Commissioned Data Processing Agreement

between

.....

as the Controller – hereinafter referred to as the Client

and

Octopus Cloud AG, Baarerstrasse 145, CH-6300 Zug,

as the Processor - hereinafter referred to as Octopus Cloud

1. Subject matter and duration of this Processing Agreement

1.1. Subject Matter

The Subject matter of this Data Processing Agreement (hereinafter "the DPA") results from (i) the Client's Subscription to Octopus Cloud Products dated …….. (hereinafter referred to as "Customer Subscription"); and (ii) Client Relationship Management tasks performed by Octopus Cloud as a result of the Customer Subscription.

Appendix 1 is an integral part of this DPA.

This DPA is an integral part of the Customer Subscription.

1.2. Duration

The duration of this DPA corresponds to the duration of the Customer Subscription.

1.3. Applicable Data Protection Law

Even though this DPA does for convenience refer to the GDPR's provision, please note that with regard to Octopus Cloud as a Swiss company it is the Swiss Federal Data Protection Act that does directly and primarily apply. However, the EU-Commission has per Art. 45 of the GDPR made an adequacy decision with regard to Switzerland, i.e. the Swiss data protection standards are deemed equivalent to those of the EU. Data transfers to Switzerland hence shall be deemed as if these were made within the EU and are possible without additional safeguards or permissions from authorities.

2. Specification of the Data Processing

2.1. Nature and Purpose of the intended Processing of Data

Nature and Purpose of Processing of personal data by Octopus Cloud for the Client are precisely defined in the Customer Subscription.

2.2. The undertaking of the contractually agreed Processing of Data shall be carried out exclusively in Switzerland and/or within a Member State of the European Union (EU) and/or within a Member State of

the European Economic Area (EEA). The adequate level of protection in Switzerland has been decided by the European Commission (Article 45 Paragraph 3 GDPR).

Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA or Switzerland requires the prior agreement of the Client and shall only occur if the specific conditions as per applicable data protection law have been fulfilled. The adequate level of protection in any such target country

a) has been decided by the European Commission;

b) is the result of binding corporate rules;

c) is the result of Standard Data Protection Clauses;

d) is the result of approved Codes of Conduct;

e) is the result of an approved Certification Mechanism;

f) is established by other means.

2.3. Type of Data

The Subject Matter of the processing of personal data comprises the following data types/categories (List/Description of the Data Categories)

– Contact Data

– Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest)

– Customer History

– License information re: individuals

– Contract Billing and Payments Data

– Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories.

2.4. Categories of Data Subjects

The Categories of Data Subjects comprise:

– Employees, third party staff members, consultants
– Customers
– Potential Customers
– Authorized Agents
– Contact Persons
– System Users

3. Technical and Organizational Measures

3.1. Before the commencement of processing, Octopus Cloud shall document the execution of the necessary Technical and Organizational Measures, set out in advance of the awarding of the processing of data, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

3.2. Octopus Cloud shall establish the security in accordance with applicable data protection law. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons (see details in Appendix 1).

3.3. The Technical and Organizational Measures are subject to technical progress and further development. In this respect, it is permissible for Octopus Cloud to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

4.1. Octopus Cloud may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts Octopus Cloud directly concerning a rectification, erasure, or restriction of processing, Octopus Cloud will immediately forward the Data Subject's request to the Client.

4.2. Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by Octopus Cloud in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of Octopus Cloud

In addition to complying with the rules set out in this DPA, Octopus Cloud shall comply with the statutory requirements; accordingly, Octopus Cloud ensures, in particular, compliance with the following requirements:

a) Octopus Cloud is not obliged to appoint a Data Protection Officer. Mr. Cihan Gökgöz (CIO, Octopus Cloud AG, Baarerstrasse 145, CH-6300 Zug, Switzerland, Phone + 41 41 552 14 99, E-Mail cihan.goekgoez@octopus.cloud) is designated as the Contact Person on behalf of Octopus Cloud.

b) Octopus Cloud entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. Octopus Cloud and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

c) Implementation of and compliance with all Technical and Organizational Measures specified in this DPA (see details in Appendix 1).

d) The Client and Octopus Cloud shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this DPA. This also applies insofar as Octopus Cloud is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with this DPA.

f) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by Octopus Cloud, Octopus Cloud shall make every effort to support the Client.

g) Octopus Cloud shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the Technical and Organizational Measures conducted by the Client as part of the Client's supervisory powers referred to in section 7 of this contract.

6. Subcontracting

6.1. Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity

and resilience of the hardware and software of data processing equipment. Octopus Cloud shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

6.2. Octopus Cloud may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client.

a) The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement:

