OCTOPUS CLOUD

DATA PROCESSING ADDENDUM

CLOUD VIEW SERVICE

Last updated May 2026

Octopus Cloud develops software, advises and trains its clients within the range of software and license management. Octopus Cloud is an independent software asset management development company.

In its capacity, Octopus Cloud has developed certain software products, which are being offered to customers for subscription under Octopus Cloud's standard contractual terms.

The Partner is interested in a collaboration with Octopus Cloud with regard to the marketing and distribution of Octopus Cloud's Products into certain channels.

1. Definitions

In this Addendum the following terms shall have the meanings set out below:

1.1 "Contract Processing" means storing, making available and otherwise Processing Personal Data by Octopus Cloud on behalf and for the purposes of the Customer in connection with the Customer's use of Cloud View including support services related thereto in accordance with Customer's Subscription Order and the applicable GTCs/EULAs and as further specified in Section 2 of this Addendum.

1.2 "Covered Personal Data" means the types of Personal Data covered by the Contract Processing, as further specified in Section 3.2.

1.3 "Data Subject" means a natural person whose Personal Data is Processed.

1.4 "Data Protection Legislation" means laws and regulations which protect the privacy rights of individuals, in so far as those laws and regulations apply to the Processing of Personal Data in connection with Customer's use of Cloud View, including without limitation the GDPR, the UK GDPR, the Swiss Federal Act on Data Protection (revFADP/SFDPA), data protection legislation enacted by EU/EEA Member States, and any successor or similar measures.

1.5 "Personal Data" means all data and information relating to an identified or identifiable natural person. Personal Data also includes pseudonymised data within the meaning of Article 4(5) GDPR where such data can be reasonably re-identified using additional information. Data that has been fully anonymised and cannot be re-identified shall not be considered Personal Data under this Addendum.

1.6 "Sensitive Data" means special categories of Personal Data within the meaning of Article 9 GDPR (in particular Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of

uniquely identifying a natural person, data concerning health, sex life or sexual orientation), as well as the equivalent categories under the SFDPA.

1.7 "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.8 "Data Controller" means the entity determining the purposes and means of the Personal Data Processing operations performed by means of using Cloud View, i.e. Customer.

1.9 "Data Processor" means the entity making available Cloud View and storing, making available or otherwise Processing Personal Data on behalf and for the purposes of the Data Controller in connection therewith, i.e. Octopus Cloud.

1.10 "Data Protection Impact Assessment" or "DPIA" means an analysis carried out under Article 35 GDPR (or its equivalent under the SFDPA) of how Personal Data is collected, used, shared, protected and maintained, and the risks such Processing poses to the rights and freedoms of Data Subjects.

1.11 "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 (General Data Protection Regulation), including any applicable implementing laws, regulations and secondary legislation, as amended or replaced from time to time.

1.12 "SFDPA" means the revised Swiss Federal Act on Data Protection in force as of 1 September 2023, together with the Ordinance on Data Protection (DPO) and other Swiss implementing instruments.

1.13 "Standard Contractual Clauses" or "SCCs" means (i) for transfers from the EEA, the standard contractual clauses adopted by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021; (ii) for transfers from the United Kingdom, the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner's Office; and (iii) for transfers from Switzerland, the EU SCCs as recognised by the Swiss Federal Data Protection and Information Commissioner (FDPIC), in each case as updated or replaced from time to time.

1.14 "Customer's Subscription Order" means Customer's subscription order with regard to Cloud View and the applicable GTCs/EULAs (plus documents referred to therein) that govern Customer's subscription to Cloud View.

1.15 "Sub-processor" means any legal entity (including affiliates of Octopus Cloud) commissioned by Octopus Cloud to carry out the Contract Processing or parts thereof on behalf of the Customer.

1.16 "Personal Data Breach" has the meaning given to it in Article 4(12) GDPR and includes any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Covered Personal Data.

1.17 Other capitalised terms not defined in this Addendum have the meanings assigned to them in Customer's Subscription Order, the GDPR, or the SFDPA.

