

Contract for commissioned processing pursuant to Art. 28 DS-GVO

Preamble

A contractual relationship exists between the controller and the processor within the meaning of Article 28 of Regulation (EU) 2016/679 (General Data Protection Regulation), EU-DSGVO.

The Controller and the Processor are aware that the requirements for commissioned data processing are governed by the Data Protection Regulation in its currently valid form.

The Controller and the Processor agree to the following standard contractual clauses to meet the requirements of Article 28 of the EU GDPR in order to provide adequate safeguards (in relation 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

- (a) These Standard Contractual Clauses ("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 27th April 2016 on the protection of individuals with regard to the processing of personal data, 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 as set out in Annex II.
- (d) Annexes I to IV form 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 compliance with the obligations relating to international data transfers under Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 Unamendability of the Clauses

- a) The Parties undertake not to amend the Clauses except to supplement or update the information specified in the Annexes.
- b) This shall not prevent the parties from incorporating the standard contractual clauses set out in these clauses into a more comprehensive contract and from adding further clauses or additional

guarantees, provided that these do not directly or indirectly conflict with the clauses or interfere with 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 or Regulation (EU) 2018/1725.
- (c) These clauses shall not be interpreted in a way that is contrary to the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, or that affects the fundamental rights or freedoms of data subjects.

Clause 4 Precedence

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 the documented instructions of the controller, unless it is obliged to process under Union law or the law of a Member State to which it is subject. In such a case, the processor shall notify the controller of those legal requirements prior to the processing, unless the law in question prohibits it on grounds of important public interest. The controller may give further instructions throughout the processing of personal data. These instructions shall always be documented.
- (b) The processor shall inform the controller without undue delay if it considers that instructions given by the controller infringe Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or applicable Union or Member State data protection law.

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 be processed by the processor only for the period specified in Annex II.

7.4 Security of processing

- (a) The processor shall implement at least the technical and organisational measures set out in Annex III to ensure the security of the personal data. This includes the protection of the data against a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of or access to the data, whether accidental or unlawful (hereinafter a personal data breach). In assessing the appropriate level of protection, the Parties shall have due regard to the state of the art, the costs of implementation, the nature, scope, circumstances and purposes of the processing, and the risks involved for the data subjects.
- (b) The Processor shall only grant its Personnel access to the Personal Data subject to the Processing to the extent strictly necessary for the performance, management and supervision of the Contract. The Processor shall ensure that the persons authorised to process the Personal Data received have committed themselves to confidentiality or are subject to an appropriate legal duty of confidentiality.

7.5 Sensitive data

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

7.6 Documentation and compliance with clauses

- a) The parties must be able to demonstrate compliance with these clauses.
- b) The Processor shall deal promptly and reasonably with requests from the Controller in relation to the processing of Data under these Clauses.
- c) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out 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 the audit of the processing activities covered by these clauses at reasonable intervals or where there are indications of non-compliance. When deciding on a review or audit, the controller may take into account relevant certifications of the processor.
- (d) The controller may conduct the audit itself or engage an independent auditor. Audits may include inspections of the Processor's premises or physical facilities and shall be carried out with reasonable advance notice, where appropriate.
- e) The Parties shall make the information referred to in this clause, including the results of audits, available to the relevant supervisory authority(ies) upon request.

7.7 Use of subcontracted processors

- (a) GENERAL WRITTEN AUTHORISATION: The Processor shall have the general authorisation of the Controller 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 that list by adding or replacing Sub-processors, thereby giving the Controller sufficient time to object to those changes before engaging the Sub-processor(s) concerned. 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 substantially the same data protection obligations on the sub-processor 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 upon the Controller's request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Processor may obscure the wording of the agreement before providing a copy.
- (d) The processor shall be fully liable to the controller for the sub-processor's compliance with its obligations under the contract concluded with the processor. The Processor shall notify the Controller if the Sub-processor fails to perform its obligations under the Contract.
- (e) The processor shall agree with the sub-processor on a third party beneficiary clause under which the controller - in the event that the processor ceases to exist factually or legally or is insolvent - has the right to terminate the subcontract 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 organisation shall only be made 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 those 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 those standard contractual clauses are met.

