

DATA PROTECTION ADDENDUM

Soliton Systems K.K.

(OneGate / International) Last updated: [14/03/2024]

This Data Processing Addendum and its Annexes (the “**DPA**”) is incorporated into and forms part of an agreement (the “**Agreement**”) between Soliton Systems K.K. (“**Soliton**”) and Customer in connection with Customer’s use of Soliton’s cloud services pursuant to the terms and conditions of Soliton Cloud Service Terms of Service (“**クラウドサービス実施要領**”, the “**Cloud Service Terms**”). This DPA reflects the parties’ agreement with respect to the Processing of Personal Data by Soliton on behalf of Customer in connection with the Service.

This DPA is made as of the date on which the Agreement between Soliton and Customer becomes effective (or on which the Licenses become effective, if purchased through a reseller) pursuant to the Cloud Service Terms. The parties agree to comply with the following provisions with respect to any Personal Data collected in the course of the provision of the Service to Customer.

In the event of any conflict between the terms of this DPA and the Cloud Service Terms or the applicable Service Appendix, the terms of this DPA shall prevail.

1. Definitions

- 1.1. “**Agreement**” has the meaning set forth in the first paragraph.
- 1.2. “**CCPA**” means the California Consumer Privacy Act, California Civil Code sections 1798.100 *et seq.*, as amended by the California Privacy Rights Act of 2020, including any implementing regulations.
- 1.3. “**Cloud Service Terms**” has the meaning set forth in the first paragraph.
- 1.4. “**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.
- 1.5. “**Customer**” means a customer who has purchased License(s) pursuant to the Agreement.
- 1.6. “**Data Protection Laws**” means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in connection with the Service provided by Soliton to Customer, including without limitation the GDPR and the CCPA, in each case as amended, repealed, consolidated or replaced from time to time.
- 1.7. “**DPA**” has the meaning set forth in the first paragraph.
- 1.8. “**GDPR**” the 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).

- 1.9. **“License”** means a license to use the Service and/or to use optional functions of the Service, pursuant to the Cloud Service Terms.
- 1.10. **“Personal Data”** means any information relating to an identified or identifiable natural person (where such information is protected similarly as personal data, personal information or personally identifiable information under the Data Protection Laws).
- 1.11. **“Processing,” “Process,” or “Processed”** means any operation which is performed upon Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, share, sell, or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 1.12. **“Processor”** means the entity which Processes Personal Data on behalf of the Controller.
- 1.13. **“Security Measures”** has the meaning set forth in Section 4.1.
- 1.14. **“Service”** means Soliton’s cloud services to be provided to Customer under the Agreement.
- 1.15. **“Service Appendix”** is an appendix to the Cloud Service Terms that sets forth terms and conditions and service descriptions applicable to a specific cloud service of Soliton.
- 1.16. **“Soliton”** has the meaning set forth in the first paragraph.

2. Processing of Personal Data

- 2.1. This DPA applies when Personal Data is Processed as part of the Service provided by Soliton to Customer and to the extent of the Personal Data Processed by Soliton and its sub-processor on behalf of Customer.
- 2.2. The parties acknowledge that, with regard to the Processing of Personal Data, Soliton acts as a Processor on behalf of Customer, which may act either as a Controller or a Processor, and that to the extent Processing of Personal Data is subject to the CCPA, Customer is the “business” and Soliton is the “service provider” (as those terms are defined in the CCPA).
- 2.3. The details of the Processing of Personal Data by Soliton, including the categories of the data subjects, the categories of the Personal Data Processed, the nature of the Processing, the purpose for which the Personal Data is Processed and the duration of the Processing, are set forth in Annex I.
- 2.4. The parties acknowledge and agree that Customer is providing Personal Data only for the purposes set forth in Annex I. Soliton shall not Process the Personal Data it collects as part of the Service provided to Customer outside the direct business relationship between Soliton and Customer.

3. Customer’s Instructions

- 3.1. Soliton shall Process Personal Data only on behalf of and in accordance with documented instructions from Customer and only for the specific purposes set forth in Annex I unless required to do so by the Data Protection Laws (in which case Soliton shall inform Customer of that legal requirement before Processing unless those Data Protection Laws prohibits

doing so on important grounds of public interest). Soliton shall not “sell” or “share” (as those terms are defined in the CCPA) the Personal Data.