Name	Country	Service
T-Systems International GmbH	Hahnstrasse 43d, 60528 Frankfurt a.M., Germany	Hosting of Cloud View online modules (Germany and the Netherlands)
Deutsche Telekom Germany Regional Solutions & Products GmbH	Friedrich-Ebert-Allee 71-77, 53113 Bonn, Germany	Sub-processor to T-Systems International GmbH, 1st & 1.5 Level Support (Germany)
IT Services Hungary	Neumann Janos u 1/c, H-11117 Budapest, Hungary	Sub-processor to T-Systems International GmbH, operation and 1st and 2nd level support (Hungary)
Deutsche Telekom IT GmbH	Landgrabenweg 151, 53227 Bonn, Germany	Sub-processor to T-Systems International GmbH, user support MyWorkplace (Germany)
Strato AG	Pascalstrasse 10, 10587 Berlin, Germany	Sub-processor to T-Systems International GmbH, Service Desk (Germany)
Axivas Deutschland GmbH	Carl-Benz-Strasse 9-11, 68723 Schwetzingen, Germany	Sub-processor to T-Systems International GmbH, Service Desk (Germany)
Deutsche Telekom Individual Solutions & Products GmbH	Friedrich-Ebert-Allee 70, 53113 Bonn, Germany	Sub-processor to T-Systems International GmbH, DC Hardware Disposal and replace (Germany and the Netherlands)
GULP Solutions Services GmbH & Co.KG	Breite Strasse 137-130, 50667 Köln, Germany	Sub-processor to Deutsche Telekom Individual Solutions & Products GmbH, Service Desk (Germany)
I.T:E.N.O.S. International Telecom Network Operation Services GmbH	Lievelingsweg 125, 53119 Bonn, Germany	Sub-processor to Deutsche Telekom Individual Solutions & Products GmbH, DC Hardware disposal and replace (Germany)
Salesforce.com Inc.	Salesforce Tower 415 Mission Street, 3rd Floor San Francisco, CA 941055, USA	Support services platform provider (for sub-processors and regional data centers for EMEA please refer to the documentation specified in Appendix 1)

b) Outsourcing to subcontractors or changing the existing subcontractor are permissible when:
- Octopus Cloud submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The Client 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
- The subcontracting is based on a contractual agreement.

6.3. The transfer of personal data from the Client to the subcontractor and the subcontractor's commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

6.4. If the subcontractor provides the agreed service outside the EU/EEA, Octopus Cloud shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

6.5. Further outsourcing by the subcontractor requires the express consent of the main Client (at the minimum in text form); all contractual provisions in the contract chain shall be communicated to and agreed with each additional subcontractor.

7. Supervisory powers of the Client

7.1. The Client has the right, after consultation with Octopus Cloud, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by Octopus Cloud in his business operations by means of random checks, which are ordinarily to be announced in good time.

7.2. Octopus Cloud shall ensure that the Client is able to verify compliance with the obligations of Octopus Cloud as contemplated by applicable data protection law. Octopus Cloud undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

7.3. Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

- Compliance with approved Codes of Conduct;
- Certification according to an approved certification procedure;
- Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor)
- A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz, i.e. IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI) or ISO/IEC 27001, 27017, 27018).

7.4. Octopus Cloud may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by Octopus Cloud

8.1. Octopus Cloud shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
b) The obligation to report a personal data breach immediately to the Client
c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
d) Supporting the Client with its data protection impact assessment
e) Supporting the Client with regard to prior consultation of the supervisory authority

8.2. Octopus Cloud may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of Octopus Cloud.

9. Authority of the Client to issue instructions

9.1. The Client shall immediately confirm oral instructions (at the minimum in text form).

9.2. Octopus Cloud shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. Octopus Cloud shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Liability

10.1. Unless specified otherwise, the liability provisions as per the Customer Subscription shall apply to this DPA.

10.2. Client shall indemnify Supplier in its sphere of responsibility from all claims brought against Supplier by a person in accordance with Art. 82 para 1 GDPR. Insofar as Client is obliged to pay compensation to such persons due to Supplier's fault, Client reserves recourse against Supplier.

10.3. Supplier shall indemnify Client in its sphere of responsibility from any and all claims brought against Client by a person in accordance with Art. 82 para 1 GDPR due to the fact that Supplier infringed upon obligations under the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instruction of Client. Insofar as Supplier is obliged to pay compensation to such persons due to Client's fault, Supplier reserves recourse against Client.

10.4. If a Party (uninvolved Party) has to pay an administrative fine in accordance with Art. 83 GDPR due to misconduct of the respective other Party (misconducting Party), the misconducting Party shall fully indemnify the uninvolved Party from such administrative fines as well as all reasonable cost of legal representation in this regard. The exclusions and/or limitations of liability as agreed in the Customer Subscription apply.

11. Deletion and Return of Personal Data

11.1. Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

11.2. After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Customer Subscription, Supplier shall hand over to the Client or – subject to prior consent – destroy all data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

11.3. Documentation which is used to demonstrate orderly data processing in accordance with the relevant agreement between Client and Supplier shall be stored beyond the contract duration by Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve Octopus Cloud of this contractual obligation.

12. Signatures

For the Client

---------- ----------

Name Name

Place and Date

For Octopus Cloud AG

---------- ----------

Name Name

Place and Date

Appendix 1 - Technical and Organizational Measures

1. Certifications & Descriptions

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 hoster 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 and Pardot), please refer to the certification landscape (https://compliance.salesforce.com/en) and the security, privacy and architecture documentation under https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-security-privacy-and-architecture.pdf (Service Cloud) and https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/pardot-security-privacy-and-architecture.pdf (Pardot).

2. Confidentiality (Art. 32 Para. 1 point b GDPR)

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 (Art. 32 Para. 1 point b GDPR)

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 and Resilience (Art. 32 Para. 1 points b and c GDPR)

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 as per Art. 32 Para 1 point c of the GDPR)

5. Process of regularly testing, assessing and evaluating (Art. 32 Para. 1 point d & Art. 25 Para. 2 GDPR)

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 with the meaning of section 28 GDPR without corresponding instructions from customer)