2. Specification of Contract Processing

2.1 Customer's Subscription Order and the service description of Cloud View and related support services determine the subject-matter, nature and purpose of the Contract Processing. Specifically, the Contract

Processing concerns the storage, making available, granting access to, transmitting and combining of Personal Data for the purposes of providing Cloud View and related support services to the Customer.

2.2 The duration of this Addendum shall be as determined in accordance with Section 7 of this Addendum.

3. Type of Personal Data and Categories of Data Subjects

3.1 The Contract Processing, depending on the Cloud View edition subscribed to by Customer, concerns the following categories of Data Subjects:

a. Customer's employees (in their capacity as Users of the Cloud View service or if interacting with Octopus Cloud's support organisation);

b. Customer's authorised agents (in their capacity as Users of the Cloud View service or if interacting with Octopus Cloud's support organisation);

c. Customer's contact persons; and

d. any other individuals in respect of whom Customer owns or has subscribed to personalised licences within the scope of Cloud View.

3.2 The Contract Processing covers the following types of Personal Data:

a. Contact data;

b. User action history captured in service and support log files;

c. Licence information (where Cloud View scans reveal personalised licences owned or subscribed to by Customer), which may include personal key data and contact data, Active Directory information, group and role information, latest log-in, and general licence information (such as licence start date).

3.3 The Parties acknowledge that the Contract Processing is not intended to involve, and Customer shall not knowingly upload or otherwise cause Octopus Cloud to Process, any Sensitive Data within the meaning of Section 1.6.

4. Data Privacy

4.1 Customer represents and warrants that Personal Data disclosed to Octopus Cloud has been collected in a lawful manner and does not infringe upon the rights and freedoms of any Data Subject and/or third party.

4.2 Customer shall comply with all obligations under applicable Data Protection Legislation to which Customer is subject in its quality as Data Controller in relation to the Contract Processing. This shall include, in particular, the following obligations:

a. to inform Data Subjects of their individual rights under applicable Data Protection Legislation;

b. to inform Data Subjects of the Personal Data collected as part of the Contract Processing;

c. where necessary under applicable Data Protection Legislation, to ensure that there is a legal basis under Article 6 GDPR (or the SFDPA equivalent) to Process Personal Data and, where the legal basis is consent of Data Subjects, to collect and log the consent of Data Subjects associated with the Contract Processing; and

d. to ensure that Covered Personal Data does not include Sensitive Data, in particular, to ensure that Customer does not upload Sensitive Data into Cloud View. Octopus Cloud shall have no obligation to monitor for Sensitive Data but reserves the right to suspend Processing if it becomes aware that such data is being processed in violation of this Addendum.

4.3 In its quality as Data Processor in relation to the Contract Processing, Octopus Cloud has certain legal obligations deriving from Article 28 GDPR and the (revised) SFDPA and shall be contractually bound to comply with the following obligations:

a. Octopus Cloud shall notify the Customer without undue delay of any change in applicable Data Protection Legislation that materially impacts the Processing activities under this Addendum, including any new legal requirements concerning international data transfers, additional security obligations, or changes to Data Subject rights.

b. Upon Customer's reasonable request, and where such assistance falls outside the scope of services already covered by Customer's Subscription Order, Octopus Cloud shall use commercially reasonable endeavours to assist Customer in its compliance with Data Protection Legislation, including without limitation the preparation of necessary notifications, registrations and documentation reasonably required by Customer in connection with Customer's Subscription Order and use of Cloud View and related support services. Such additional assistance may be subject to separate compensation where the assistance is materially beyond ordinary support.

c. Octopus Cloud shall Process Covered Personal Data only on documented instructions from Customer, including with regard to transfers of Covered Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Octopus Cloud is subject; in such a case, Octopus Cloud shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Customer's instructions are set out in Customer's Subscription Order, this Addendum, and any further written instructions reasonably issued by Customer; if Octopus Cloud has reasonable grounds to believe that any instruction infringes Data Protection Legislation, it shall promptly inform Customer and shall be entitled to suspend the relevant Processing until Customer modifies the instruction.