- 3.2. The parties agree that Customer’s use of the Service in accordance with the Cloud Service Terms to which it has agreed to, including this DPA, constitutes Customer’s instructions to Soliton. Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws, and Soliton shall not be required to comply with Customer’s instructions if such instructions would violate any Data Protection Laws. Soliton shall, immediately inform Customer if, in Soliton’s opinion, instructions given by Customer violate any Data Protection Laws. Subsequent instructions may also be given by Customer throughout the duration of the Processing of Personal Data. These instructions shall always be documented.
- 3.3. In Customer’s use of the Service, Customer shall be responsible for complying with all requirements that apply to it under the Data Protection Laws with respect to its Processing of Personal Data and the instructions it issues to Soliton.

4. Technical and Organizational Measures

- 4.1. Soliton shall at least implement the technical and organizational measures specified in Annex II to ensure the security of the Personal Data (the “**Security Measures**”). This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the Personal Data. In assessing the appropriate level of security, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for the data subjects. Notwithstanding anything to the contrary, Soliton may modify or update the Security Measures at its discretion; provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.
- 4.2. Soliton shall grant access to the Personal Data undergoing processing to its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Service. Soliton shall ensure that its personnel authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Compliance and Audit

- 5.1. The parties shall be able to demonstrate compliance with the terms of this DPA. Soliton shall deal promptly and adequately with inquiries from Customer regarding the Processing of Personal Data in accordance with this DPA.
- 5.2. Soliton shall make available to Customer all information necessary to demonstrate compliance with the obligations set out in this DPA. At Customer’s request, Soliton shall also permit and contribute to audits of the Processing activities covered by this DPA, at reasonable intervals (no more than once per calendar year) or if there are indications of non-compliance; provided that Customer shall reimburse Soliton for any time expended for such audits at Soliton’s then-current professional service fees, and before conducting such audits, the parties shall mutually agree on the scope, timing and duration of the audit in

addition to the reimbursement rate for which Customer shall be responsible. Customer may choose to conduct the audit by itself or mandate an independent auditor.

- 5.3.** The parties shall make the information referred to in this DPA, including the results of any audits, available to the competent supervisory authority/ies upon request.

6. Sub-processing

- 6.1.** Customer hereby grants its general authorization to engage sub-processors. Soliton's current sub-processors are listed in Annex III. If required by applicable Data Protection Laws, Soliton shall specifically inform in writing Customer of any intended changes of the list in Annex III through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving Customer sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). Upon request, Soliton shall provide Customer with the information necessary to enable Customer to exercise the right to object.
- 6.2.** Where Soliton engages any sub-processor for Processing of the Personal Data as part of the provision of the Service to Customer, Soliton shall do so on the basis of a written contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on Soliton in accordance with this DPA. Soliton shall ensure that the sub-processor complies with the obligations to which Soliton is subject pursuant to this DPA and the GDPR, if applicable.
- 6.3.** At Customer's request, Soliton shall provide a copy of such a sub-processor agreement and any subsequent amendments to Customer. To the extent necessary to protect business secret or other confidential information, including Personal Data, Soliton may redact the text of the agreement prior to sharing the copy.
- 6.4.** Soliton agrees to be fully responsible to Customer for the performance of the sub-processors to the same extent as Soliton would be liable if performing the services of the sub-processors under the terms of the Soliton Cloud Terms.

7. International Transfer

- 7.1.** Customer acknowledges and agrees that Soliton may transfer the Personal Data it collects on behalf of Customer in the course of the Service within the EEA and/or Japan. To the extent that Processing of Personal Data is subject to the GDPR, any such transfer of Personal Data by Soliton shall take place in compliance with Chapter V of the GDPR..

