor. The audits may include inspections of the processor's premises or physical facilities and shall be carried out with reasonable prior notice where appropriate.

e) The Parties shall make the information referred to in this clause, including the results of audits, available to the competent supervisory authority(ies) upon request.

7.7 Use of subcontracted processors

a) GENERAL WRITTEN AUTHORIZATION: The processor has the Controller's general authorization to engage sub-processors included in an agreed list. The processor shall expressly inform the Controller in writing at least 30 days in advance of any intended changes to this list by adding or replacing sub-processors, thereby giving the Controller sufficient time to object to such changes before engaging the relevant sub-processor(s). The processor shall provide the controller with the necessary information to enable the controller to exercise its right to object.

b) Where the processor engages a sub-processor to carry out certain processing activities (on behalf of the Controller), such engagement shall be by way of a contract which imposes on the sub-processor substantially the same data protection obligations as those applicable to the processor under these Clauses. The processor shall ensure that the Sub-processor complies with the obligations to which the processor is subject under these Clauses and under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall provide the Controller with a copy of any such subcontracting agreement and any subsequent amendments at the Controller's request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the processor may redact the wording of the agreement before providing a copy.

d) The processor shall be fully liable to the Controller for ensuring that the Sub-processor fulfills its obligations under the contract concluded with the processor. The processor shall notify the Controller if the Sub-processor fails to fulfill its contractual obligations.
e) The processor agrees a third-party beneficiary clause with the sub-processor, according to which the controller - in the event that the processor factually or legally ceases to exist or is insolvent - has the right to terminate the subcontracting agreement and instruct the sub-processor to delete or return the personal data.

7.8 International data transfers

a) Any transfer of data by the processor to a third country or an international organization shall take place exclusively on the basis of documented instructions from the controller or to comply with a specific provision under Union law or the law of a Member State to which the processor is subject and shall comply with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
b) The Controller agrees that in cases where the processor uses a sub-processor pursuant to clause 7.7 for the performance of certain processing activities (on behalf of the controller) and where such processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission pursuant to Article 46(2) of Regulation (EU) 2016/679, provided that the conditions for the application of such standard contractual clauses are met.

Clause 8 Support of the person responsible

a) The processor shall inform the controller without undue delay of any request received from the data subject. It shall not respond to the request itself unless it has been authorized to do so by the controller.
b) Taking into account the nature of the processing, the processor shall assist the controller in fulfilling the controller's obligation to respond to requests from data subjects to exercise their rights. In fulfilling its obligations under points (a) and (b), the processor shall follow the instructions of the controller.
c) In addition to the processor's obligation to assist the Controller pursuant to Clause 8(b), the processor shall also assist the Controller in complying with the following obligations, taking into account the nature of the data processing and the information available to the processor:
    1) Obligation to carry out an assessment of the impact of the intended processing operations on the protection of personal data (hereinafter "data protection impact assessment") if a form of processing is likely to result in a high risk to the rights and freedoms of natural persons;
    2) Obligation to consult the competent supervisory authority(ies) prior to processing if a data protection impact assessment indicates that the processing would result in a high risk, unless the controller takes measures to mitigate the risk;
    3) Obligation to ensure that the personal data is accurate and up to date by the processor informing the controller immediately if it discovers that the personal data it is processing is incorrect or out of date;
    4) Obligations under Article 32 of Regulation (EU) 2016/679.
d) The Parties shall set out in Annex III the appropriate technical and organizational measures to assist the Controller by the processor in the application of this Clause and the scope and extent of the assistance required.

Clause 9 Notification of personal data breaches

In the event of a personal data breach, the processor shall cooperate with and assist the Controller to enable the Controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679

or, where applicable, Articles 34 and 35 of Regulation (EU) 2018/1725, taking into account the nature of the processing and the information available to the processor.