d. Octopus Cloud shall ensure (i) that any persons authorised to perform Contract Processing do so only in accordance with the terms of this Addendum; and (ii) that all such persons have committed themselves to confidentiality (whether by contract or by statute) and have received appropriate training on the protection of Personal Data.

e. Octopus Cloud shall not carry out the Contract Processing in, or transfer Covered Personal Data to, countries outside Switzerland, the European Economic Area or any country or territory recognised by the European Commission and/or the FDPIC as providing an adequate level of data protection, unless Octopus Cloud implements appropriate safeguards in accordance with Articles 44–49 GDPR (and the corresponding SFDPA requirements), which may include the conclusion of Standard Contractual Clauses with the relevant Sub-processor and the conduct of a Transfer Impact Assessment in line with EDPB Recommendations 01/2020. In such a case, Octopus Cloud shall, prior to the first transfer of Covered Personal Data, inform Customer of the relevant country to which Covered Personal Data is transferred and the safeguards put in place. Octopus Cloud shall only be required to implement transfer safeguards for transfers under its direct control; Customer shall remain solely responsible for ensuring lawful transfers of Personal Data to and from its own third-party systems, partners or affiliates that are not Sub-processors of Octopus Cloud.

f. Octopus Cloud shall engage Sub-processors only with the authorisation of Customer:

(i) Customer hereby provides Octopus Cloud with a general written authorisation to engage Sub-processors, provided that Octopus Cloud enters into a written agreement with each Sub-processor that imposes data protection obligations substantially equivalent to those set out in this Addendum and sufficient to enable Octopus Cloud to comply with its obligations hereunder.

The current list of Sub-processors engaged by Octopus Cloud is set out in Appendix 2 to this Addendum and is also made available on Customer's Cloud View tenant or, upon request, electronically by email.

(ii) Octopus Cloud may appoint new Sub-processors or replace existing Sub-processors provided that (1) Octopus Cloud informs Customer in advance, in writing or in text form (including by amending the list of Sub-processors made available on Customer's Cloud View tenant, the Octopus Cloud Customer Portal or similar publication channel), giving at least thirty (30) calendar days' advance notice; (2) Customer has not objected on reasonable data-protection grounds in writing or in text form by the date the new Sub-processor is engaged; and (3) the engagement is based on a contractual agreement in accordance with applicable Data Protection Legislation. Where Customer raises a reasonable objection, the Parties shall work together in good faith to resolve it; if no resolution can be reached, Customer's sole and exclusive remedy shall be to terminate the affected portion of the Cloud View service.

(iii) Octopus Cloud shall remain fully liable to Customer for the performance of each Sub-processor's data protection obligations as required under Article 28(4) GDPR.

g. Octopus Cloud shall promptly notify Customer of any request received from a Data Subject seeking to exercise rights under Articles 15–22 GDPR (or equivalent rights under the SFDPA) in respect of Covered Personal Data, and shall not respond to such requests itself unless authorised by Customer or required by law. Octopus Cloud shall, upon request, assist Customer with appropriate technical and organisational measures, insofar as reasonably possible, in responding to such requests within the statutory deadlines. Where the requested assistance is materially beyond ordinary support, separate compensation may apply.

h. At Customer's reasonable request, Octopus Cloud shall provide Customer with the information and assistance reasonably required to enable Customer to carry out a Data Protection Impact Assessment under Article 35 GDPR and any prior consultations with supervisory authorities under Article 36 GDPR in relation to the services provided under this Addendum.

i. Octopus Cloud shall make available to Customer all information necessary to demonstrate compliance with Article 28 GDPR and shall allow for, and contribute to, audits — including inspections — conducted by Customer or another auditor mandated by Customer (or by any competent regulator). Customer shall provide Octopus Cloud with at least ten (10) business days' prior written notice of any such audit; audits shall be conducted only during regular business hours and in a manner that minimises disruption to Octopus Cloud's operations and shall be subject to reasonable confidentiality undertakings. Octopus Cloud may satisfy its audit obligations under this Section by providing recent reports and certifications issued by independent third-party auditors of Octopus Cloud or its Sub-processors, provided that such reports reasonably permit Customer or competent regulators to assess Octopus Cloud's compliance with this Addendum. Customer shall bear its own costs of audits; Octopus Cloud may charge reasonable compensation only for assistance materially exceeding what is required to comply with Article 28(3)(h) GDPR.