8. Assistance to Customer

- 8.1.** Soliton shall promptly notify Customer of any request it has received from the data subject in connection with the Service. Soliton will not respond to the request itself.
- 8.2.** Soliton shall assist Customer in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the Processing, in complying with Customer's instructions.
- 8.3.** Soliton shall assist Customer in fulfilling the obligations it may be subject to under the applicable Data Protection Laws. In particular, to the extent that Processing of Personal

Data is subject to the GDPR, in addition to Soliton's obligation to assist Customer as set out above, Soliton shall assist Customer in ensuring compliance with the following obligations, taking into account the nature of the Processing of the Personal Data by Soliton on behalf of Customer and the information available to Soliton:

- 8.3.1.** the obligation to carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;
- 8.3.2.** the obligation to consult the competent supervisory authority/ies prior to Processing where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by Customer to mitigate the risk;
- 8.3.3.** the obligation to ensure that Personal Data is accurate and up to date, by informing Customer without delay if Soliton becomes aware that the Personal Data it is Processing is inaccurate or has become outdated;
- 8.3.4.** the obligations in Article 32 of the GDPR.

9. Notification of Personal Data Breach

- 9.1.** In the event of a breach of Personal Data, Soliton shall cooperate with and assist Customer for Customer to comply with its obligations under the Data Protection Laws, where applicable, taking into account the nature of Processing and the information available to Soliton.

9.2. Data Breach concerning Personal Data Processed by Customer

- 9.2.1.** In the event of a Personal Data breach concerning Personal Data Processed by Consumer, Soliton shall assist Consumer:
 - (a) in notifying the data breach to the competent supervisory authority/ies, without undue delay after Customer has become aware of it, where relevant;
 - (b) in obtaining such information as shall be stated in Customer's notification to the competent supervisory authority/ies; and
 - (c) in complying with the legal obligation to communicate the data breach to the data subject.

9.3. Data Breach concerning Personal Data Processed by Soliton

- 9.3.1.** In the event of a Personal Data breach concerning Personal Data Processed by Soliton, Soliton shall notify Customer without undue delay after Soliton having become aware of the breach. Such notification shall contain, at least:
 - (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
 - (b) the details of a contact point where more information concerning the personal data breach can be obtained; and
 - (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

10. Non-compliance with this DPA and Termination

- 10.1.** In the event that Soliton is in breach of its obligations under this DPA, Customer may instruct Soliton to suspend the Processing of Personal Data until Soliton complies with this DPA. Soliton shall promptly inform Customer in case it is unable to comply with this DPA.
- 10.2.** Following termination of the Service, Soliton shall delete all Personal Data Processed on behalf of Customer and delete existing copies thereof unless Data Protection Laws require storage of the Personal Data within 45 days of the termination. Until the Personal Data is deleted, Soliton shall continue to ensure compliance with this DPA.

11. Amendment

- 11.1.** Notwithstanding anything to the contrary in this DPA and without prejudice to Section 3 (Customer's Instructions) and Section 4 (Technical and Organizational Measures), Soliton reserves the right to amend the terms of this DPA by notifying Customer of the proposed amendments and its effective date through its webpage and/or by email to the email address registered by Customer or by a reseller from which Customer has purchased Licenses for Service-related communication. In this case, Customer is deemed to have agreed with the amended DPA, and the Service provided after the effective date is subject to such amended DPA.

ANNEX I: DESCRIPTION OF THE PROCESSING

Subject matter of processing

- The performance of the Service pursuant to the Cloud Service Terms (including the DPA)

Categories of data subjects whose Personal Data is Processed

- Customers and business partners and vendors of Customers (who are natural persons)
- Employees, contractors and contact persons of Customers and business partners and vendors of Customers (who are natural persons)
- Employees, agents, advisors, contractors, or any user authorized by Customer to use the Service (who are natural persons)

Categories of Personal Data Processed

- Identification and contact information (email address, user ID)
- Configuration information (further details are described in the Soliton OneGate Administrator's Manual)
- Device information (device product name, version, IMEI, UDID, and MAC address)
- System logs (as described in the Soliton OneGate Administrator's Manual)
- Certificate authority logs (DN and serial number of the certificate)
- System logs (administrator account, IP address of operating terminal)
- Logs related to user authentication (user ID, device MAC address)

Sensitive data (as defined in the GDPR) processed

The parties do not anticipate the Processing of sensitive data.

Nature of the Processing

Personal Data will be processed in accordance with the Cloud Service Terms (including the applicable Service Appendix and this DPA) and may be subject to the following Processing activities:

1. Storage and other Processing necessary to provide, maintain and improve the Service provided to Customer; and/or
2. Disclosure in accordance with the Cloud Service Terms (including the applicable Service Appendix and this DPA) and/or as compelled by Data Protection Laws.