9.1 Violation of the protection of data processed by the controller

In the event of a personal data breach in connection with the data processed by the controller, the processor shall assist the controller as follows:

a) in notifying the personal data breach to the competent supervisory authority or authorities without undue delay after the controller becomes aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
b) when obtaining the following information to be included in the controller's notification pursuant to Article 33(3) of Regulation (EU) 2016/679, which shall include at least the following information:
    1) the nature of the personal data, where possible, indicating the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    2) the likely consequences of the personal data breach;
    3) the measures taken or proposed to be taken by the controller to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

If and to the extent that not all such information can be provided at the same time, the initial notification will contain the information available at that time and further information will be provided as soon as it becomes available without undue delay thereafter;

c) in complying with the obligation under Article 34 of Regulation (EU) 2016/679 to notify the data subject without undue delay of a personal data breach where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Violation of the protection of data processed by the processor

In the event of a personal data breach in connection with the data processed by the processor, the processor shall notify the controller without undue delay after becoming aware of the breach. This notification must contain at least the following information:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects concerned and the approximate number of data records concerned);
b) contact details of a contact point where further information on the personal data breach can be obtained;
c) the likely consequences and the measures taken or proposed to address the personal data breach, including measures to mitigate its possible adverse effects.

If and to the extent that not all such information can be provided at the same time, the initial notification will contain the information available at that time and further information will be provided as soon as it becomes available without undue delay thereafter.

The Parties shall specify in Annex III any other information to be provided by the Processor to assist the Controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679].

SECTION III - FINAL PROVISIONS

Clause 10 Breaches of the clauses and termination of the contract

a) Without prejudice to the provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, if the Processor fails to comply with its obligations under these Clauses, the Controller may instruct the

processor to suspend the processing of personal data until it complies with these Clauses or the contract is terminated. The processor shall inform the controller immediately if, for whatever reason, it is unable to comply with these clauses.

b) The controller is entitled to terminate the contract insofar as it concerns the processing of personal data in accordance with these clauses if
   1) the controller has suspended the processing of personal data by the processor in accordance with point (a) and compliance with these clauses has not been restored within a reasonable period and in any event within one month of the suspension;
   2) the processor materially or persistently breaches these clauses or fails to comply with its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725
   3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority(ies) relating to its obligations under these Clauses, Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall be entitled to terminate the Contract insofar as it relates to the Processing of Personal Data under these Clauses if the Controller insists on the fulfillment of its instructions after being informed by the processor that its instructions violate applicable legal requirements under Clause 7.1(b).

d) Upon termination of the contract, the processor shall, at the choice of the controller, erase all personal data processed on behalf of the controller and certify to the controller that this has been done, or return all personal data to the controller and erase existing copies, unless there is an obligation to retain the personal data under Union or Member State law. Until the deletion or return of the data, the processor shall continue to ensure compliance with these clauses

ANNEX I - List of parties

Person responsible

The person responsible in terms of data protection and contact person is the client.

Processor

Processor		Data Protection Officer*		Contact person		
Name	Address	Name	Contact details	Name	Function	Contact details
cloudworx GmbH	Rupert-Mayer-Straße 44, 81379 Munich	Timo Müller	Rupert-Mayer-Straße 44, 81379 Munich E-mail: privacy@ cloudworx.agency	Timo Müller	Managing Director	Rupert-Mayer-Straße 44, 81379 Munich Phone: +49 800 25 68 396 E-mail: info@cloudworx.agency

* **Note:** Cloudworx is not obliged to appoint a data protection officer. If you have any questions about data protection, please contact the management.

