Data Processing Agreement

in Accordance with Article 28 of the GDPR

between

Mechtel GmbH
Fritz-Riedel-Strasse 16 16
10407 Berlin
GERMANY
K1009678524
- Controller within the meaning of the GDPR, hereinafter referred to as the Client -

and

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Germany
- Processor within the meaning of the GDPR, hereinafter referred to as the Supplier -

Version	Date	Notes
1.0	25.05.2018	Initial creation of the DPA
1.1	10.02.2025	Text clarified; no substantive changes
1.2	16.02.2026	Addition of TOMs

Introduction

This Data Processing Agreement (DPA) defines the data protection obligations of the contractual parties, and the data processing that takes place as a result of the Client's main contract. The DPA applies to all activities relevant to the main contract and in which employees of the Supplier or third parties commissioned by the Supplier process personal data on behalf of the Client.

§ 1 Subject matter and duration of the Agreement

(1) This Data Processing Agreement (DPA) defines the data protection obligations of the contractual parties, and the data processing that takes place as a result of the Client's main contract. The main contract consists of the product description and our terms and conditions.

(2) The Processor will process personal data on behalf of the Client in accordance with Art. 4 No. 2 GDPR under this Agreement.

(3) Within the scope of this DPA, the Client is solely responsible for compliance with data protection regulations. In particular, the Client will ensure that both the transfer of data to the Supplier and its data processing are lawful. The Client is considered the "Controller" within the scope of Art. 4 No. 7 GDPR.

(4) This DPA is dependent on the existence of a main contractual relationship in accordance with § 1 (1) of this Agreement (for the duration of data processing). The cancellation or other termination of the main contractual relationship will simultaneously terminate this DPA.
The right to extraordinary termination of this DPA and the right to exercise statutory rights of withdrawal remain unaffected.

§ 2 Object, nature, and purpose of the collection, processing or use of data as well as the Data Subjects

The object, nature and purpose of any possible collection, processing, or use of per- sonal data, the nature of data, and the Data Subjects will be described to the Supplier by the Client in accordance with Appendix 1 of this document as completed by the Client, insofar as this is not governed by the contractual relationships described in the content of § 1 of this DPA.

§ 3 Third country data transfer

(1) The provision of the contractually agreed upon data processing will occur exclusively in a member state of the European Union or in another member state party to the Agreement on the European Economic Area.

(2) Any transfer to a third country will require the prior consent of the Client and may only occur if the special conditions defined in Articles 44 et seq. of the GDPR are fulfilled.

(3) The Supplier will inform the Client in advance which third country or countries are involved and how the appropriate level of protection within the scope of Art.

44 et seq. GDPR is ensured for the data processing there. The Supplier agrees to provide the Client with evidence of the implemented guarantees upon request.

(4) The appropriate level of protection for data processing in the third country is ensured by one of the following measures:
- Adequacy decision of the Commission (Art. 45 No. 3 GDPR),
- Binding internal data protection rules, including additional safeguards where appropriate (Art. 46 No. 2 lit. b GDPR in conjunction with Art. 47 GDPR),
- Appropriately modified standard data protection clauses, including additional safeguards where applicable (Art. 46 (2) (c) and (d) GDPR).
- Approved codes of conduct (Art. 46 No. 2 clause e in conjunction with Art. 40 GDPR),
- Approved certification mechanism (Art. 46 No. 2 clause f in conjunction with 42 GDPR),
- Another manner provided for in Art. 44 et seq. GDPR, of which the Supplier will inform the Client in advance.

§ 4 Technical and Organizational Measures

(1) The Supplier will implement Technical and Organizational Measures (TOMs) that ensure adequate protection of the Client's data and comply with the requirements of the General Data Protection Regulation (Art. 32 GDPR). In doing so, the Supplier will specifically assess the risk to the rights and freedoms of the Data Subjects and will take appropriate measures to ensure that the confidentiality, integrity, availability and resilience of the systems and services in connection with the data processing are constantly guaranteed.

