Data Processing Amendment Agreement
(including EU Standard Contractual Clauses)

(hereinafter referred to as "**Terms of Data Processing**")
by and between

1. Graylog, Inc., a Delaware corporation, located at 1301 Fannin St., Suite 2140, Houston, TX 77019

- hereinafter referred to as "**Graylog**" -

and

2. [Please insert name and address of the Customer

- hereinafter referred to as "**Customer**" -

- Graylog and Customer hereinafter referred to as "**Parties**" and each as "**Party**" -

PREAMBLE

Graylog is a software company which offers log management and security software and/or support and maintenance services, hereinafter altogether called ("**Services**") in accordance with "Enterprise General Terms," "Hosted Service Terms," and "Support Terms" as entered into between the Parties (hereinafter together known as "**All Terms**"). These Terms of Data Processing forms part of these "All Terms."

In the course of providing the Services, Graylog will process personal data in compliance with "Applicable Law."

These Terms of Data Processing regulate the data protection obligations of the Parties when processing Customer Personal Data under All Terms and will reasonably ensure such processing will only be rendered on behalf of and under the Instructions of Customer and in accordance with "Applicable Law"

1. DEFINITIONS

In addition to the definitions in the SCC, the following shall apply:

– "**Instruction**" means any documented instruction, submitted by Customer to Graylog, directing Graylog to perform a specific action with regard to personal data. Instructions shall initially be specified in All Terms and may, from time to time thereafter, be amended, supplemented or

replaced by Customer by separate written or text form instructions, provided that such instructions still fall within the scope of the Services. Instruction issued for the purpose of complying with statutory claims under the General Data Protection Regulation (EU) 2016/679 (GDPR) such as rectification, erasure, restriction or portability of personal data fall within the scope of the Services.

– **“Affiliate”** of any specified party means any other person directly or indirectly controlling or controlled by or under common control with such specified person. For the purposes of this definition, “control” (including, with correlative meanings, the terms “controlled by” and “under common control with”), as used with respect to any party, shall mean the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of such party, whether through the ownership of voting securities or by agreement or otherwise.

– "**Applicable Law**" means all data protection laws, rules and regulations applicable to either party’s processing of personal information under these Terms of Data Processing, including the processing of personal data. Applicable Law includes but is not limited to the Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, and any European Economic Area (“EEA”) or EEA member state law, regulation, act, measure or guidance implementing the Directive, and Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, and any law, regulation, act, measure, or guidance implementing the GDPR, as well as any other data protection privacy and information security laws and regulations that may from time to time apply to Personal Data. References to “Applicable Law” mean the Applicable Law regarding data protection as may be amended, modified, supplemented, or restated.

– Terms used but not defined in this Section or in the SCC, including but not limited to "personal data", "personal data breach", "processing", "controller", "processor" and "data subject", shall have the same meaning as set forth in Art. 4 GDPR. Where the scope of the definitions in Art. 4 GDPR go beyond of what is defined in the SCC, the broader understanding shall apply.

2. AMENDMENT OF ALL TERMS

2.1 These Terms of Data Processing amend All Terms with respect to any processing of Customer Personal Data provided by Customer or Customer’s affiliates.

2.2 For purposes of these Terms of Data Processing, Customer and Graylog agree that Customer, and/or its Affiliate in the EU (“EU Customer Affiliate”) is the controller of personal data and Graylog is the Processor of such data, except when Customer or EU Customer Affiliate acts as a processor of personal data, in which case Graylog is a subprocessor.

3. DATA PROCESSING AND STANDARD CONTRACTUAL CLAUSES

3.1 Any processing operation as described in Sec. 5. shall be subject to these Terms of Data Processing which include the SCC as contained in **Exhibit A** whereby the SCC shall prevail over any conflicting clauses in All Terms or these Terms of Data Processing.

3.2 The Parties agree that the SCC shall be directly binding between Graylog as Data Importer (as defined therein), Customer and each EU Customer Affiliate as Data Exporter (as defined therein) in relation to the personal data provided by Customer or such EU Customer Affiliate.

3.3 Customer is authorized to enter into these Terms of Data Processing on behalf of its EU Customer Affiliates in which case each EU Customer Affiliate will have the same rights and obligations as referred to Customer with the exception of this Sec. 3.3. Alternatively, each EU Customer Affiliate can co-sign these Terms of Data Processing. Customer is responsible for ensuring that each of the EU Customer Affiliates is bound by these Terms of Data Processing.