ANNEX II - Description of the processing

Note: The processing described below is offered by Cloudworx as a SaaS solution. The actual processing depends on the main contract.

in.bounz in.bounz is a solution for monitoring email inboxes as well as automated and context-related documentation in Salesforce.
Categories of data subjects whose personal data are processed
Customers Employees Suppliers End user
Categories of personal data that are processed
Master data and communication data of customers' Cloudworx accounts. IT system-specific data, e.g. user name, access rights, IP addresses. Customer data processed by the Service under the Customer's e-mail accounts.
Sensitive data processed and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for employees who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures
Sensitive customer data processed by the service under the customer's e-mail accounts. Restrictions and safeguards applied: Strict purpose limitation, access restrictions, access only for Cloudworx employees who have undergone specific training, records of access to data, restrictions on onward transfers.
Type of processing
computation, processing, storage, synchronization and other services as described in the Documentation and initiated by the Customer from time to time.
Purpose(s) for which the personal data are processed on behalf of the controller
Documentation of e-mails. Synchronization with Salesforce. Remote maintenance, service and support.
Duration of processing
According to the term of the main contract.
Processing by (sub)processors. In the case of processing by (sub)processors, the subject matter, type and duration of the processing must also be specified at .
Subcontractor 1: Host Europe GmbH

Object: Storage and backup of customer data. Type: Processing, storage and transmission of customer data. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 2: Scalyr, Inc. Object: SaaS platform for log management and server monitoring. Type: Processing, storage and transmission of log data of the customer. Duration: According to the term of the main contract or the term of the service and support agreement.

out.bounz out.bounz is a solution for the manual, semi-automated and fully automated sending of emails from Salesforce.
Categories of data subjects whose personal data are processed
Customers Employees Suppliers End user
Categories of personal data that are processed
Master data and communication data of customers' Cloudworx accounts. IT system-specific data, e.g. user name, access rights, IP addresses. Customer data processed by the Service under the Customer's e-mail accounts.
Sensitive data processed and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for employees who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures
Sensitive customer data processed by the service under the customer's e-mail accounts. Restrictions and safeguards applied: Strict purpose limitation, access restrictions, access only for Cloudworx employees who have undergone specific training, records of access to data, restrictions on onward transfers.
Type of processing
computation, processing, storage, synchronization and other services as described in the Documentation and initiated by the Customer from time to time.
Purpose(s) for which the personal data are processed on behalf of the controller
Documentation of e-mails. Synchronization with Salesforce. Remote maintenance, service and support.

Duration of processing
According to the term of the main contract.
Processing by (sub)processors. In the case of processing by (sub)processors, the subject matter, nature and duration of the processing must also be stated.
Subcontractor 1: Host Europe GmbH Object: Storage and backup of customer data. Type: Processing, storage and transmission of customer data. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 2: Scalyr, Inc. Object: SaaS platform for log management and server monitoring. Type: Processing, storage and transmission of log data of the customer. Duration: According to the term of the main contract or the term of the service and support agreement.

millio
millio is a banking solution for Salesforce. Transaction data can be stored automatically in Salesforce and payments and direct debits can be executed.
Categories of data subjects whose personal data are processed
Customers Employees Suppliers End user
Categories of personal data that are processed
Master data and communication data of customers' Cloudworx accounts. IT system-specific data, e.g. user name, access rights, IP addresses.
Sensitive data processed and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for employees who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures
Sensitive customer data from the customer's Salesforce system. Restrictions and guarantees applied: Strict purpose limitation, access restrictions, access only for Cloudworx employees who have undergone special training, records of access to the data, restrictions on onward transfers, encryption.
Type of processing
Calculation, processing, storage, synchronization and other services as described in the documentation.

Purpose(s) for which the personal data are processed on behalf of the controller
Remote maintenance, service and support.
Duration of processing
According to the term of the main contract.
Processing by (sub)processors. In the case of processing by (sub)processors, the subject matter, nature and duration of the processing must also be stated.
Subcontractor 1: Host Europe GmbH Object: Storage and backup of customer data. Type: Processing, storage and transmission of customer data. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 2: Scalyr, Inc. Object: SaaS platform for log management and server monitoring. Type: Processing, storage and transmission of log data of the customer. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 3: FinAPI GmbH Object: Interface for retrieving bank data and transferring data to banks. Type: Processing, storage and transmission of the customer's bank data. Duration: According to the term of the main contract or the term of the service and support agreement.