(2) The Technical and Organizational Measures will be subject to technical progress and further development. In this respect, the Supplier is permitted to implement alternative adequate measures. The safety level of the measures specified in Appendix 2 of this DPA must not be compromised. The Supplier must document any substantial changes.

(3) Before the commencement of data processing, the Supplier shall document the execution of the necessary Technical and Organizational Measures defined in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the Agreement or Contract.

(4) Documentation for the relevant Technical and Organizational Measures can be found in Appendix 2 of this DPA. The most current version of the Technical and Organizational Measures can be found at https://www.hetzner.com/AV/TOM_en.pdf.

§ 5 Quality assurance and other duties of the Supplier

The Supplier confirms that they are aware of the relevant general data protection regulations. They agree to follow the principles of proper data processing. In this respect, the Supplier guarantees in particular compliance with the following requirements:

1. Appointed Data Protection Officer

The Supplier has an appointed data protection officer. They can be contacted at any time at data-protection@hetzner.com or +49 9831 505-216. There is additional information on the Supplier's website at: https://www.hetzner.com/unternehmen/zertifizierung/.

2. Maintaining confidentiality

The Supplier entrusts only such employees with the data processing defined in this agreement who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. This confidentiality must continue even after the main contract has ended.

3. Implementation of Technical and Organizational Measures

The Supplier agrees to implement and follow all necessary Technical and Organizational Measures relevant to this DPA. See also § 4 of this DPA.

4. Cooperation with supervisory authority

The Supplier and the Client will, upon request, cooperate with the supervisory authority in the performance of their duties.

The Supplier will inform the Client immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this DPA. This will not apply if the Party that is required to share said information is obliged to maintain secrecy about the disclosure due to statutory regulations and/or an official court order. This will also not apply if the party that is required to share said information is otherwise required, under threat of punishment, to maintain confidentiality due to an official government order or court order.

5. Support in regulatory procedures

Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offense or criminal procedure, a liability claim of a Data Subject or a third party or any other claim in connection with the processing of the Agreement or Contract by the Supplier, the Supplier will make every effort to support the Client to the best of their ability.

6. Regular reviews of TOMs

The Supplier will regularly monitor the internal processes as well as the effectiveness of the Technical and Organizational Measures (TOMs) to ensure that the processing in their area of responsibility is executed in accordance with the requirements of the applicable data protection law and that the rights of the Data Subjects are protected.

7. Support for requests from Data Subjects

The Processor shall reasonably assist the Controller in fulfilling requests and claims of Data Subjects pursuant to Chapter III of the GDPR. If a Data Subject contacts the Processor directly in this regard, the Processor shall promptly refer the Data Subject to the Controller and immediately forward the request to the Controller.

8. Reporting data protection violations

The Supplier will inform the Client immediately if the Supplier becomes aware of any violations of the Client's personal data protection. At a minimum, the report must include:

- a description of the nature of the personal data breach, including, where possible, the categories and approximate number of Data Subjects, the affected categories, and the approximate number of affected personal data records;
- the name and contact details of the Data Protection Officer or other contact people for further information;
- a description of the likely consequences of the personal data breach;
- a description from the Data Protection Officer about any measures they have already made or plan to make to address the personal data violation, and, where appropriate, any measures to mitigate its possible negative effects.

§ 6 The Client's responsibilities

The Client must inform the Supplier immediately and in full if they discover any errors or irregularities in the results of their processed data.

§ 7 Sub contractual relationships

(1) For the purposes of this DPA, sub contractual relationships are defined as those services which relate directly to the provision of the principal commission. This does not include ancillary services which the Supplier uses, e.g. telecommunications services; postal/transport services; maintenance and user support services; as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.