3.4 References to various Articles and terms from the Directive 95/46/EC in the SCC will be treated as references to the relevant and appropriate Articles in the GDPR.

4. INTERNATIONAL DATA TRANSFERS

4.1 Graylog agrees and warrants that it has no reason to believe that the Applicable Law, including any requirements to disclose Customer Personal Data or measures authorizing access by public authorities, prevents Graylog from fulfilling its obligations under these Terms of Data Processing and the SCC contained herein.

4.2 Graylog shall promptly notify Customer if Graylog becomes aware of any laws or change in law, government policies or jurisprudence in particular if any such law or government policies or jurisprudence has a substantial adverse effect on the warranties and obligations provided by this Agreement.

4.3 Graylog certifies that (i) it has not purposefully created back doors (non-transparent access capabilities) or similar programming that could be used to access the system and/or Customer Personal Data (ii) it has not purposefully created or changed its business processes in a manner that facilitates unauthorized access to Customer Personal Data or systems, and (iii) that Applicable Law does not require Graylog to create or maintain back doors or to facilitate unauthorized access to Customer Personal Data or systems or for Graylog to be in possession or to hand over keys to decrypt the Customer Personal Data.

4.4 To mitigate risks to the rights and freedoms of data subjects, the Parties agree that in the case of a transfer of Personal Data to a third country not providing an adequate level of protection, the following provisions will apply to the Parties in addition to the SCC:

4.4.1 As provided for in the SCC, Graylog undertakes to implement and maintain appropriate technical and organizational security measures as described in Annex 2 of **Exhibit A**. The Parties acknowledge that the technical measures should reflect the risks associated with the transfer of Customer Personal Data to a third country not providing an adequate level of protection.

4.4.2 Customer will ensure that data subjects will be informed about where and by whom their data is processed.

4.4.3 In addition to the SCC, Graylog represents and warrants that it will promptly notify the Customer and, where possible and in cooperation with Customer, also the data subjects

about any legally binding request for disclosure of or actual or documented access attempts by public authorities to Customer Personal Data by a law enforcement authority unless otherwise prohibited by Applicable Law. Such notification shall generally include information about the Customer Personal Data requested, the requesting authority, the legal basis for the request and the response provided. If such notification is prohibited, Graylog will seek further guidance from a competent supervisory authority. If Graylog is prohibited from disclosing such information to the data subject by law, it will inform Customer of any request received from the competent supervisory authorities. The data subject can enforce this Sec. 4.4.3 against Graylog in accordance with the requirements the SCC.

4.4.4 Indemnification pursuant to Sec. 9.1 is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Graylog´s infringement of the GDPR.

5. SUBJECT MATTER, DURATION, NATURE AND PURPOSE, AND SPECIFICATION OF PROCESSING OPERATIONS

5.1 The subject matter, nature and purpose of the processing are described in All Terms, Annex 1 of the SCC in **Exhibit A** and this Sec. 5.1.

5.1.1 For On-Premise products, Graylog does not process or store Customer Content, except to the extent it may be included in diagnostic files submitted in connection with Graylog's Support services. Unless provided for otherwise in All Terms, the processing will be limited to when rendering support and maintenance services for on-premise solutions. When providing support or maintenance services, there shall be no access to or processing of Customer Personal Data but incidental access to Customer Personal Data cannot be excluded.

5.1.2 For Cloud-based solutions, Graylog may use approved sub-processors listed on Index III of the SCCs ("Exhibit B"), to collect usage analytics and data from Customer's or its EU Customer Affiliate's logged-in users. Such processing, unless provided otherwise in the All Terms, is necessary for Graylog to assess the performance and usability of the Cloud-based solutions, as well as for product improvement and enhancement. Customer and its EU Customer Affiliates should review Graylog's privacy policy at [insert url] to review Graylog's policy regarding the use and security of such data, which may include personal data of Customer's and its EU Customer Affiliate's users.

5.2 The categories of personal data and data subjects which may be concerned by the processing are listed Annex 1 of the SCC in **Exhibit A**.

5.3 The duration of the processing shall correspond to the duration of these Terms of Data Processing as set forth in Sec. 11.

