DATA PROCESSING AGREEMENT

Effective December 11th 2024
SSH Communications Security and its subsidiaries as the processors

1. DEFINITIONS

"Company" refers to SSH Communications Security and its subsidiaries;

"Data Protection Legislation" means the GDPR and other applicable data protection laws;

"GDPR" means the General Data Protection Regulation of the European Union (2016/679/EU);

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Personal Data Breach" means an event leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data processed;

"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.

2. GENERAL

This Data Processing Agreement ("DPA") sets out the terms and conditions under which the Company processes the Customer's Personal Data. The purpose of this DPA is to take into account the responsibilities and obligations set by the GDPR.

The Customer is the data controller of the Customer's Personal Data Processed in connection with the service agreed in the Agreement. As a data controller, the Customer determines the purposes and means of the Processing of Personal Data. The Company is the data processor, who Processes the said Personal Data on behalf of and by the order of the Customer as agreed in this DPA. The Parties may agree more specifically on the categories of data subjects, categories of Processing carried out by Supplier, data security procedures and the purpose for which the Company Processes the Customer's Personal Data e.g. by using the template attached as Schedule A.

The Parties understand that authorities may issue orders and guidelines within the scope of the GDPR after the signing of the Agreement. The Parties commit to, if necessary, amend this DPA based on such orders and guidelines.

The Parties shall inform each other of the contact details of their possible data protection officers.

3. RESPONSIBILITIES OF THE CUSTOMER

The Customer shall process the Personal Data in compliance with the Data Protection Legislation. The Customer is responsible for the lawfulness and completeness of the possible written instructions on the Processing of Personal Data it provides to Company and that there are no defects or errors in the said instructions. Possible changes to the instructions and possible cost effects shall always be agreed on separately in writing.

The Customer is responsible for the Personal Data provided to the Company and the lawfulness of the Processing during the whole term of this DPA. The Customer is responsible for providing all appropriate notices and information related to the Processing of Personal Data to the data subjects in accordance with applicable laws. The Company does not monitor the content, quality or timeliness of the Personal Data provided by the Customer.

The Customer shall ensure that the Processing and the purpose and grounds for it are in compliance with the Data Protection Legislation. The Customer shall also ensure that Personal Data has been collected in accordance with the Data Protection Legislation and that the Customer has the right to transfer the Personal Data to be Processed by the Company as set out in this DPA.

The Parties do not intend to transfer any of the controller's legal obligations arising from the Data Protection Legislation to the Processor with this DPA.

4. RESPONSIBILITIES OF THE COMPANY

The Company shall Process the Personal Data in accordance with the Data Protection Legislation and the possible separately agreed written instructions , unless otherwise required by law applicable to the Company. In such case, the Company shall inform the Customer of such legal requirement before the Processing, unless the applicable law prohibits such notification. For the sake of clarity, the Customer will always be deemed to have instructed the Company to provide the services related

to the Processing of Personal Data agreed under the Agreement.

Taking into account the nature of the Processing, the Company shall assist and support the Customer with appropriate technical and organisational measures chosen byt Company so that the Customer can fulfil its obligation to respond to requests concerning the exercise of the following rights of the data subjects, as set out in Chapter III of the GDPR (provided that the data subject has the said right under the GDPR):

a) right of access to the Personal Data;
b) right to rectification and erasure;
c) right to restriction of Processing;
d) right to Personal Data portability; and
e) right to object to Processing of Personal Data.

In case a Party receives a request concerning the use of the data subject's rights, the Party receiving the request shall notify the other Party of the request immediately and at the latest on the day following the receipt of the request, if fulfilment of the request requires any actions from the other Party. The notification will contain all information necessary to the other Party to fulfil the request. The Company is entitled to charge the Customer for all actions taken to fulfil the request of the data subject on a time and material basis in accordance with its price list applicable at the time. Taking into account the nature of the Processing, the Company shall implement the functionalities concerning the fulfilment of the data subject's rights provided for in sections 5 c-d as a part of the agreed service only as of 25 May 2018.