j. Upon termination of the Contract Processing, Octopus Cloud shall, at Customer's choice, return to Customer or delete all Covered Personal Data, to the extent technically possible, except where storage of the Covered Personal Data is required by Union or Member State law to which Octopus Cloud is subject. Where Customer requests deletion, Octopus Cloud shall, on Customer's written request, certify the deletion in writing. Backup copies will be deleted in accordance with Octopus Cloud's standard backup retention cycle, and shall remain protected by the obligations of this Addendum until deletion.

5. Security

5.1 Customer is responsible for the proper creation and management of its user accounts, including user account disabling and account reviews. Customer shall in particular ensure that:

a. access and authorisations are granted on a need-to-have basis;

b. each User is assigned a unique account;

c. accounts are periodically reviewed to validate their continued relevance;

d. generic accounts are not used; and

e. suspected compromised accounts are disabled without delay.

5.2 Octopus Cloud shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons:

a. implement and maintain the technical and organisational measures set out in Appendix 1 to this Addendum, designed to protect the confidentiality, integrity, availability and resilience of Covered Personal Data, in line with Article 32 GDPR. Customer accepts that Octopus Cloud may adjust or optimise these measures provided that (1) the resulting overall level of protection is materially equivalent or higher; and (2) Octopus Cloud informs Customer in advance, in writing or in text form (including by amending the list of measures made available on Customer's Cloud View tenant), with appropriate advance notice;

b. notify Customer without undue delay, and in any event within seventy-two (72) hours of becoming aware, of any Personal Data Breach affecting Covered Personal Data. Such notification shall include, to the extent then known: (i) a description of the nature of the Personal Data Breach (including, where possible, the categories and approximate number of Data Subjects and records concerned); (ii) the likely consequences of the Personal Data Breach; and (iii) the measures taken or proposed to address it, including measures to mitigate its possible adverse effects;

c. in the event of a Personal Data Breach, (i) without undue delay investigate, contain, mitigate, remediate and otherwise address the Personal Data Breach, including by identifying Covered Personal Data affected and taking sufficient steps to prevent recurrence; and (ii) provide such information and assistance as Customer may reasonably require to enable Customer to evaluate the Personal Data Breach and to comply with any applicable notification obligations to supervisory authorities and Data Subjects under Articles 33–34 GDPR or equivalent provisions of the SFDPA.

6. Limitation of Liability

6.1 To the maximum extent permitted by applicable law, Octopus Cloud's total aggregate liability under this Addendum, whether arising in contract, tort (including negligence) or otherwise, shall be limited to the fees paid by the Customer to Octopus Cloud for the twelve (12) months preceding the event giving rise to the claim.

6.2 In no event shall Octopus Cloud be liable for any indirect, incidental, punitive or consequential damages, including but not limited to loss of profits, loss of revenue, loss of goodwill, loss of anticipated savings, business interruption, or loss, corruption or unauthorised disclosure of data, even if advised of the possibility of such damage.

6.3 The Parties acknowledge that this Addendum does not foresee the Processing of Sensitive Data. Octopus Cloud shall bear no liability for any Sensitive Data that the Customer unintentionally or unlawfully uploads, stores or causes to be Processed in violation of this Addendum.

6.4 Octopus Cloud shall not be liable for damages or breaches caused by third-party providers or Sub-processors, provided that Octopus Cloud has exercised reasonable due diligence in selecting and monitoring such providers in accordance with this Addendum and remains liable for the Sub-processor obligations expressly assumed in Section 4.3(f)(iii).

6.5 Octopus Cloud shall not be liable for any delays, failures or modifications to the Cloud View service resulting from changes in applicable laws, regulations or regulatory guidance beyond its reasonable control. Octopus Cloud shall also not be liable for any failure to perform its obligations under this Addendum due to force majeure events, including but not limited to natural disasters, cyberattacks, strikes, war, governmental actions or other unforeseen circumstances beyond its reasonable control.