6. GRAYLOG'S OBLIGATIONS

6.1 Graylog shall in the course of providing Services process Customer Personal Data only on behalf of and under the documented Instructions of Customer unless otherwise required to do so by

Applicable Law; in such a case, Graylog shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (the corresponding SCC shall remain unaffected). Graylog is permitted to anonymize Customer Personal Data and use such anonymized data for own research and development purposes.

6.2 Graylog shall take steps reasonably necessary to ensure that any natural person acting under its authority who has access to Customer Personal Data does not process any Customer Personal Data except on Instructions from Customer, unless Graylog, or he/she is otherwise required to do so by EU or Member State law.

6.3 Graylog ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that the obligation will remain after termination of these Terms of Data Processing.

6.4 Technical and Organizational Data Security Measures

6.4.1 The measures specified in Annex 2 of the SCC in **Exhibit A** are subject to technical advancements and development (the SCC shall remain unaffected).

6.4.2 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, Graylog shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Art. 32 GDPR.

6.4.3 When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

6.4.4 If Graylog significantly modifies measures specified in Annex 1 of the SCC in **Exhibit A**, such modifications have to meet the obligations pursuant to Sec. 6.4.2 and 6.4.3. Customer shall not refuse to accept any modification that meets the requirements pursuant to Sec. 6.4.2 and 6.4.3.

6.4.5 Graylog shall implement a data protection management procedure according to Art. 32 para 1 lit. d) GDPR, for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to reasonably ensure the security of the processing. Graylog will further, by way of regular self-audits, reasonably ensure that the processing of Customer Personal Data conforms with the provisions as agreed with Customer or to Customer's Instructions.

6.5 Graylog shall, while taking into account the nature of the processing, assist Customer through appropriate technical and organizational measures, with the fulfilment of Customer's obligations to respond to requests for exercising rights of data subjects in accordance with Applicable Law, in particular Art. 15 through 18 and 21 GDPR.

6.6 Audit Rights

6.6.1 Graylog will contribute to audits requested by Customer, not more than once annually (except in the event of a Data Breach or request from a Supervisory Authority) to demonstrate Graylog's compliance with its obligations under this DPA. In the case of On-Premises products, we do not access, process, or store Customer data unless requested to do so by Customer. If so requested, we will provide information about the data instructed to be stored. We will also provide information maintained in our ticket support system to demonstrate Graylog's compliance with its obligations as a Data Processor.

6.6.2 If Customer is required under Data Protection Law to request any further information to confirm Graylog's compliance with its obligations under this DPA, such additional information (including any on-site inspections) will be provided and/or conducted at Graylog's then-current Professional Services rates, taking into account the amount of resources and time required. Customer and Graylog will mutually agree upon the scope, timing and duration of any on-site inspection, including with respect to any third-party inspector selected by the Customer. Customer will promptly notify Graylog of any non-conformance discovered during an on-site audit.

6.7 Notification Duties

6.7.1 Graylog shall inform Customer without undue delay in text form (e.g. letter, fax or e-mail) of the events listed in the SCC and the following events:

- Requests from third parties including such from a data protection supervisory authority regarding Customer Personal Data;

- Threats to Customer Personal Data in possession of Graylog by garnishment, confiscation, insolvency and settlement proceedings or other incidents or measures by third parties. In such case, Graylog shall immediately inform the respective responsible person/entity that Customer holds the sovereignty and ownership of the personal data.

The corresponding SCC shall remain unaffected.

6.7.2 For the purpose of complying with the SCC and for enabling Customer to comply with its own data breach notification obligations pursuant to Art. 33 para 1 GDPR and Art. 34 para 1 GDPR, Graylog shall notify Customer without undue delay after becoming aware of a personal data breach. Such notice will, if possible, include the following information:

- 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;

- a description of the measures taken or proposed to be taken by Graylog and/or Customer to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects; and

- any further information which is available and known to Graylog and (i) that is necessary for Customer to comply with Customer's notification obligations

according to this Sec. 6.7.2 and (ii) which Customer does not otherwise have access to.

- name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing these Terms of Data Processing.

6.8 Rectification, Erasure (Deletion), Restriction

6.8.1 At Customer's request, Graylog shall conduct a data protection-compliant destruction of data media and other material provided by Customer. Alternatively, at the request of Customer, Graylog shall provide the data carriers and other material to Customer or store it on Customer's behalf.