(2) A sub contractual relationship requiring consent exists if the Supplier commissions other contractors with the processing of personal data agreed to in the Client's main contract. If the Supplier places orders with subcontractors, it is the responsibility of the Supplier to transfer its data protection obligations under this contract to the subcontractor and to make appropriate agreements to ensure that the subcontractor also provides an adequate level of data protection and takes appropriate information security measures.

(3) The Client agrees to the Supplier commissioning further subcontractors. The Supplier agrees to inform the Client in good time and in an appropriate way before they engage a subcontractor or replace one.
The Client has the right to exercise their data protection rights within a reasonable period of 14 days by contacting the Supplier if the Supplier makes such a change. If the Client does not object within this period, it will be assumed that the Client agrees to this change. If there is a good reason in the sense of data protection rights that the Client objects to this change, and the Client and the Supplier cannot reach an agreement, the Client will be granted special rights to terminate their main contract.

(4) The period of 14 days can be shorted to a reasonable period if special circumstances occur that make a two-week waiting period unreasonable for the Supplier.

(5) The Client agrees to the Supplier commissioning subcontractors listed in Appendix 3 of this DPA.

§ 8 The Client's inspection rights

(1) The Supplier will ensure that the Client has suitable means to verify to its satisfaction compliance with the responsibilities defined in this DPA. The Supplier agrees to provide the Client with all relevant information upon request, and in particular, to provide evidence of the implementation of the Technical and Organizational Measures.

(2) The Supplier can provide proof of compliance with the responsibilities defined in this DPA in the following forms:

- compliance with the codes of conduct in accordance with Art. 40 GDPR,
- certification using approved certification processes in accordance with Art. 42 GDPR,
- up-to-date assessments, reports, or excerpts of reports from an independent party (such as a financial auditor, internal auditor, data protection officer, IT security department, data protection auditor, quality control inspectors), or
- relevant certification gained via an IT security audit or data protection audit (for example, in accordance with "BSI-Grundschutz" [IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology, or BSI], ISO 27001, ISO 27018, or ISO 27701).

(3) The Supplier will have the Technical and Organizational Measures (TOMs) reviewed regularly, and at least once a year, by an independent and qualified party in order to demonstrate compliance with the data protection requirements in accordance with Art. 28, para. 3, clause 2, item h of the GDPR. The results of this audit will be made available to the client without being requested and free of charge at https://accounts.hetzner.com/account/dpa.

(4) The Client has the right, in cooperation with the Supplier, to perform additional checks in accordance with Art. 28, para. 3, clause 2, item h of the GDPR to ensure compliance with data protection regulations and contractual agreements, and to do so to an appropriate and reasonable extent. The Supplier agrees to support the Client with their checks to ensure compliance with data protection regulations and contractual agreements, and to do so to an appropriate and reasonable extent.

The Client may perform these checks themselves or may commission a third party to perform the checks. The Supplier has the right to object if the Client commissions a third party to perform the checks and the third party is a direct competitor of the Supplier.

If the Client commissions a third party to perform the check, then the Client is required to conclude a non-disclosure agreement with the third party. The Supplier also has the right to demand that the commissioned third party submit a separate non-disclosure agreement, in particular with regard to professional non-disclosure and/or statutory confidentiality requirements.
The Client will perform on-site checks during normal business hours and after having given the Supplier reasonable advanced notice. The inspections may only be performed without interrupting the Supplier's operations and in compliance with the Supplier's security and confidentiality interests, and are limited to one check per calendar year. Special-purpose checks are excluded from this. The costs are defined in § 12 of this DPA.