REEDR
REEDR is an AI-based OCR assistant for automated text recognition and the intelligent extraction of structured data from any document - for example invoices, ID documents, vehicle registration documents and many more. REEDR can act either on the basis of AI or on the basis of defined rules.
Categories of data subjects whose personal data are processed
Customers Employees Suppliers End user
Categories of personal data that are processed
Master data and communication data of customers' Cloudworx accounts. IT system-specific data, e.g. user name, access rights, IP addresses.

Sensitive data processed and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for employees who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures
Sensitive customer data from the customer's Salesforce system. Restrictions and guarantees applied: Strict purpose limitation, access restrictions, access only for Cloudworx employees who have undergone special training, records of access to the data, restrictions on onward transfers, encryption.
Type of processing
Calculation, processing, storage, synchronization and other services as described in the documentation.
Purpose(s) for which the personal data are processed on behalf of the controller
Remote maintenance, service and support.
Duration of processing
According to the term of the main contract.
Processing by (sub)processors. In the case of processing by (sub)processors, the subject matter, nature and duration of the processing must also be stated.
Subcontractor 1: Host Europe GmbH Object: Storage and backup of customer data. Type: Processing, storage and transmission of customer data. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 2: Scalyr, Inc. Object: SaaS platform for log management and server monitoring. Type: Processing, storage and transmission of log data of the customer. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 3: Klippa App B.V. Object: Interface for transferring documents transmitted by the end customer for reading and processing with the help of artificial intelligence (AI). Type: Processing, storage and transmission of documents of the end customer. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 4: Hypatos GmbH Object: Interface for transferring documents transmitted by the end customer for reading and processing with the help of artificial intelligence (AI). Type: Processing, storage and transmission of documents of the end customer. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 5: Natif.ai GmbH Object: Interface for transferring documents transmitted by the end customer for reading and processing with the help of artificial intelligence (AI). Type: Processing, storage and transmission of documents of the end customer.

Duration: According to the term of the main contract or the term of the service and support agreement.

integraid integraid is an application that enables secure and fast API integrations in Salesforce. Data from various apps, platforms and systems is integrated via standardized interfaces. This facilitates the automated transfer of relevant information and the smooth exchange of data within a company.
Categories of data subjects whose personal data are processed
Customers Employees Suppliers End user
Categories of personal data that are processed
Master data and communication data of customers' Cloudworx accounts. IT system-specific data, e.g. user name, access rights, IP addresses. Customer data processed by the Service under the Customer's e-mail accounts.
Sensitive data processed and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for employees who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures
Sensitive customer data processed by the service under the customer's e-mail accounts. Restrictions and safeguards applied: Strict purpose limitation, access restrictions, access only for Cloudworx employees who have undergone specific training, records of access to data, restrictions on onward transfers.
Type of processing
computation, processing, storage, synchronization and other services as described in the Documentation and initiated by the Customer from time to time.
Purpose(s) for which the personal data are processed on behalf of the controller
Synchronization with Salesforce. Remote maintenance, service and support.
Duration of processing
According to the term of the main contract.
Processing by (sub)processors. In the case of processing by (sub)processors, the subject matter, nature and duration of the processing must also be stated.
Subcontractor 1: Host Europe GmbH Object: Storage and backup of customer data.

Type: Processing, storage and transmission of customer data. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 2: Scalyr, Inc. Object: SaaS platform for log management and server monitoring. Type: Processing, storage and transmission of log data of the customer. Duration: According to the term of the main contract or the term of the service and support agreement.