Taking into account the nature of the Processing and information available to the Company, the Company shall assist the Customer in ensuring compliance with the following obligations under Articles 32-36 of the GDPR (taking into account the nature of the Processing and the information available to the Company):

ensuring the security of Processing by implementing appropriate technical and organisational measures;

notification of Personal Data Breaches to supervisory authority and the data subjects;

participating in data protection impact assessment if such impact assessment is necessary under Article 35 of the GDPR; and

participating in the prior consultation of the supervisory authority if such prior consultation is necessary under Article 36 of the GDPR.

The Company shall assist the Customer only to the extent required of a data processor in the Data Protection Legislation. The Company is entitled to charge the Customer for the aforementioned measures on a time and material basis in accordance with its price list applicable at the time.

5. DATA SECURITY

The Parties undertake to implement the technical and organisational measures commonly used in the industry to protect the Personal Data. In connection with agreeing on the implementation of such measures, the Parties shall in planning and implementation take 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. When assessing appropriate level of security, the Parties shall also take into account the risks of the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise Processed.

Such measures include e.g.:

a) pseudonymisation and encryption of Personal Data;
b) the ability to ensure the continuing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of data Processing.

The aforementioned measures are examples of how the Parties may ensure the security of the Processing of Personal Data. The Parties may separately agree in writing (using e.g. the template in Schedule A) on the aforementioned measures or other data security procedures that the Company shall implement in the Processing of Personal Data. The Customer shall ensure appropriate and sufficient data security of the equipment and IT environment under its control. Unless agreed otherwise in the Agreement, the Customer shall be responsible for taking backups of the Personal Data and the verification of the functionality of the backups.

The Customer shall inform the Company of all issues related to the Personal Data provided by the Customer, such as risk assessment and the inclusion of special categories of Personal Data, which issues affect the technical and organizational measures implemented under this DPA. For the sake of clarity, possible changes to the data security procedures shall be agreed in writing and the cost impacts of such changes will always be agreed separately in writing.

The Company shall ensure that the persons Processing Personal Data are committed to confidentiality or are under an appropriate statutory obligation of confidentiality. The Company shall implement

necessary measures to ensure that the said persons only process Personal Data in accordance with the Data Protection Legislation and possible separately agreed instructions.

6. TRANSFER OF PERSONAL DATA

Unless otherwise agreed in writing, the Company has the right to transfer Personal Data outside the EU or EEA in accordance with the Data Protection Legislation. The Company shall be entitled to transfer the Personal Data freely within the EU or EEA for the purpose of providing the agreed service.

7. SUBCONTRACTORS

The Company is entitled to use subcontractors in the provision of the service and the related Processing of Personal Data. At the time of signature of this DPA, the Company shall notify the Customer of the subcontractors used in the Processing of Personal Data. The Company shall be responsible that its subcontractors Process the Personal Data in accordance with this DPA and the Data Protection Legislation.

The Company shall notify the Customer if it plans on changing or adding subcontractors participating in the Processing of Personal Data. The Customer is entitled to object to such changes on reasonable grounds. The Customer shall notify the Company of the objection without undue delay after receiving the said notice from the Company. Should the Customer not accept the change or the addition of a subcontractor, the Company has the right to terminate the Agreement with 30 days' notice.

8. PERSONAL DATA BREACHES

Each Party shall notify the other Party without undue delay, if it becomes aware of a Personal Data Breach. When notifying the Company of a Personal Data Breach, the Customer shall provide tot Company all information that can be deemed to help in the investigation, restriction and prevention of the Personal Data Breach. The Parties may separately agree on the notification procedure more specifically. Unless otherwise agreed by the Parties, the notification will be made to the contact person informed by each Party.

When notifying the Customer of a Personal Data Breach the Company shall, to the extent such information is available to the Company, provide the Customer with the following information:

a) a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned (as far as the information is available to the Company);
b) the contact information of the Company's data protection officer or other contact point where more information can be obtained;
c) a description of the likely consequences of the Personal Data Breach; and
d) a description of the measures taken by the Company to address the Personal Data Breach and the measures taken by the Company to mitigate the adverse effects of the Personal Data Breach.

If the Personal Data Breach is caused by a reason that is under the responsibility of the Customer, the Customer shall be liable for the Company's costs resulting from the Personal Data Breach. The Customer shall be responsible for notifying the supervisory authority and the data subjects of the Personal Data Breach as set out in the GDPR.