§ 9 Further responsibilities to provide support

(1) The Supplier will support the Client in complying with duties described in Articles 32-36 of the GDPR. These include, among others:

a. Obligation to implement appropriate Technical and Organizational Measures
This means ensuring an appropriate level of protection by using Technical and Organizational Measures that take into account the circumstances and purposes for why the data is being processed; they should also take into account the probability and severity of a possible data breach that could occur due to a security vulnerability; they should also make it possible to immediately detect when a relevant data breach has occurred.

b. Notifying the Client of data breaches
This is an obligation for the Supplier to report personal data breaches to the Client without delay.

c. Supporting the Client with Client's duty to inform Data Subjects
The Supplier has the obligation to support the Client with the Client's duty to inform Data Subjects and to provide the Client with all relevant information about this duty without delay.

d. Supporting the Client with data protection impact assessments
This is support for the Client in making their data protection impact assessments.

e. Supporting the Client in prior consultations with the supervisory authority
This is support for the Client in the context of prior consultations with the supervisory authority.

(2) The Supplier may charge a fee for providing support services that are not included in the above section, that go beyond the Supplier's statutory responsibilities, or that are necessary for actions that are not considered misconduct on the part of the Supplier. The cost for these services are defined in § 12 of this DPA.

§ 10 The Client's authority to issue instructions

(1) The Supplier and any of its subordinates who have access to personal data may process the data that is subject to this DPA exclusively within the scope of the Client's main contract with the Supplier, and may do so in accordance with the instructions from the Client, unless the Supplier is legally required to process said data, or unless an exceptional situation exists that meets the requirements described in Art. 28 para. 3 item a of the GDPR.

(2) The Client's instructions are initially defined in this DPA and the Client may amend, supplement, or replace instructions in writing or in text form (for example, via email) by making specific separate instructions. The Client will confirm any oral instructions they may make without delay and (at a minimum, in written form). Any instructions that are not mentioned in the contract will be considered as a request for a change in performance.

(3) The Supplier will inform that Client immediately if they believe that one of the Client's instructions violates the GDPR or other data protection regulations from the EU or other Member States ("duty to remonstrate"). The Supplier will be within their rights to stop the implementation of said instruction until the Client affirms or amends it.

§ 11 Deletion and return of personal data

(1) Copies or duplicates of the data will not be created without the knowledge of the Client. Exceptions to this are:
- backup copies as far as they are necessary to ensure the proper processing of the data,
- data required for compliance with statutory storage obligations.

(2) Data, data storage devices, and all documents must either be returned or deleted at the request of the Client (in writing or a signed request) after the conclusion of the main contract, provided that these are the property of the Client.

(3) If it is not possible to delete this data in compliance with data protection regulations, the Supplier will ensure that the data storage devices and documents containing any contractually relevant data are destroyed in compliance with data protection regulations.
If, because of any other specified instructions from the Client, costs are incurred for the return, deletion, or destruction of the data, the Client will bear these costs. These costs are defined in § 12 of this DPA.

(4) The Supplier will retain documentation that serves as proof of proper data processing in accordance with the main contract and statutory regulations after the end of the contract in accordance with the respective retention periods. The Supplier may return this information to the Client at the end of the contract.

§ 12 Reimbursement

(1) The amount for fees to be agreed to in advance for the rights specified in §§ 8, 9, and 11 of this DPA will be based on an hourly rate for the Supplier's employee who performs the relevant support services.

(2) The Supplier is not entitled to remuneration for providing services which are necessary due to any data protection regulations that the Supplier violates.

§ 13 Other agreements

13.1 Choice of law

The laws of the Federal Republic of Germany will apply.
The exclusive, including international, place of jurisdiction for all disputes arising from this contractual relationship is the Supplier's registered headquarters in Gunzenhausen. However, we, the Supplier, are entitled to initiate legal action in any case at the customer's registered location of business. Overriding statutory provisions, especially those regarding exclusive jurisdiction, will remain unaffected.

13.2 Liability

The liability clause agreed to between the parties of the main contract will also apply to data processing defined in this DPA.