Clause 8 Support of the responsible person

- (a) The processor shall inform the controller without delay of any request received from the data subject. He shall not respond to the request himself unless he has been authorised 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 under Clause 8(b), the Processor shall, taking into account the nature of the Data Processing and the information available to it, also assist the Controller in complying with the following obligations:
- 1) Obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (hereinafter 'data protection impact assessment') where 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 where 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 personal data is accurate and up to date by the processor informing the controller without undue delay if it discovers that the personal data it processes is inaccurate or out of date;
 - 4) Obligations under Article 32 of Regulation (EU) 2016/679.
- (d) The Parties shall specify in Annex III the appropriate technical and organisational measures for the Processor's assistance to the Controller in the application of this Clause and the scope and extent of the assistance required.

Clause 9 Personal data breach notification

In the event of a personal data breach, the Processor shall cooperate with and provide appropriate assistance to 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 relation to 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 the breach, where relevant (unless the personal data breach is unlikely to result in a risk to the personal rights and freedoms of natural persons);
- (b) in obtaining the following information to be included in the notification by the responsible person pursuant to Article 33(3) of Regulation (EU) 2016/679, which information shall include at least the following:
 - 1) the nature of the personal data, where possible, indicating the categories and approximate number of data subjects and the categories and approximate number of personal data sets concerned;
 - 2) the likely consequences of the personal data breach;
 - 3) the measures taken or proposed 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 all such information cannot be provided at the same time, the initial notification shall contain the information available at that time and further information shall be provided thereafter without undue delay as and when it becomes available;

- (c) in complying with the obligation under Article 34 of Regulation (EU) 2016/679 to notify the data subject without undue delay of the personal data breach where that 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 relation to the data processed by the Processor, the Processor shall notify the Controller without undue delay after becoming aware of the breach. This notification shall contain at least the following information:

- (a) a description of the nature of the breach (specifying, if possible, the categories and the approximate number of individuals concerned and the approximate number of data sets 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 remedy the personal data breach, including measures to mitigate its possible adverse effects.

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

The parties shall set out in Annex III any other information to be provided by the processor to assist the controller in fulfilling the controller's 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 immediately inform the controller if, for whatever reason, it is unable to comply with those clauses.
- b) The Controller shall be entitled to terminate the Contract insofar as it relates to the processing of Personal Data pursuant to these Clauses if
 - 1) the controller has suspended the processing of personal data by the processor pursuant to point (a) and compliance with those clauses has not been restored within a reasonable period of time 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) concerning 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 pursuant to these Clauses if the Controller insists on the performance of its instructions after having been notified by the Processor that its instructions are in breach of applicable legal requirements pursuant to 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 under Union or Member State law to retain the personal data. Until the deletion or return of the data, the processor shall continue to ensure compliance with these clauses.

ANNEX I - List of parties

Responsible

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

Processor

Processor		Data Protection Officer*		Contact		
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 Tel.: +49 800 25 68 396 Email: info@cloudworx.agency

* **Note:** cloudworx is not obliged to appoint a data protection officer. For questions regarding data protection, the management is available as a contact person.

ANNEX II - Description of the processing

Notice: 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 processed
Master data and communication data of customers' cloudworx accounts. IT system-specific data, such as user name, access rights, IP addresses. Customer data processed under the Customer's email accounts by the Service.
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 staff who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures
Sensitive customer data processed under the customer's email accounts by the Service. Restrictions and safeguards applied: Strict purpose limitation, access restrictions, access only for cloudworx employees who have completed specific training, records of access to data, restrictions on onward transfers.
Type of processing
Calculation, processing, storage, synchronisation and other services as described in the Documentation and initiated by the Client from time to time.
Purpose(s) for which the personal data are processed on behalf of the controller
Documentation of emails. Synchronisation with Salesforce. Remote maintenance, service and support.
Duration of the 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 shall also be indicated.
Subcontractor 1: Host Europe GmbH

Subject: Storage and backup of customer data.
Type: Processing, storage and transmission of client data.
Duration: According to the term of the main contract or the term of the service and support agreement.