XRSF XRSF is an application for processing electronic invoices directly in Salesforce. The tool enables the creation and reading of invoices in various formats, such as XRechnung or ZUGFeRD, within the CRM system. This allows invoice-related data to be processed in a structured way, reduces manual work steps, and makes digital invoicing processes more efficient and compliant with applicable standards.
Categories of data subjects whose personal data are processed
Customers Employees Suppliers End user
Categories of personal data that are processed
Master data and communication data of customers' Cloudworx accounts. IT system-specific data, e.g. user name, access rights, IP addresses. Customer data processed by the Service under the Customer's e-mail accounts.
Sensitive data processed and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for employees who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures
Sensitive customer data that is processed by the service during the creation of documents. Restrictions and safeguards applied: Strict purpose limitation, access restrictions, access only for Cloudworx employees who have undergone specific training, records of access to data, restrictions on onward transfers.
Type of processing
computation, processing, storage, synchronization and other services as described in the Documentation and initiated by the Customer from time to time.
Purpose(s) for which the personal data are processed on behalf of the controller
Synchronization with Salesforce. Remote maintenance, service and support.

Duration of processing
According to the term of the main contract.
Processing by (sub)processors. In the case of processing by (sub)processors, the subject matter, nature and duration of the processing must also be stated.
Subcontractor 1: Host Europe GmbH Object: Provision of cloud infrastructure for the temporary processing and caching of customer data for the creation of electronic documents. Type: Processing, temporary storage, and transmission of the customer's data. The processing is carried out exclusively for the technical provision of document creation within XRSF. Duration: In accordance with the term of the main agreement or the term of the service and support agreement. Temporarily cached data is processed only for the period required to create and provide the respective documents and is subsequently deleted in accordance with the defined deletion processes.
Subcontractor 2: Scalyr, Inc. Object: SaaS platform for log management and server monitoring. Type: Processing, storage and transmission of log data of the customer. Duration: According to the term of the main contract or the term of the service and support agreement.
Subcontractor 3: Amazon Web Services EMEA SARL Object: Provision of cloud infrastructure for the temporary processing and caching of customer data for the creation of electronic documents. Type: Processing, temporary storage, caching, and transmission of the customer's data on server infrastructure in the AWS Region Europe (Frankfurt). The processing is carried out exclusively for the technical provision of document creation within XRSF. Duration: In accordance with the term of the main agreement or the term of the service and support agreement. Temporarily cached data is processed only for the period required to create and provide the respective documents and is subsequently deleted in accordance with the defined deletion processes.

ANNEX III - Technical and organizational measures, including to ensure the security of data

Object

The subject of this annex is the definition of technical and organizational measures to ensure the protection of personal data.

According to Art. 32 GDPR, when processing personal data, it must be ensured that appropriate technical and organizational measures are in place and complied with to ensure the confidentiality, integrity, availability, resilience and recoverability of the data. The obligation of the contractor to take appropriate measures to protect personal data only extends, in accordance with Art. 32 para. 1 GDPR, to measures whose cost is proportionate to the intended purpose of protection. Proof must be provided of the technical and organizational measures implemented.

This document summarizes the technical and organizational measures implemented by the Contractor. It applies to all information processing systems and networks, documents and information of the contractor with which personal data is collected, processed, used and stored. It applies both to data in paper form and to data that is processed digitally.

1. General information

cloudworx GmbH has ensured that

- a written or electronic record of processing activities is kept in accordance with Art. 30 (2) GDPR,
- a data protection management system is in place that meets the requirements of the GDPR
- a data protection officer is appointed to ensure compliance with data protection requirements,
- employees are informed about the requirements of data protection and the technical and organizational measures to be taken through regular training,
- the employees involved in the processing of personal data have been obliged to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality,
- a process for reporting personal data breaches in accordance with Art. 33 GDPR has been introduced.

2. Measures for pseudonymization and encryption pursuant to Art. 32 para. 1 lit. a) GDPR

- Stored data on stationary or mobile storage media of cloudworx GmbH (Data at Rest), such as office PCs, notebooks, tablets and external hard disks, are encrypted according to the state of the art.
- Data stored with cloud service providers (Data in Motion) is also encrypted according to the state of the art.
- Data in transit, e.g. in the cloudworx network or between cloud services, is encrypted according to the state of the art.
- The WLAN of cloudworx GmbH is encrypted according to the state of the art.