13.3 Safekeeping of the data

If the Client's data stored at the Supplier is jeopardized due to seizure, confiscation, insolvency, or bankruptcy proceedings or other events or measures undertaken by third parties, the Supplier will immediately inform the Client about it. The Supplier will immediately inform all responsible parties that the sovereignty and ownership of the data lies exclusively with the Client/"the Controller" within the meaning of the General Data Protection Regulations.
This will not apply in the event that the Party required to share said information is obliged by law and/or official court order to maintain secrecy about the disclo- sure. In addition, it will not apply if the Party required to share said information is required to maintain confidentiality due to an official government order or court order or is under threat of punishment.

13.4 Amendments and modifications

Any amendments or modifications to this DPA and its provisions, including any commitments made by the Supplier, require a written agreement, which may also be made in an electronic form (signed text). It must be clearly stated in said agreement that it is an amendment or modification to this DPA. The same applies to the waiver of this formal requirement.

13.5 Data protection regulations take precedence

If there are any contradictions, the provisions of this DPA on data protection will take precedence over the provisions of the main contract.

13.6 Severability clause

If any part of this DPA becomes invalid, it will not affect the validity of the remaining provisions.

Signatures

_____, date _____

Client

Gunzenhausen, date 27/05/2026

HETZNER ONLINE
Hetzner Online GmbH | Industriestr. 25
91710 Gunzenhausen | www.hetzner.com

Supplier

Appendix 1: Scope, type, and purpose of data storage, processing, and use, as well as the type of data and Data Subjects

Scope, type, and purpose of data storage, processing

These are defined above in the main body of this DPA.

Types of data

- Log data

Affected People

- The Client's customers and interested parties

Appendix 2: Technical and Organizational Measures

The Technical and Organizational Measures (TOMs) are in place to make sure that there is an appropriate level of protection for personal data, and more specifically, to protect the rights and freedoms for data subjects. Below, you will find detailed information about Hetzner's TOMs. You can also find more information at https://docs.hetzner.com/general/others/technical-and-organizational-measures.

1 Physical access control

Physical access control defines who has physical access to a site, building, or room.

Measure	Data Centers	Admin buildings
Electronic access control system with logging	✓	✓
Documented distribution of access media	✓	✓
Comprehensive video monitoring	✓	✓
Policy about how to handle visitors	✓	✓
High security perimeter fencing (with anti-climbing and anti-tunnelling protection) around the entire data center park	✓	NA
Separate colocation area with lock-able racks	✓	NA

For the next few sections of this appendix, the following is true:
Dedicated servers/Cloud servers: You/the Client are completely responsible for the management, maintenance and security of the server.
Managed products: For these products, we at Hetzner take responsibility for the maintenance, administration, and security of your systems.

2 Electronic access control

The electronic access control defines who is allowed to log on to a system so that only authorized people have access to it.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Individual customer accounts with numerous management options and access to the administration interface	✓	✓	✓	✓	✓	✓	✓	✓
Traceable access logs and change logs for customer accounts	✓	✓	✓	✓	✓	✓	✓	✓
Required passwords for customer accounts with defined minimum requirements	✓	✓	✓	✓	✓	✓	✓	✓
Option for two-factor authentication (2FA) for customer accounts	✓	✓	✓	✓	✓	✓	✓	✓
Client has exclusive access to server	✓	✓	✓	NA (see next line)	NA (see next line)	NA (see next line)	NA (see next line)	NA (see next line)
Only authorized Hetzner employees have administrative access, within the scope of the agreed service; via multilevel authentication and	NA (see last line)	NA (see last line)	NA (see last line)	✓	✓	✓	✓	✓

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
cryptographic protection Access done for tasks ranging from infrastructure maintenance to complete server management depending on product (Access done for tasks ranging from instrastructure maintenance to complete server management epending on product)								
Additional measures are the responsibility of the Client	✓	✓	✓	✓	✓	✓	✓	✓