Subcontractor 2: Scalyr, Inc.

Subject: SaaS platform for protocol 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 automatically stored 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 processed

Master data and communication data of customers' cloudworx accounts.
IT system-specific data, such as user name, access rights, IP addresses.
Customer data processed under the Customer's email accounts by the Service.

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 staff 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 safeguards applied: Strict purpose limitation, access restrictions, access only for cloudworx employees who have completed specific training, records of access to data, restrictions on onward transfers, encryption.

Type of processing

Calculation, processing, storage, synchronisation 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 the 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 shall also be indicated.

Subcontractor 1: Host Europe GmbH

Subject: Storage and backup of customer data.

Type: Processing, storage and transmission of client data.

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

Subcontractor 2: Scalyr, Inc.

Subject: SaaS platform for protocol 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

Subject: Interface for retrieving bank data and transmitting data to banks.

Type: Processing, storage and transmission of the Client's bank data.

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

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

Subject

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

Pursuant to Article 32 of the GDPR, when processing personal data, it must be ensured that appropriate technical and organisational measures are in place and complied with to protect the confidentiality, integrity, availability, resilience and recoverability of the data. The obligation of the contractor to take suitable measures to protect the personal data only extends to such measures in accordance with Article 32 (1) of the GDPR, the cost of which is in reasonable proportion to the intended purpose of the protection. Proof of the technical and organisational measures implemented must be kept.

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

1. General

The cloudworx GmbH has ensured that

- a written or electronic register of processing activities is kept in accordance with Art. 30(2) of the GDPR,
- a data protection management system is established 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 organisational measures to be taken through regular training,
- the employees involved in the processing of the personal data have been bound to confidentiality or are subject to an appropriate legal duty of confidentiality,
- a personal data breach notification process is in place in accordance with Art. 33 GDPR.

2. Measures for pseudonymisation and encryption pursuant to Art. 32 para. 1 lit. a) DSGVO

- Stored data on stationary or mobile storage media of cloudworx GmbH (Data at Rest), such as office PCs, notebooks, tablets and external hard drives, are encrypted according to the state of the art.
- Data stored with cloud service providers (Data in Motion), are also encrypted according to the state of the art.
- Data in transmission, 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) lit. b) DSGVO

Access control

"Access" means the physical access of persons to rooms and buildings in which IT systems are operated and/or used. This includes, for example, data centres 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. Also included are offices or other workspaces where employees use the PC systems.

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

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

Access control

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

The aim of access control is to prevent IT systems used to process personal data from being used by unauthorised persons.

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

- Passwords are assigned in accordance with a **password policy that is** based on current standards and **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 individually assigned to individual employees must be deactivated in their entirety immediately after they leave.
- If the application in question allows a configuration to this effect, frequent, failed login attempts should lead to time-out **periods**.

Access control

Access control is the demand-oriented planning, control and monitoring of access to IT resources. Essential points of access control are an appropriate authorisation concept for the allocation, modification and revocation of access rights, as well as its monitoring and logging.

The aim of access control is to ensure that authorised persons can only access the released data.

- When assigning user rights and programme authorisations, it is ensured that the authorised persons only receive the authorisations necessary to complete their tasks (**need to know principle**). The allocation is based on an **authorisation concept** whose roles and rights are regularly reviewed and adjusted. The roles assigned and the rights granted are regularly checked and adjusted if necessary.
- **Administrator rights** are only assigned to selected employees if necessary. Logging on with administrator rights is only possible for the installation of software, for configuration changes and for the operation of the customer services.
- **External service providers do** not have access to IT systems or telecommunication facilities of cloudworx. Insofar as service providers fulfil support tasks, e.g. 3rd level support, access only takes place within the framework of supervised support sessions.
- To prevent unauthorised access, **workstation computers** are locked when leaving the room. An automatic screen lock is activated for the workstation computers. If necessary, the screen lock can also be activated manually.
- The screens of the computers are placed in such a way that the **screen contents are** protected from prying eyes.
- Unused **network ports** are deactivated.
- A **deletion concept** exists. Data carriers are deleted according to the specifications of DIN 66399. If files or data carriers are destroyed by cloudworx or a commissioned service provider and physically destroyed in the process, the destruction is carried out in accordance with the specifications 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 according to requirements and regularly updated.