- When communicating with the cloudworx GmbH website, the transmitted data is encrypted using state-of-the-art transport encryption.

3. Measures to safeguard the confidentiality, integrity, availability and resilience of systems and services pursuant to Art. 32 (1) (b) GDPR

Access control

Access" refers to the physical access of persons to rooms and buildings in which IT systems are operated and/or used. This includes, for example, data centers in which web servers, application servers, databases and storage systems are operated and rooms in which infrastructure components for the operation of networks and the associated cabling are located. This also includes offices or other workspaces where employees use the PC systems.

The aim of access control is to prevent unauthorized access to rooms or unauthorized use of IT systems in or with which personal data is processed or used.

- The **business premises** are secured against unauthorized access. The doors of the business premises have security locks. Keys are issued in accordance with a key policy, which also specifies the circumstances under which the keys must be returned. There is a record of the keys issued.
- **There are no IT infrastructure rooms on** the business premises in which cloudworx GmbH operates its central IT systems (servers, storage) or network infrastructure components.
- Personal data is processed by cloud service providers whose services were checked for GDPR compliance before they were commissioned. **Contracts for order processing in accordance with Art. 28 GDPR** have been agreed with all providers. Access to these rooms is only permitted to specially authorized persons in accordance with the regulations of the cloud service providers. The access regulations agreed there have been checked or are documented by certifications. There is a right to audit.
- The **doors** are secured by electronic locks that are protected by an automatic access control system in combination with electronic badges.
- **Visitors** may only enter the business premises when accompanied by a cloudworx employee.
- **External service providers** who are present on the business premises outside of business hours, such as cleaning staff, are carefully selected.

Access control

Access control ensures that an IT system is only used by authorized users or only communicates with other authorized IT systems. Access control also includes preventing unauthorized access via external interfaces, such as Internet connections.

The aim of access control is to prevent unauthorized persons from using IT systems that are used to process personal data.

- **Different** passwords are used for **different applications and services**. The passwords are managed in password managers in accordance with the state of the art. Where supported, login to online services is carried out using two-factor authentication.
- **Passwords** are tied to natural persons and may not be passed on.

- Passwords are assigned in accordance with a **password policy** based on current standards, which is regularly reviewed and updated if necessary.
- **Compromised passwords** must be changed immediately.
- **Preset passwords, temporary passwords, passwords in the delivery state** and automatically assigned passwords for hardware and software must be changed immediately.
- Accounts assigned to individual employees must be deactivated immediately after their departure.
- If the application in question allows such a configuration, frequent failed login attempts should lead to time **blocks**.

Access control

Access control is the needs-based planning, control and monitoring of access to IT resources. Key aspects of access control are an appropriate authorization concept for assigning, changing and withdrawing access rights, as well as monitoring and logging these.

The aim of access control is to ensure that authorized users can only access the approved data.

- When assigning user rights and program authorizations, it is ensured that the authorized persons only receive the authorizations required to complete their tasks (**need-to-know principle**). The assignment is based on an **authorization concept** whose roles and rights are regularly reviewed and adjusted. The assigned roles and the assigned rights are regularly reviewed and adjusted if necessary.
- **Administrator rights** are only assigned to selected employees where necessary. Login with administrator rights is only possible for the installation of software, for configuration changes and for the operation of customer services.
- **External service providers** do not have access to cloudworx IT systems or telecommunications equipment. If service providers fulfill support tasks, e.g. 3rd level support, access is only granted within the scope of supervised support sessions.
- To prevent unauthorized access, **workstations** are locked when leaving the room. An automatic screen lock is activated for the workstations. If required, the screen lock can also be activated manually.
- The computer screens are positioned in such a way that the **screen content** is protected from prying eyes.
- Unused **network ports** are deactivated.
- A **deletion concept** is in place. Data carriers are deleted according to the specifications of DIN 66399. If files or data carriers are destroyed by cloudworx or a contracted service provider and are physically destroyed in the process, they are destroyed in accordance with the requirements of DIN 66399.