3 Internal access control

Internal access control defines which authorizations people have within a system. It defines what a user may see, change, or execute after accessing a system.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Regular updates	Client's responsi-bility	Client's responsi-bility	✓ for the underlying cloud infrastructure	✓ for the underlying infrastructure	✓	✓	✓	✓
Audit-proof, binding authorization procedure based on a role and authorization policy	Client's responsi-bility	Client's responsi-bility	✓ The cloud infrastructure is accessed. Client's responsibility for virtual machine.	✓ Client's responsibility for file access	✓ Client's responsibility for file access	✓ Client's responsibility for file access	✓ Client's responsibility for file access	✓ Client's responsibility for file access
Maintaining, securing, and updating transferred data/software	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility
Additional measures are the responsibility of the Client	✓	✓	✓ regarding access to cloud servers	✓	✓	✓	✓	✓

4 Transfer control

Transfer control includes measures and procedures that make sure that the use, access, and transport of physical data storage media are monitored and protected against unauthorized access.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Defined process for deleting data from storage drives after contract is complete Implemented differently depending on product type	Client's responsi-bility	✓	✓	✓	✓	✓	✓	✓
Storage drives are physically destroyed if data cannot be successfully erased	Client's responsi-bility	✓	✓	✓	✓	✓	✓	✓
Physical access to storage devices only in defined areas; transport across locations exclusively in locked transport boxes	Client's responsi-bility	✓	✓	✓	✓	✓	✓	✓

5 Isolation control

Measures for isolation control make sure that data for each different customer or application within a system is separated from each other when they are processed and stored.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Physical or logical separation of data	Client's responsi-bility	Client's responsi-bility	✓	✓	✓	✓	✓	✓
Physical and logical separation of backup data	Client's responsi-bility	Client's responsi-bility	✓	✓	✓	✓	NA	Client's responsi-bility
Additional measures are the responsibility of the Client	✓	✓	✓	✓	✓	✓	NA	NA

6 Pseudonymization

Using pseudonymization methods, personal data is modified in such a way that it cannot be tied to specific people without additional information being provided.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Pseudonymization of data stored within the systems	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility

7 Confidentiality

Confidentiality measures make sure that personal data is protected from unauthorized access or disclosure while it is being processed and stored.

Measure	Implementation
Hetzner employees sign a confidentiality agreement before they begin doing any work with personal data in compliance with data protection regulations	✓
Confidentiality agreement and implementation of TOMs by external persons before starting their activities for Hetzner (if necessary)	✓
Hetzner employees regularly get training to raise awareness for and knowledge about data protection and information security	✓
Encryption options for data transfers (Implemented differently depending on product type)	✓
Encryption of Data (at rest)	Client's responsibility
Encryption of Backups (at rest)	Client's responsibility. Exception Managed Servers: ✓

8 Integrity

Data integrity measures make sure that data and systems remain complete, uncorrupted, and correct while they are being stored or transferred.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Data changes are logged in an audit-proof manner	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	✓	✓	✓	✓	✓
Responsiblity for entering and processing data	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility
Virus scanner / Security tests	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	✓	✓	Rootkit tests	Rootkit tests	-
Additional measures are the responsibility of the Client	✓	✓	✓	✓	✓	✓	✓	✓

9 Availability, resilience and network security

Availability measures focus on keeping the systems in continued working order. Resilience measures make sure that the data remains available even under exceptional circumstances. Network security includes measures to protect the network infrastructure from unauthorized access and attacks.

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Operation and support								
24/7 technical support directly in data center	NA Remote Hands on request	✓	✓	✓	✓	✓	✓	✓
Escalation chain for disruptions and emergencies	See product description							
Monitoring	Client's responsi-bility	Client's responsi-bility	✓ for Host Client's responsibility for virtual machine	✓	✓	✓	✓	✓
Power supply, climatization and facility management								
Uninterruptible power supply using redundant UPSs and emergency power supply system	✓	✓	✓	✓	✓	✓	✓	✓
Redundant power supply from the substation	✓	✓	✓	✓	✓	✓	✓	✓