- All end devices are protected by a **virus protection programme** whose virus signatures are regularly updated. Data carriers and services that enable the transmission 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 staff devices** are not used for the processing of clients' personal data.
- The operating systems used for 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 virus protection programmes, 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 qualified and sensitised to an appropriate extent on issues of IT security and the security of the processing of personal data. In particular, information is provided on the dangers posed by external content, such as unchecked opening.

Availability

Availability refers to the probability that an IT system or service can be found in a functioning state at a given time.

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

- The **hardware** of cloudworx GmbH is regularly maintained and renewed taking into account the state of the art.
- The IT systems and services of the cloud service providers (servers, storage) are protected against the main environmental and natural risks (humidity, dust, temperature, fire, water, etc.) and have a redundant infrastructure (power, internet).
- Data is **not** stored **locally** on the workstations, but in cloud environments that are backed up.
- In the case of **remote maintenance**, a log is created so that it is comprehensible which changes were made and who 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 (avoidance of login effects).

Resilience

Resilience, referred to in the English version of the GDPR as "resilience", is the ability of an IT system or service to return to its initial state despite massive external or internal disruptions. A technical system is called resilient if the system performs and maintains system operation despite an internal or external disruption.

The objective of resilience is to maintain functionality in order 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 to a larger number of servers as the load increases.

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

Restoration of availability and access to data refers to the restoration of original data after a loss of data from a backup copy, as well as the detection of erroneously transferred data units and their restoration 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 specifies who initiates measures to restore IT services under which circumstances. The information required for this, such as access data, passwords, authentication information, contact persons and contact details are documented and securely stored.
- cloudworx GmbH has created and implemented a backup concept. The backup concept includes
 - the responsibility for the backup is regulated,
 - specified that the backup includes all data,
 - that the backup is carried out according to the so-called 3-2-1 rule,
 - specified that 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) DSGVO

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

Annex IV - The responsible person has authorised the use of the following sub-processors:

Sub-processor		Contact person			Processing
Name	Address	Name	Role	Contact information	Description of the processing (including a clear delineation of responsibilities if multiple sub-processors are approved).
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: https://www.salesforce.com/form/other/privacy-request/ Email: privacy@salesforce.com Phone: 1-844-287-7147	Provision of a SaaS solution for project management.
Host Europe GmbH	Hansestrasse 111 51149 Cologne, Germany	RA Dr. Karsten Kinast	Data protection officer	Email: mail@kinast.eu Tel.: +49 221 222183-0	Storage and backup of client data.
Scalyr, Inc.	2929 Campus Drive, Suite 200, San Mateo California 94403, USA	Katja Hauser	Data Protection Manager	Email: 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		Email: rivacy@twilio.com	Provision of a service for the transmission of short messages.
finAPI GmbH	Adams-Lehmann-Str. 44 80797 Munich, Germany	finAPI GmbH zu Hd. Abteilung Datenschutz Adams-Lehmann-Str. 44 80797 Munich, Germany		Email: Datenschutz@finapi.io	Provision of an interface for the transmission of financial information.
Google LLC	1600	Google LLC		Tel.: +1 650	Providing a cloud-based

	Amphitheatre Parkway Mountain View, CA 94043, USA	Attn: Data Protection 1600 Amphitheatre Pkwy Mountain View CA 94043 United States of America	253 0000	communication and collaboration solution and 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/support	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		Email: privacy@spanning.com	Provision of a cloud service for the backup and recovery of data.