Privacy Policy

Application area

This Privacy Policy regards all information that firstcolo GmbH processes in the context of products and services ordered by customers where no alternate, more specific, guidelines apply. Our services include Cloud Services (firstcolo Cloud, firstkube, VMware Cloud, Proxmox Cloud), Managed Services (Managed Hosting, Cloud management, Microsoft Services, Nextcloud, DaaS), Storage Services (Cloud Storage Services, Storage on Demand) and, where applicable, Hardware Services (Dedicated Server) and Colocation & Housing (Colocation, Private Cage).
This Privacy Policy specifies the parties' duties to protect data that results from the General Terms and Conditions of the contractor ("**firstcolo GmbH**," also known as the "**Contractor**") and from the subsequent individual contract with the customer (hereinafter the "**Customer**"). The Contractor shall provide the Customer with the services described in further detail in the existing service agreement, on the basis of that agreement. The provisions of this Policy take precedence over the provisions of the service agreement and any other agreements between the parties, if and to the extent that this is necessary in order to comply with applicable data privacy laws.
This Policy applies to all activities during which the data processor, employees of the processor, or recipients contracted by the processor according to this Policy obtain access to personal data of the Customer and/or process (in particular collect, save, and use) such personal data for the Customer on the Customer's behalf.
Any duties of the data processor based on statutory provisions or on official or judicial orders remain unaffected by this Policy.

Subject, specification and term of the data processing

Following the conclusion of a framework or supplementary contract, the processor shall in some circumstances process personal data for the Customer in the sense of *Art. 4 No. 2* and Art. 28 GDPR on the basis of this Policy. The framework contract defines the subject and term of the data processing.

Geographic scope

The contractually agreed service shall be provided exclusively within a member state of the European union or a signatory to the Agreement on the European Economic Area. Any outsourcing of the service or parts thereof to a third country must be approved by the Customer in advance, and shall take place only if the special conditions of Art. 44 et seqq. GDPR are fulfilled (e.g. adequacy decision by the Commission, standard data protection clauses, approved codes of conduct).

Type of data

The type of data, the type and purpose of processing, and the categories of data subjects are dependent upon the services booked in the framework or supplementary contract.

General

For invoicing and processing of Customer tickets, a Customer account shall be established with the necessary master data and payment information. Additional joint user accounts can be created independently by the main account user.
This data, as well as information provided through Customer tickets, shall be saved and anonymized by us according to the statutory provisions.

Cloud Services and Storage Services

The type of data includes all content that the Customer saves in the provided services. firstcolo GmbH does not access the data directly. Indirect processing of personal data may take place through:

- Log evaluation of API endpoints to secure the systems, identify attacks, and ensure correct functionality of the endpoints
- Backups of data in the OpenStack environment so it can be restored in the event of a system failure

- Log evaluation of the firewalls and web proxy to secure the systems, identify attacks, and ensure correct functionality of the firewalls
- Log evaluation of the DNS servers to secure the systems, identify attacks, and ensure correct functionality of the DNS servers

At the end of the contract term, all remaining data regarding the Customer shall be permanently deleted.

Managed Services
The type of data includes all content that the Customer saves in the provided services. firstcolo GmbH does not have any direct access to the data. Indirect processing of personal data may take place through:

- Logging system changes. Changes in certain systems are logged to ensure traceability later on. Data in the logs such as user ID / IP address can potentially be used to identify natural persons.
- Backups of data in the managed environment so it can be restored in the event of a system failure.
- Provision of virtual server solutions. There is no direct processing of Customer data, but in the context of creating and maintaining the administrative systems used to rent servers to Customers, we have a high level of direct influence on the availability of the information stored on these servers.
- Provision of DDoS solutions. There is no direct processing of Customer data, but in the context of providing protection against DDoS attacks, it may be necessary to restrict the availability of individual Customer systems in order to ensure the availability of many systems.

At the end of the contract term, all remaining data regarding the Customer shall be permanently deleted.

