DATA PROCESSING ADDENDUM CLOUD VIEW SERVICE

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

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

1.2. "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.

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

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

1.5. "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 Cloud View, including without limitation Data protection legislation enacted by Switzerland (i.e. the SFDPA), the EU/EEA and EU/EEA Member States, and similar measures;

1.6. "Personal Data" means all data and information relating to an identified or identifiable natural person;

1.7. "Sensitive Data" means Personal Data revealing racial or ethnic origin, political opinions, religious beliefs, health, sexual orientation, etc. (as specified in the SFDPA);

1.8. "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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.9. "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;

1.10. "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;

1.11. "Data Protection Impact Assessment" means an analysis of how Personal Data is collected, used, shared, protected and maintained.

1.12. "SFDPA" means the Swiss Federal Data Protection Act.

1.13. "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.

1.14. "Sub-processor" shall mean a legal entity commissioned by Octopus Cloud to carry out the Contract Processing or parts thereof.

1.15. Other capitalized terms not defined in this Addendum have the meanings assigned to them in Customer's Subscription Order, and any additional data protection-related terms shall have the meanings given to them in the SFDPA.

2. Specification of Contract Processing

2.1. Customer's Subscription Order and 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 storage, making available, granting access to, transmitting and combining Personal Data for the purposes of providing Cloud View and related support services to the Customer.

2.2. The duration of the Addendum shall be as determined in accordance with section 6 of this Addendum.

3. Type of Personal Data and categories of Data Subject

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

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

b. Authorized Agents (in their capacity as Users of the Octopus View service or if interacting with Octopus Cloud's support organization);

c. Contact Persons.

All individuals regarding which Customer owns or has subscribed to personalized licenses.

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

a. Personal Master Data (Key Personal Data);

b. Contact Data;

c. User Action History in Service & Support Log Files.

d. License information (in the event Cloud View scans reveal personalized licenses owned or subscribed to by Customer), which does include personal key data and contact data, active directory information, group and role information, latest log-in, general license information (such as license start date).

4. Data Privacy

4.1. Customer represents and warrants that Personal Data disclosed to Octopus Cloud was collected in a lawful way and does not infringe upon the rights and freedoms of the Data Subject and/or third parties.

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 will 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 to Process Personal Data and, if the legal basis is consent of Data Subjects, collect and log the consent of Data Subjects associated to the Contract Processing; and

d. to ensure that Covered Personal Data will not include Sensitive Data, in particular, to ensure that Customer will not upload Sensitive Data into Cloud View.

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

a. Upon Customer's request and in exchange for separate compensation, Octopus Cloud shall use commercially reasonable endeavors to assist Customer in its compliance with Data Protection Legislation, including without limitation the preparation of necessary notifications, registrations and documentation which Customer may be reasonably required to make or enter into in order to comply with Data Protection Legislation in connection with Customer's Subscription Order and use of Cloud View and related support services.

b. Octopus Cloud will only process the Covered Personal Data for the purpose of making available Cloud View and related support services in accordance with the Customer's Subscription Order, and use all commercially reasonable endeavors to implement Customer's additional documented written instructions; such additional instructions may be specific instructions or standing instructions of general application in relation to the Contract Processing, provided that their implementation is feasible and objectively reasonable within the scope of the Cloud View service agreed with Customer; if Octopus Cloud has reasons to believe that implementation of Customer's additional instructions would breach applicable law to which Octopus Cloud is subject, Octopus Cloud shall inform Customer of that legal requirement and shall be entitled to refuse or suspend Contract Processing on such additional instruction until Customer modifies the instruction.

c. Octopus Cloud will put in place measures to ensure (i) that any employees authorized to perform Contract Processing will do so only in accordance with the terms of this Addendum; and (ii) that any employees who have access to Covered Personal Data have committed themselves to confidentiality.

d. Octopus Cloud will not to carry out the Contract Processing in or transfer Covered Personal Data to countries outside of Switzerland or the European Economic Area, except if Octopus Cloud implements suitable guarantees in accordance with obligations under applicable Data Protection Legislation relating to the international transfer of Personal Data (this may include the obligation of Octopus Cloud to enter into Standard Contractual Clauses with its Sub-processor), in which case Octopus Cloud will, prior to the first transfer of Covered Personal Data, inform Customer of the relevant country to which the Covered Personal Data is transferred and the guarantees put in place to ensure an adequate level of data protection.