9. RECORDS OF PROCESSING ACTIVITIES

The Company shall maintain a record of Processing activities carried out behalf of the Customer. The record contains the following information:

a) the name and contact details of the Customer, the Company and the Company's possible data protection officer and information about possible subcontractors;
b) the categories of Processing carried out behalf of the Customer;
c) information on transfers of Personal Data outside the EU or EEA; and
d) where possible, a general description of the technical and organisational safety measures implemented in accordance with section 6 of this DPA.

10. RIGHT TO AUDIT

During the term of the Agreement, the Customer or an independent third party auditor appointed by the Customer, which third party may not be the Company's competitor, will have the right to audit the Company's compliance with the obligations addressed to it under this DPA. The subject of the audit will be the Company's relevant material related to the Processing of the Customer's Personal Data and the Company's systems and premises used in the Processing of Customer's Personal Data. The audit may be carried out no more than once per year and the Company shall be notified of the audit in writing at least 30 days in advance. However, the Company shall always allow the regulatory authority supervising the Customer's business to conduct audits targeted at the Customer's data processor's operations. The relevant parts of this DPA will be applied to such audits.

The Company shall participate in the audit and provide to the auditor information required to demonstrate the

Company's compliance with the requirements addresses to it under this DPA. The audit may not interfere with the Company's operation of services and the auditor will not be entitled to access information of the Company's customers or partners. Should the Customer not be the one performing the audit, the auditor will enter into a confidentiality agreement with the Company prior to the execution of the audit.

The Customer shall bear all costs resulting from the audit and compensate the Company for all costs incurred as a result of the audit. If the audit reveals material deficiencies in the Company's performance, the Company shall bear its own resulting from the audit.

11. END OF THE PROCESSING OF PERSONAL DATA

Upon termination of the Agreement and provision of service related to the Processing of Personal Data, the Company undertakes, in accordance with the Customer's written request, to delete or return the Personal data to the Customer. Additionally, upon termination of the Agreement, the Company shall delete all existing copies of the Personal Data, unless the Company is required to store the said Personal Data under applicable law or regulation. The Company is entitled to charge the Customer for the return or destruction of the Personal Data on a time and material basis in accordance with its price list applicable at the time. The Parties may agree more specifically on the practices related to the deletion or return of Personal Data.

12. DAMAGE CAUSED BY THE PROCESSING OF PERSONAL DATA

If a data subject suffers damages due to a breach of the GDPR, each Party shall itself be liable for the damage caused to the data subject in accordance with Article 82 of the GDPR. Each Party shall also itself be liable for any administrative fines imposed by a supervisory authority to it in accordance with Article 83 of the GDPR.

The limitation of liability clause of the Agreement is applied to this DPA.

13. SCHEDULES

Schedule A	Template for description of the Personal Data Processed by the Company

Schedule A: Description of the Personal Data Processed
The Parties may amend or update this schedule in writing, if necessary.

1 The purpose of the processing

The Company shall process Personal Data only for the following purpose: Provision of services under the Main Agreement.

2 Contents of the processing

The Company shall perform the following Processing activities on the Personal Data:

☒ Collection	☐ Consultation
☒ Recording	☒ Use
☒ Organisation	☐ Making data available (disclosure of data by e.g. transmission or dissemination)
~~☐ Structuring~~	☐ Alignment or combination
☒ Storage	☐ Restriction
☒ Adaptation, alteration	☒ Erasure and destruction
☒ Retrieval	☐ Other processing operations:

3 Categories of data subjects and Personal Data

The Company shall Process the following categories of data subjects and Personal Data:

Administrative users (data might include e.g. username, forename, surname, IP-address, e-mail address, profile picture, possibly phone number, device identifiers, users browser identifier)

End user information of the users of Information Security products are saved in the product (data might include e.g. forename, surname, possibly e-mail address, SSN or similar personallista identifier, IP-address profile picture, device identifiers, users browser identifiers, preferred language, location data, conversation content)

Applicable data security procedures:

The Company shall comply with its own data security guidelines when Processing Personal Data. For more information regarding the processing, please visit at https://www.ssh.com/legal/website_data_privacy. The Company shall also implement the following data security procedures:

- All databases including the above defined Personal Data encrypted and SSN and similar data is also separately encrypted.