6.8.2 Without prejudice to the generality of the SCC, if a data subject addresses Graylog with claims for access, rectification, erasure, restriction, objection or data portability, Graylog shall refer the data subject to Customer.

7. CUSTOMER'S OBLIGATIONS

7.1 Customer shall provide all Instructions pursuant to these Terms of Data Processing to Graylog in written, electronic or verbal form (the SCC shall remain unaffected). Verbal Instructions shall be confirmed immediately in written form thereafter.

7.2 Customer shall notify Graylog in writing of the names of the persons who are entitled to issue Instructions to Graylog. Any consequential costs incurred resulting from Customer's failure to comply with the preceding sentence shall be borne by Customer. In any event, the managing directors and personnel/human resource management of Customer are entitled to issue Instructions.

7.3 Customer shall inform Graylog immediately if processing by Graylog might lead to a violation of data protection regulations.

7.4 In the case claims based on Art. 82 GDPR are raised against Graylog, Customer shall reasonably support Graylog with its defense to the extent the claim arises in connection with the processing of personal data by Graylog in connection with performing the Services to Customer.

7.5 Customer shall name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing these Terms of Data Processing.

8. SUBPROCESSING

8.1 Any subprocessor is obliged before initiating the processing, to commit itself in writing for the benefit of Customer and its EU Customer Affiliates to comply with the same data protection obligations as the ones under these Terms of Data Processing or legal Act within the meaning of Art. 28 para 3, 4 and 6 GDPR vis-à-vis Customer unless explicitly agreed otherwise. The agreement with the subprocessor must provide at least the level of data protection required by these Terms of Data Processing. Where the subprocessor fails to fulfill its data protection obligations, Graylog shall

remain fully liable to Customer for the performance of the subprocessor's obligations (the SCC shall remain unaffected).

8.2 Any subprocessor must in particular agree to comply with the agreed technical and organizational security measures in accordance with Sec. 6.4 herein and provide Graylog and also Customer, with a list of the implemented technical and organizational measures. Subprocessor's measures may differ from the ones agreed between Customer and Graylog but shall not fall below the level of data security as provided by the measures of Graylog.

8.3 Where a subprocessor refuses to be bound by the same data protection obligations as the ones under these Terms of Data Processing, Customer may consent thereto whereby such consent shall not be unreasonably withheld.

8.4 Graylog may provide a website or provide another notice that lists all subcontractors to access personal data of its Customer as well as the limited or ancillary services they provide. Upon Customer's request, Graylog will provide all information necessary to demonstrate that the subprocessor will meet all requirements pursuant to Sec. 8.1 and 8.2. In the case Customer objects to the subprocessing, Graylog can choose to either not engage the subprocessor or to terminate All Terms or any related service agreement with two (2) months prior written notice. Until the termination of All Terms/services agreement, Graylog may suspend the portion of the Services which is affected by the objection of Customer. Customer shall not be entitled to a pro-rata refund of the remuneration for the Services, unless the objection is based on justified reasons of non-compliance with applicable data protection law.

8.5 Subject to Graylog complying with the obligations of the SCC and Art. 28 para 2 GDPR, Customer herewith agrees (including, on behalf of its EU Customer Affiliates) to the subprocessors list as set out in **Exhibit B**.

9. LIABILITY

9.1 Customer and Graylog shall be each liable for damages of concerned data subjects according to Art. 82 GDPR (external liability). Either Party shall be entitled to claim back from the other, Graylog or Customer, that part of the compensation corresponding to their part of responsibility for the damage.

9.2 As regards the internal liability and without any effect as regards the external liability towards data subjects, the Parties agree that notwithstanding anything contained hereunder, when providing the Services, Graylog's liability for breach of any terms and conditions under these Terms of Data Processing shall be subject to the liability limitations agreed in All Terms. Further, no EU Customer Affiliate shall become beneficiary of these Terms of Data Processing without being bound by these Terms of Data Processing and without accepting this liability limitation. Customer will indemnify Graylog against any losses that exceed the liability limitations in All Terms suffered by Graylog in connection with any claims of EU Customer Affiliates or data subjects who claim rights based on alleged violation of these Terms of Data Processing including the SCC.