Integrity

Integrity is the assurance of the correctness (integrity) of data and the correct functioning of IT systems.

The aim of integrity is to ensure the correctness of the data and the correct functioning of the IT system

- The entire cloudworx GmbH network is protected by a **firewall** that is configured and regularly updated in line with requirements.
- All end devices are protected by an **antivirus program** whose virus signatures are updated regularly. Data carriers and services that enable the transfer of files from third parties, e.g. e-mail attachments, are

monitored. Received files are checked before they are opened.

- Received e-mails are checked for **spam and malware**.
- Internet access is provided for guests via a separate, dedicated **guest WLAN**.
- **Private employee devices** are not used for the processing of customers' personal data.
- The operating systems used on the end devices are supported by the manufacturer. The **regular updates** provided by the manufacturer are installed. The security updates provided by the manufacturers (especially for antivirus programs, Office applications and central IT systems such as firewalls, routers, etc.) are regularly checked and installed.
- Documents provided by external sources are checked for **malware** before being opened. Only checked and digitally signed macros are activated in Office applications, provided this is technically possible and the other systems and software can be used without restrictions.
- Employees are regularly trained and sensitized to an appropriate extent on issues of IT security and the security of personal data processing. In particular, they are informed about the risks posed by external content, such as unchecked opening.

Availability

Availability refers to the probability that an IT system or service will be in a functional state at a given time.

The aim of availability is to ensure that a system or service is available to the authorized person at the intended time and that it functions correctly.

- The **hardware** of cloudworx GmbH is regularly maintained and updated in accordance with the state of the art.
- The IT systems and services of the cloud service providers (servers, storage) are protected against the main environmental and elemental risks (humidity, dust, temperature, fire, water, etc.) and have a redundant infrastructure (electricity, internet).
- Data is **not** stored **locally** on the workstations, but in cloud environments that are backed up.
- During **remote maintenance**, a log is created so that it is possible to trace which changes have been made and who has accessed which data. Remote maintenance is carried out via an encrypted connection.
- To avoid dependencies on the availability of system components or IT services, cloudworx relies on open standards that can be obtained from several manufacturers or cloud service providers (avoiding login effects).

Resilience

Resilience is the ability of an IT system or service to return to its original state despite massive external or internal disruptions. A technical system is described as resilient if the system continues to perform and maintain system operation despite an internal or external disruption.

The aim of resilience is to maintain functionality in to be able to properly carry out the processing of personal data as intended.

- cloudworx GmbH ensures the resilience of IT services with the help of a SaaS solution for log management and server monitoring.

- Cloud services are used to ensure the performance of IT services, which distribute the work across a larger number of servers as the load increases.

4. Measures for the rapid restoration of the availability of and access to the data in the event of an incident pursuant to Art. 32 (1) (c) GDPR

Restoring availability and access to data refers to the recovery of original data from a backup copy after data loss, as well as the detection of incorrectly transferred data units and their recovery in a broader sense.

The aim of recovery is to make the original data available so that the processing of personal data can take place properly as intended.

- cloudworx GmbH has created an emergency concept that defines who initiates measures to restore IT services and under what circumstances. The information required for this, such as access data, passwords, authentication information, contact persons and contact details, is documented and stored securely.
- cloudworx GmbH has created and implemented a backup concept. The backup concept includes
  - the responsibility for the backup,
  - that the backup includes all data,
  - that the backup is carried out according to the so-called 3-2-1 rule,
  - The backup is regularly checked for completeness, correctness and recoverability.
- The backup media and the data transmission path are encrypted according to the state of the art.

5. Control of the aforementioned measures pursuant to Art. 32 para. 1 lit. d) GDPR

- cloudworx GmbH regularly reviews the measures for compliance and effectiveness, usually annually or if there is a specific reason to do so.
- cloudworx GmbH has created documentation of the IT infrastructure, including a network plan. The IT documentation is reviewed regularly, usually annually, or if there is a specific reason, and updated if necessary.