Purpose(s) for which the Personal Data is processed on behalf of Customer

- Processing in order to provide the Service to Customer in accordance with the the Cloud Service Terms (including the applicable Service Appendix and this DPA).
- Processing initiated by users in their use of the Service.

- Processing to comply with other documented, reasonable instructions provided by Customer where such instructions are consistent with the terms the Cloud Service Terms (including the applicable Service Appendix and this DPA).

Duration of the Processing

- Processing by Soliton only takes place during the duration of the Service. The Personal Data will be deleted within 45 days after termination of the Service.

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Soliton implements and provides at least the following technical and organizational measures for the security of the Personal Data it Processes in connection with the Service.

- All routes to access the OneGate system are encrypted to protect the contents of communications to the system. For the encryption, Soliton complies with the TLS Encryption Guidelines issued by Information-technology Protection Agency, Japan (IPA).
- All data stored in the cloud service infrastructure system is encrypted using Google Cloud Platform's function.
- Physical and environmental security: Soliton OneGate service infrastructure is hosted on Google Cloud Platform and logically and physically secured from Soliton's internal IT systems.
- To maintain the availability of the Soliton OneGate service, the service utilizes a redundancy configuration within the same Google Cloud region so that if one data center is down, the service can continue to be available through another data center. All data is backed up on a daily basis.
- Soliton maintains an ISMS certification, and its system is audited by an independent auditor. Soliton's Management review periodic report submitted by its system administrators regarding its Information System Management System. The reports include how the instructions given to the Management in the previous review have been taken care of.
- Soliton's personnel logging on to administrator accounts to access the systems within the Soliton OneGate infrastructure are required to use Multi-Factor Authentication.
- Users of the OneGate service are required to use a digital certificate-based Multi-Factor Authentication to use the Soliton OneGate service.
- Soliton implements a room entrance management system that is designed to ensure that only personnel who are authenticated can enter the rooms from which the OneGate service is accessible.
- The OneGate service system logs are regularly monitored and stored on Google Cloud Platform.
- Soliton implements a system that automatically sends alerts regarding certain unusual or suspicious events.
- The number of the ports, protocol and services accessible to the Soliton OneGate system are restricted to the minimum required level.
- Soliton has established and comply with its security requirements policy for OneGate concerning access to and the retention, processing and disposal of data for the OneGate service (confidential).

- Soliton implements and maintains its physical security control rules, which include, among others, the following
 - No business data must be stored in laptops or portable devices.
 - If a laptop or a portable device is lost, the administrator immediately disables access from the device to all business data controlled by Soliton.
 - No data on the OneGate system must be copied or transferred outside of the system.
- Soliton requires that any sub-processor it engages to provide the Service on its behalf in connection with this DPA does so solely on the basis of a written contract which imposes on such sub-processor terms no less protective of Personal Data than those imposed on Soliton in this DPA.

ANNEX III: LIST OF SUB-PROCESSORS

Following is a list of the sub-processors Soliton currently engages for Processing activities:

1. Google LLC

Address: 1600 Amphitheatre Parkway, Mountain View, California, 94043

Location of data center: Germany

Subject matter, nature and purpose of processing: hosting and infrastructure

Duration of processing: during the duration of the Service. The personal data will be deleted within 45 days after termination of the Service.

2. Soliton Systems Europe N.V.

Address: Barbara Strozilaan 364, 1083 HN Amsterdam, The Netherlands

Location of data center: no data center.

Subject matter, nature and purpose of processing: communication with Customers and resellers from which Customers have purchased the Licenses.

Duration of processing: during the duration of the Service. The personal data will be deleted within 45 days after termination of the Service.

3. Luvina Software Joint Stock Company

Address: 4F Hoa Binh Tower, 106 Hoang Quoc Viet Str., Cau Giay Dist., Ha Noi, Vietnam

Location of data center: no data center.

Subject matter, nature and purpose of processing: operation and management of the Service.

Duration of processing: during the duration of the Service. The personal data will be deleted within 45 days after termination of the Service.