6.6 Nothing in this Section 6 shall limit or exclude liability for: (a) wilful misconduct or gross negligence; (b) liability that cannot be lawfully limited under applicable Data Protection Legislation, including the rights of Data Subjects to compensation under Article 82 GDPR; or (c) any administrative fines imposed on Octopus Cloud directly attributable to its own breach of this Addendum or applicable Data Protection Legislation.

7. Term

7.1 This Addendum shall enter into force on the effective date of Customer's Subscription Order and shall co-terminate with Customer's subscription to Cloud View.

7.2 Octopus Cloud's obligations specified herein shall continue to apply if and to the extent Contract Processing continues post-termination of Cloud View and this Addendum (for instance during any grace period during which Customer can migrate data from its Cloud View tenant).

Appendix 1 — Technical and Organisational Measures

1. Information Security Programme

1.1 Octopus Cloud maintains an information security programme (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Covered Personal Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable internal and external risks to security and unauthorised access to the Cloud View service, and (c) minimise security risks, including through periodic risk assessment and regular testing. Octopus Cloud has designated one or more employees to coordinate and be accountable for the information security programme. The information security programme is structured around the control families defined in ISO/IEC 27001:2022 and is aligned with the requirements of the GDPR and the SFDPA.

1.2 Octopus Cloud's information security programme covers the following pillars:

- **Privacy & Data Protection:** data minimisation and purpose limitation, privacy by design and default, governed international data transfers, Data Subject rights handling, breach response, and a documented data retention and deletion policy.
- **Governance, Risk & Compliance:** an internal Information Security Management System (ISMS) and GRC framework, dedicated privacy and security roles, comprehensive policies (access management, encryption, incident response, logging, endpoint security), and continuous risk assessment.
- **Technical Security Controls:** encryption at rest using AES-256 and in transit using TLS 1.2 or higher; role-based access control (RBAC) with mandatory multi-factor authentication (MFA); strong password and account lifecycle management; secure remote access; device hardening and anti-malware protection; firewalls, intrusion detection and continuous monitoring; centralised logging and SIEM-based real-time detection.
- **Incident Response & Business Continuity:** a documented and tested Incident Response Plan covering detection, analysis, containment, eradication, recovery and lessons-learned; a Business Continuity and Disaster Recovery Plan with regular backup and restore testing, redundant infrastructure and operational playbooks for crisis scenarios.
- **Personnel Security & Awareness:** mandatory periodic security and data protection training, least-privilege access, background checks for sensitive roles, and signed confidentiality and compliance agreements for all staff.
- **Independent Oversight:** regular penetration testing and security assessments by independent third parties.

1.3 While Octopus Cloud's own ISMS is not separately certified at the date of this Addendum, the main sub-processors are independently certified to recognised international standards, as summarised below:

- **T-Systems International GmbH** (host of the Cloud View SaaS solution on Open Telekom Cloud / T Cloud Public): ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, ISO 9001, BSI C5 (Type 2), SOC 1 (ISAE 3402), SOC 2, and Trusted Cloud Data Protection Profile (TCDP). See: Trusted Cloud listing; current certifications & compliance overview: T Cloud Public — Certifications & Compliance; service description: Open Telekom Cloud Service Description; supplementary terms for commissioned data processing (DPA): Supplementary Terms — Data Processing; Deutsche Telekom Privacy and Security Assessment (PSA) procedure: Privacy and Security Assessment process.
- **Zendesk, Inc.** (support ticketing platform provider): ISO/IEC 27001, ISO/IEC 27018, ISO/IEC 27701, ISO/IEC 42001 (AI management), SOC 2 Type II, FedRAMP, and Cyber Essentials Plus. Zendesk has approved Binding Corporate Rules (BCRs) for international transfers. See: Zendesk Trust Center;

international standards commitment: ISO 27001/27018/27701/42001 commitment; Zendesk Data Processing Agreement: Zendesk DPA.