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Redundant and energy-efficient cooling using direct free cooling and climate controls	✓	✓	✓	✓	✓	✓	✓	✓
Cold-aisle containment in above-average raised flooring	✓	✓	✓	✓	✓	✓	✓	✓
Monitoring of process-relevant parameters via intelligent measurement, control, regulation, and monitoring system	✓	✓	✓	✓	✓	✓	✓	✓
Fire protection								
Site-wide early warning fire system; direct connection to the local fire and rescue coordination center	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic fire protection measures	✓	✓	✓	✓	✓	✓	✓	✓
Regular training for emergencies and fire protection	✓	✓	✓	✓	✓	✓	✓	✓

Measure	Colo-cation	Dedicated servers	Cloud servers	Managed servers	Web hosting	Storage Shares	Storage Boxes	Object Storage
Network and attack protection								
Redundant and highly available network infrastructure (99.9% network availability in accordance with GTC)	✓	✓	✓	✓	✓	✓	✓	✓
Continuous active DDoS recognition	✓	✓	✓	✓	✓	✓	✓	✓
Use of firewall and port management	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	✓	✓	✓	✓	✓
Individually configured firewall	NA	✓	✓	NA (see next line)	NA (see next line)	NA (see next line)	NA (see next line)	✓
Hetzner-managed firewall with 24/7 monitoring	NA	NA (see last line)	NA (see last line)	✓	✓	✓	✓	NA (see last line)
Backup and system protection								
Backup and recovery plan	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility Backups and snapshots can be added for a fee	✓ partially depends on purchased services	✓	✓ Own backup recommended	Client's responsi-bility Snapshots, depending on purchased services	Client's responsi-bility Redundant storage within the cluster system
Disk mirroring	Client's responsi-bility	Client's responsi-bility	Client's responsi-bility	✓	✓	✓	✓	✓

10 Procedures for regular testing, assessment, and evaluation

Regularly testing, assessing, and evaluating the data protection and security standards ensures that the measures stay in compliance with regulations and improve over time.

Measure	Implementation
Data protection and information security management system (DMS, ISMS)	✓
Employment of a data protection and information security officer who is integrated into the operational processes	✓
Data-protection-friendly default settings (privacy by default and privacy by design)	✓
Incident response management	✓
Certifications according to ISO 27001, § 8a BSI-KritisV and BSI C5 Type 2 certification	✓
Annual review of TOMs by external service provider	✓
Annual review of the proper calculation and billing of connection charges by expert opinion in accordance with § 63 TKG	✓
EMAS certification (ISO 14001) of the environmental management system at German locations	✓

Appendix 3: Approved Subcontractors

Hetzner Online GmbH (the Supplier) uses services of third parties (subcontractors) while processing data on behalf of its customers (the Client). These subcontractors process data on behalf of Hetzner Online GmbH.
The following is a list of approved subcontractors:

Server location	Subcontractor	Subcontractor's address	Type of service
Finland	Hetzner Finland Oy	Huurrekuja 10, 04360 Tuusula (Finland)	Building rental, technical support
USA	Hetzner US LLC	1500 Broadway, 19th Fl, New York, NY 10036 (USA)	Server rental on location in USA
	NTT Global Data Centers Americas, Inc.	1 625 National Drive, Sacramento, CA 95834 (USA)	Colocation provider on location in USA
	QTS Investment Properties Hillsboro, LLC	Overland Park, 12851 Foster Street, Overland Park, KS 66213 (USA)	Colocation provider on location in USA
Singapore	Hetzner Singapore Pte. Ltd.	1 Scotts Road, #21-10 Shaw Centre, Singapore 228208 (Singapore)	Server rental on location in Singapore
	NTT Global Data Centers SG1 Pte Ltd	8 Kallang Avenue #15-01/09, Aperia, 339509 Singapore (Singapore)	Colocation provider on location in Singapore

Please note:
If you have chosen a server location within the EU, your data will only be processed within the EU. The technical and customer support services for all server locations are provided within the EU.