Colocation & Housing and Hardware Services
These services do not give firstcolo GmbH the ability to access Customer data or to influence processing systems. Under no circumstances shall firstcolo GmbH's employees attempt to gain independent access to the Customer's servers or rental servers. If defective data carriers are replaced in rental servers, or if rental servers are returned after the end of the contract term, the data carriers shall be wiped and destroyed, if applicable. No data processing takes place in the sense of the GDPR.
If a Customer explicitly requests support from specialized staff to perform work at the system level, this represents an expansion of the services concluded up to that point; within the scope of these activities, the information about "Managed Services" applies.

Rights and duties of the Contractor

Compliance with applicable law
The Contractor's duties during processing are based on this Policy and on applicable law. In particular, applicable law includes the German Federal Data Protection Act ("**BDSG**") and the General Data Protection Regulation ("**GDPR**").

Processing only according to instructions
The Contractor shall process the Customer's personal data only in order to fulfill the correspondingly contracted services, or according to additional documented instructions from the Contractor (Customer ticket).

Person authorized to give instructions
Fundamentally, all employees of the Contractor are authorized to give instructions if they have access to the processor's ticket system.
Fundamentally, all employees of the processor are authorized to receive instructions.

Confidentiality duty
The processor shall obligate all persons engaged to process the personal data to maintain confidentiality where they are not subject to a statutory secrecy obligation. The confidentiality/secrecy duty shall continue to apply even after the end of the contract.

Support for protecting data subjects' rights
Where possible, the processor shall support the Customer in its duties by providing suitable technical and organizational measures with regard to processing requests to exercise the data subjects' rights named in Chapter III of the GDPR. If a data subject contacts the processor directly to assert data subject rights with regard to data that the processor is processing on behalf of the Customer, the processor shall forward this request to the Customer without delay. The processor shall not be liable if the data subject's request is not answered, not answered correctly, or not answered in a timely manner by the Customer.

Support for complying with Art. 32 - 36 GDPR
With consideration for the type of processing and the information available to the processor, the processor shall to the best of its ability support the Customer with suitable technical and organizational measures to comply with the duties named in Art. 32-36 GDPR, especially with regard to the security of processing, the data protection impact assessment, and consultation with supervisory authorities.

Appointing a data protection officer
The processor shall appoint a data protection officer. In the event of any questions about data protection, the Customer can contact the data protection officer directly. The officer's contact information is published on the processor's website.

Reporting breaches of personal data protections
In the event of a breach of personal data protections, the processor shall work with the Customer and provide corresponding support so that the Customer can fulfill its duties pursuant to Articles 33 and 34 of the GDPR; the processor shall take into account the type of processing and the information available.

Technical and organizational measures

Basic principle
Within its area of responsibility, the processor shall create an internal organization system that meets the special requirements of data protection. The processor shall take technical and organizational measures to appropriately protect the Customer's data, in compliance with the requirements of the General Data Protection Regulation (Art. 32 GDPR).

Design
The processor shall implement technical and organizational measures that consistently ensure the confidentiality, integrity, availability, and robustness of systems and services in conjunction with the processing. The Customer is aware of these technical and organizational measures, and is responsible for ensuring that these provide an appropriate level of protection for the risks associated with the data to be processed.

Changes
The technical and organizational measures are subject to technical progress and further development. In this regard, the processor is permitted to implement suitable alternative measures.

Any significant changes shall be documented. The processor reserves the right to change the implemented security measures, but must ensure that the contractually agreed protection level is met.

Approval by the Customer
When the Customer accepts the service contract, the processor's measures documented in the "**Technical and organizational measures**" shall become the basis for the provision of service.

Subcontractors

General written permission

The processor has general permission from the Customer to engage sub-processors as named in this Privacy Policy. The processor shall explicitly inform the Customer at least four weeks in advance, in text form, about all intended changes to this list (addition or removal of sub-processors), thereby giving the Customer sufficient time to raise an objection to these changes before the relevant sub-processor(s) is/are engaged. The processor shall provide the Customer with the information necessary for the Customer to exercise this objection right.