Annex IV - The controller has authorized the use of the following sub-processors:

Sub-processors		Contact person			Processing
Name	Address	Name	Function	Contact details	Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are authorized).
salesforce.com, inc.	The Landmark @ One Market Street, San Francisco, CA 94105, USA	Salesforce Data Protection Officer (Salesforce Privacy Team) 415 Mission St, 3rd Floor San Francisco, CA 94105, USA		Web service: www.salesforce.com/form/other/privacy-request/ E-mail: privacy@salesforce.com Phone: 1-844-287-7147	Provision of a SaaS solution for project management.
Host Europe GmbH	Hansestrasse 111 51149 Cologne, Germany	Attorney Dr. Karsten Kinast	Data protection officer	E-Mail: mail@kinast.eu Phone: +49 221 222183-0	Storage and backup of customer data.
Scalyr, Inc.	2929 Campus Drive, Suite 200, San Mateo California 94403, USA	Katja Hauser	Data Protection Manager	E-mail: privacy@teamviewer.com	Operation of a SaaS solution for log management and server monitoring.
Twilio Ireland Limited,	25-28 North Wall Quay Dublin 1, Ireland	Twilio Privacy Team		E-mail: privacy@twilio.com	Provision of a service for the transmission of short messages.
finAPI GmbH	Adams-Lehmann-Str. 44 80797 Munich, Germany	finAPI GmbH For the attention of the Data Protection Department Adams-Lehmann-Str. 44 80797 Munich, Germany		E-Mail: Data protection @finapi.io	Provision of an interface for the transmission of financial information.
Google LLC	1600	Google LLC		Phone: +1 650	Provision of a cloud-

	Amphitheatre Parkway Mountain View, CA 94043, USA	Attn: Data Protection 1600 Amphitheatre Pkwy Mountain View CA 94043 United States of America	253 0000	based solution for communication and collaboration as well as associated apps for creating text documents, spreadsheets and presentations (Google Workspace).
Dropbox, Inc.	333 Brannan Street, San Francisco, CA 94107, USA		https://www.dropbox.com	Provision of a cloud service for the storage and exchange of data.
Spanning Cloud Apps, LLC	501 Congress Ave, Ste 200, Austin, TX 78701, USA		E-mail: privacy @spanning.com	Provision of a cloud service for backing up and restoring data.
Klippa App B.V.	Laan Corpus Den Hoorn 1 9728 JM Groningen The Netherlands		Phone: +44 330 828 0642 E-mail: support@klippa.com	Provision of interfaces for processing documents for reading with the help of artificial intelligence (AI).
Hypatos GmbH	Hypatos GmbH ,c/o Unicorn Workspaces Am Neuen Markt 9 E-F 14467 Potsdam Germany	Proliance GmbH / www.datenschutzexperte.de Data Protection Officer Leopoldstr. 21 80802 Munich data protection officer @datenschutzexperte.de	Phone: +49 (0) 302 09 97 00 info@hypatos.ai	Provision of interfaces for processing documents for reading with the help of artificial intelligence (AI).
Natif.ai GmbH	Campus Starter Center Building A1 1 66123 Saarbrücken Germany	natif.ai GmbH Managing director: Johannes Korves Campus Starter Center Building A1 1 66123 Saarbrücken Germany	E-Mail: contact@natif.ai	Provision of interfaces for processing documents for reading with the help of artificial intelligence (AI).
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855	Data Protection Officer / AWS Privacy Team	Email: aws-EU-privacy@amazon.com	Provision of cloud infrastructure for the temporary processing and caching of

	Luxembourg, Luxembourg			customer data for the creation of electronic documents. The processing takes place in the AWS Region Europe (Frankfurt) on server infrastructure in Germany. AWS's responsibility is limited to the operation and provision of the required cloud infrastructure.