e. Octopus Cloud will engage Sub-processors only with authorization of Customer.

   i. Customer hereby generally authorizes Octopus Cloud to engage Sub-processors, provided that Octopus Cloud enters into an agreement with its Sub-processors to that sets out obligations that are substantially similar to and alloy Octopus Cloud to comply with Octopus Cloud's obligations under this Addendum; a list of Sub-processors engaged by Octopus Cloud at any time during Customer's use of the Cloud View is 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 if (1) Octopus Cloud informs Customer in advance in an appropriate manner in writing or in text form (such as an amendment of the list of Sub-processors made available on Customer's Cloud View tenant) with appropriate advance notice; (2) Customer has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to Octopus Cloud; and (3) the subcontracting is based on a contractual agreement in accordance with applicable Data Protection Legislation.

f. Octopus Cloud will promptly notify Customer if Octopus Cloud receives a request from a Data Subject to have access to Covered Personal Data or exercise any other applicable Data Subject rights, and assist the Customer, upon request, with technical means and support insofar as reasonably possible and in exchange for separate compensation, in responding to any such complaint or request.

g. At Customer's request and in exchange for separate compensation, Octopus Cloud will provide Customer with information and support Customer may reasonably require in order to carry out a Data Protection Impact Assessment in relation to the services Octopus Cloud provides pursuant to this Addendum.

h. Octopus Cloud will permit Customer (or the duly authorized representatives or any competent regulator) to inspect and audit the Contract Processing carried out by Octopus Cloud Processing activities under this Addendum (and/or by any Sub-processors), and comply with all reasonable requests or directions by Customer to enable them to verify and/or procure that Octopus Cloud is in full compliance with the obligations under this Addendum; Octopus Cloud may claim a reasonable compensation for all costs such an inspection or audit may involve; Customer acknowledges and accepts that the afore-mentioned inspection and audit rights only apply to the extent documentation provided by Octopus Cloud, its Sub-processors or their respective auditors does not otherwise allow Customer or competent regulators to assess Octopus Cloud' compliance with the terms of this Addendum; specifically, instead of allowing for inspections or audits, Octopus Cloud or its Sub-processors may provide reports on information security or contract processing-related reports (including certifications in accordance with recognized standards) that an auditor of the Octopus Cloud or the respective Sub-processor has prepared for use in relation to all of Octopus Cloud' or the respective Sub-processor's customers.

i. Upon termination of the Contract Processing Octopus Cloud will return all Covered Personal Data to Customer (as specified in Customer's Subscription Order) or, at Customer's choice, delete all Covered Personal Data to the extent technically possible, except where applicable law requires Octopus Cloud to retain copies of such data.

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 mainly ensure that:

a. Access and authorizations are granted on the need to have;

b. Each User is assigned with a unique account;

c. Accounts are periodically reviewed to validate their relevance;

d. Generic accounts are not used;

e. Suspected compromised accounts are disabled at once.

5.2. Octopus Cloud shall:

a. in the interest of protecting the confidentiality, integrity and contractual availability of the Covered Personal Data, implement and maintain the security measures set forth in Technical and Organizational Measures provided in Appendix 1 to this Addendum; Customer accepts that Octopus Cloud may adjust or optimize Technical and Organizational Measures, provided that (1) overall, a similar or higher level of protection results from such adjustments or optimization; (2) Octopus Cloud informs Customer in advance in an appropriate manner in writing or in text form (such as an amendment of the list of Technical and Organizational Measures made available on Customer's Cloud View tenant) with appropriate advance notice

b. notify Customer as soon as reasonably possible if Octopus Cloud knows, discovers or reasonably believes that there has been (1) any unauthorized access to or acquisition of Covered Personal Data that compromises the confidentiality, integrity or contractual availability of Covered Personal Data, or (2) any unauthorized disclosure of, access to or use of any Covered Personal Data, or (3) any unauthorized intrusion into systems containing Personal Data resulting in unauthorized access or access in excess of authorization ("Data Security Breach");