Subcontractors engaged at the time of conclusion of contract
Subcontractors have been engaged only for the following services:

Managed Services
croit GmbH – Provides support for debugging technical problems if necessary, and is given access to the CEPH infrastructure only in the context of this work (and only for the duration of the work). There is no direct access to the Customer's data.

Careful selection of subcontractors
The processor shall choose subcontractors carefully and shall ensure, before engaging the subcontractors, that these can comply with the contract concluded between the parties and with the statutory requirements of the GDPR.

Subcontractor commitments
The processor shall design contracts with subcontractors such that they fulfill the requirements of the applicable data protection laws and this Policy. In particular, subcontractors shall agree not to hire additional or different subcontractors if there is no commitment for them to comply with the Policy. The processor shall monitor whether sufficient guarantees are provided to ensure that the suitable technical and organizational measures are carried out such that the applicable data protection laws and this Policy are followed.

Ancillary services
Services that are not considered subcontractor relationships in the sense of the above provisions are third-party services that the processor utilizes as an ancillary service to support contract execution. This includes, for example, telecommunication services, cleaning services, auditing services, and in some circumstances also maintenance services. However, in order to guarantee the protection and security of the Customer's data and to ensure confidentiality even where third-party ancillary services are utilized, the processor shall make legally compliant and appropriate contractual agreements as well as implementing control measures.

Rights and duties of the Customer

Compliance with the GDPR
In the context of implementing this Policy, the Customer is responsible for ensuring compliance with the requirements of the GDPR and other statutory data protection regulations, and particularly for ensuring that the data processing is legal and that the statutory rights of data subjects are granted with regard to their personal data.

Duty to supply information

The Customer shall inform the processor without delay and fully if it finds any faults or irregularities in the ordered results with regard to data protection provisions.

Inspections

If inspections by the Customer or an auditor engaged by the Customer become necessary in individual cases, these shall be performed during normal business hours without disrupting the course of business and with appropriate advance notice. The processor may make this inspection contingent upon appropriate advance notice as well as upon the signing of a confidentiality agreement regarding the data of other controllers and the established technical and organizational measures. If the auditor engaged by the Customer is a competitor of the processor, the processor has the right to object to this auditor.

Reservation of rights

In relation to the processor, the Customer reserves all rights to the personal data and other data processed on the basis of this Policy, to any provided data carriers, and to any documents provided in order to enable fulfillment of this Policy. Moreover, the Customer has exclusive control over the data.

Liability

The Customer and the processor shall be liable toward data subjects according to the provision specified in Art. 82 GDPR. However, the processor shall be liable only for damages caused within its area of responsibility and not for damages that can clearly be attributed to the Customer. The Customer shall be fully liable for damages that can clearly be attributed to the Customer.

Final provisions

Validity

If individual provisions of this Policy are ineffective or invalid in whole or in part, or if they become ineffective or invalid in whole or in part due to a change in the legal situation or due to a supreme court decision or by some other means, or if this Policy contains gaps, the parties hereby agree that the remaining provisions of this Policy shall remain unaffected and valid. In this event, the parties hereby agree to establish a provision in place of the invalid provision, in good faith, that as closely as possible approximates the invalid provision and that the parties would have established if they had been aware of or foreseen the ineffectiveness or invalidity at the time when the Policy was concluded. The same applies correspondingly if this Policy contains a gap.

Supplementary provisions

If individual points in this Policy contradict the General Terms and Conditions of the processor, the Policy shall take legal precedence over these documents. If the Policy lacks provisions that are found in the General Terms and Conditions, these supplementary provisions shall apply in addition to this Policy.

Applicable law and place of jurisdiction

German law applies exclusively. The place of jurisdiction for all disputes arising from or in conjunction with this Policy is the Customer’s registered place of business.