- **Hetzner Online GmbH** (direct cloud infrastructure sub-processor for the Cloud View production environment; EU-only data residency at Nuremberg and Falkenstein, Germany, and Helsinki, Finland): ISO/IEC 27001:2022 (SOCOTEC), BSI C5 Type 2, and § 8a BSIG / BSI-KritisV. TOMs audited annually by TÜV Rheinland (i-sec GmbH); audit report available to controllers via the Hetzner customer portal upon execution of a DPA. See: Hetzner Data Protection Certificates and Hetzner TOMs. Full

2. Confidentiality

Requirement	Established Measures
a) Physical Access / Admittance Control	• Prevention of unauthorised access to data processing systems through magnetic / chip cards, key-controlled access, electric door openers, on-site security personnel and concierge service, alarm systems and CCTV (sub-processors).
b) Electronic Access Control	• Strong password policies, automatic session-locking mechanisms, multi-factor authentication (MFA) for administrative and privileged access, encryption of data media, and TLS 1.2 or higher for all access channels.
c) Internal Access Control (user permissions and amendment of data)	• Role-based access control (RBAC) with formally documented authorisation concepts and least-privilege / need-to-know access rights. • Centralised logging of system access; real-time monitoring through a Security Information and Event Management (SIEM) platform.
d) Separation Control	• Logical separation of data Processed for different purposes through multitenancy and sandboxing; tenant-level segregation of customer data.

3. Integrity

Requirement	Established Measures
a) Data Transfer & Disclosure Control	• End-to-end encryption of data in transit using TLS 1.2 or higher; encrypted VPN channels for administrative access; encrypted backups; AES-256 encryption of data at rest.
b) Input Control	• Logging of input, modification and removal events with operator identification; tamper-resistant document and case management; centralised log retention to support investigations and regulatory enquiries.

4. Availability & Resilience

Requirement	Established Measures
a) Availability Control	• Documented backup strategy (online/offline; on-site/off-site) with regular restore testing; uninterruptible power supply (UPS); anti-malware and anti-virus protection; perimeter and host-based firewalls; centralised SIEM-based monitoring; documented escalation paths and emergency response procedures.

Requirement	Established Measures
b) Data Recovery	• Tested ability to restore the availability of and access to Covered Personal Data in a timely manner in the event of a physical or technical incident, in accordance with documented recovery time and recovery point objectives (RTO/RPO).

5. Regular Testing, Assessment and Evaluation

Requirement	Established Measures
a) Tests, Assessments, Evaluations	• Documented data protection management (incident handling, DSR processing, retention enforcement). • Tested and exercised incident response management. • Privacy-by-default settings and continuous control monitoring. • Order Control: no commissioned data Processing without corresponding documented instructions from the Customer. • Periodic internal and independent third-party penetration testing and security assessments. • Periodic supplier and sub-processor due diligence and reassessment.

Appendix 2 — List of Sub-processors

Name	Address / Country	Service / Role
T-Systems International GmbH	Hahnstrasse 43d, 60528 Frankfurt am Main, Germany	Hosting of the Cloud View online modules (Germany and the Netherlands).
Zendesk, Inc.	989 Market Street, Suite 300, San Francisco, California 94103, USA	Support ticketing platform provider. Transfers safeguarded by Zendesk's approved Binding Corporate Rules and applicable Standard Contractual Clauses.
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Germany. Production data centres: Nuremberg and Falkenstein (Germany); Helsinki (Finland)	Direct cloud infrastructure sub-processor for the Cloud View production environment. EU-only data residency for Covered Personal Data; non-EU Hetzner data centre locations (Ashburn (VA), Hillsboro (OR), Singapore) are not used for Covered Personal Data. Certified to ISO/IEC 27001:2022 (SOCOTEC), BSI C5 Type 2, § 8a BSIG / BSI-KritisV; TOMs audited annually by TÜV Rheinland (i-sec GmbH). DPO contact: data-protection@hetzner.com. Full sub-processor profile is set out in Appendix 1, Section 1.4 of this Addendum.