c. in the event of a Data Security Breach, (1) immediately investigate, correct, mitigate, remediate and otherwise handle the Data Security Breach, including without limitation, by identifying Covered Personal Data affected by the Data Security Breach and taking sufficient steps to prevent the continuation and recurrence of the Data Security Breach; and (2) provide information and assistance needed to enable Customer to evaluate the Data Security Breach and, if applicable, to provide timely notices disclosing a Data Security Breach and to comply with any obligations to provide information that the Data Security Breach to relevant regulators.

6. Term

6.1. This Addendum shall co-terminate with Customer's subscription to Cloud View.

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

Appendix 1 – Technical and Organizational Measures

Capitalized terms not otherwise defined in this Appendix 1 have the meanings assigned to them in Customer's Subscription Order or the Data Processing Addendum.

1. Information Security Program

1.1. Octopus Cloud will maintain an information security program (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 and internal risks to security and unauthorized access to the Cloud View Service, and (c) minimize security risks, including through risk assessment and regular testing. Octopus Cloud will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the measures set forth in this Appendix.

1.2. Octopus Cloud does not have certifications in relation to the technical and organizational measures to protect personal data, but all of our external partners with which personal data are being held and hosted (most prominently T-Systems as host to the Cloud View SaaS solution and Salesforce) are GDPR-compliant and do have certifications such as SOC 2, ISO 27001, ISO 27017, ISO 27018, Trusted Cloud Data Protection Profile certification (TCDP).

With regard to T-System (hoster of the Cloud View SaaS solution in Open Telekom Cloud), please see https://www.trusted-cloud.de/de/cloudservices/2116/Open-Telekom-Cloud. Please also refer to T-System's 'Open Telecom Cloud Service Description' (https://open-telekom-cloud.com/resource/blob/data/173316/7046bdf0ff016c67f0ecb209a65d093e/open-telekom-cloud-service-description.pdf) and T—System's DEKRA-certified Privacy and Security Assessment procedures (https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/details/privacy-and-security-assessment-verfahren-342724).

With regard to Salesforce (Business Cloud Service), please refer to

a. the certification landscape (https://compliance.salesforce.com/en)

b. the security, privacy and architecture documentation (https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforcee-security-privacy-and-architecture.pdf and https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/)

2. Confidentiality

Requirements	Established Measures
a) Physical Access/Admittance Control	Cloud View SaaS Solution: ● No unauthorized access to data processing systems, e.g.: magnetic or chip cards, keys, electric door openers, plant security and/or concierge, alarm systems, video systems
b) Electronic Access Control	Cloud View SaaS Solution: ● No unauthorized use of the system, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data media

c) Internal Access Control (permissions for user rights of access to and amendment of data)	Cloud View SaaS Solution: ● No unauthorized reading, copying, modifying or removal within the system, e.g.: authorization concepts and need-based access rights and logging of system access
d) Separation Control	Cloud View SaaS Solution: ● Separate processing of data that has been collected for different purposes, e.g.: multitenancy, sandboxing

3. Integrity

Requirements	Established Measures
a) Data Transfer & Disclosure Control	Cloud View SaaS Solution: ● No unauthorized reading, copying, modifying or removal during electronic transfers or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature.
b) Input Control	Cloud View SaaS Solution: ● Definition of whether or by whom personal data was entered into, modified or removed from data processing systems, e.g.: logging, document management

4. Availability & Resilience

Requirements	Established Measures
a) Availability Control	Cloud View SaaS Solution: ● Protection against accidental or deliberate destruction and/or loss of personal data, e.g.: backup Strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), anti-virus protection, firewall, reporting paths and emergency planning
b) Data Recovery	Cloud View SaaS Solution: ● Ability to restore availability of data

5. Regular testing, assessment and evaluation of Network Security

Requirements	Established Measures
a) Tests, Assessments, Evaluations	Cloud View SaaS Solution: ● Data protection management ● Incident response management ● Default settings that promote data protection ● Order Control (i.e. no commissioned data processing without corresponding instructions from customer)