10. COSTS FOR ADDITIONAL SERVICES

If Customer's Instructions lead to a change from or increase of the agreed Services or in the case of Graylog's compliance with its obligations pursuant to Sec. **Error! Reference source not found.**, 6.8 or **Error! Reference source not found.** to assist Customer with Customer's own statutory obligations, Graylog is entitled to charge reasonable fees for such tasks which are based on the prices agreed for rendering the Services and/or notified to Customer in advance.

11. CONTRACT PERIOD

The duration of these Terms of Data Processing depends on the duration of All Terms. It commences and terminates with the provision of the Services under All Terms, unless otherwise stipulated in the provisions of this Data Processing Agreement.

12. MODIFICATIONS

Graylog may modify or supplement these Terms of Data Processing in its discretion in respond to changes in the Applicable Law, and may also modify or supplement these Terms of Data Processing by providing any required notice to Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the GDPR. Customer shall notify Graylog if it does not agree to a modification, in which case Graylog may terminate these Terms of Data Processing and All Terms with two (2) weeks' prior written notice, whereby in the case of an objection not based on non-compliance of the modifications with the Applicable Law, Graylog shall remain entitled to claim its agreed remuneration until the term end.

13. WRITTEN FORM

Any verbal agreements to these Terms of Data Processing as well as changes and amendments of these Terms of Data Processing or the Services hereunder, including this Sec. 13, shall not be effective unless in writing and authorized by the parties.

14. CHOICE OF LAW

These Terms of Data Processing is governed by, and shall be interpreted in accordance with, the relevant Applicable Laws.

15. MISCELLANEOUS

15.1 With respect to any issues arising out of or in connection with data protection, these Terms of Data Processing shall prevail over all other agreements between the Parties.

15.2 In the event a clause under All Terms has been found to violate the GDPR or any other Applicable Law, the Parties will mutually agree on modifications to All Terms to the extent necessary to ensure data privacy-law compliant processing.

Signatures:

_____	_____
Customer	Graylog

Exhibit A – Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Annex to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Annex. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a)An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Annex and signing Annex I.A.

(b)Once it has completed the Annex and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c)The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a)The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b)The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Annex as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Annex to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). 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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without

undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a)The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b)The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c)The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d)The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e)The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a)SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b)Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([8]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the

sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c)Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i)lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d)The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a)Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c)Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d)The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e)Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f)The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a)Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b)The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a)The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b)The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a)The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i)receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii)becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b)If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d)The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a)The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory

authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c)The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i)the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii)the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the

transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

([1]) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

([2]) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

([3]) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

([4]) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

([5]) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

([6]) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

([7]) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

([8]) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

([9]) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

([10]) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

([11]) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

([12]) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

ANNEX I

TO THE STANDARD CONTRACTUAL CLAUSES

This Annex forms part of the Clauses

Data Exporter

Customer as specified in the Terms of Data Processing is the Data Exporter.

Data Importer

Graylog as specified in the Terms of Data Processing is the Data Importer.

Data subjects

Employees, contractors, agents, etc. of Customer or EU Customer Affiliate and the employees of Customer's or EU Customer Affiliate's contractors, agents, etc. as well as the Customer's or EU Customer Affiliate's customers' employees, and the employees of their contractors, agents, etc.

Categories of data

Names, usernames, user IDs, business/personal addresses, phone numbers, departments, email addresses, and IP addresses, computer or device names.

When rendering support or maintenance services and performing cloud-based solutions performance and usage analytics, the following types of personal data and categories of data subjects may be affected:

Any kind of personal data which is stored on Customer's premises and which relates to any kind of data subjects and/or usage analytics collected by Graylog or its sub-processors for the purpose of product improvement and enhancement.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

None.

Processing operations

The data listed above is processed solely to provide support or maintenance services and to provide usage analytics for product improvement and enhancement, each as more fully described in All Terms. Specifically, the processing will be limited to incidental access to such certain limited Customer Personal Data stored on Data Exporter's servers when rendering maintenance services for on premise solutions and usage analytics for analysis for cloud-based solutions in connection with performance analysis and product improvement and enhancement, each as allowed in All Terms.

ANNEX II

TO THE STANDARD CONTRACTUAL CLAUSES

This Annex forms part of the Clauses

Description of the Technical and Organizational Security Measures implemented by the Data Importer of the SCC:

Sub-Processors will be bound to adhere to similar but not identical organizational security measures which shall not fall below the level of data security as agreed herein. Any organizational security measures are subject to change of technical standards and can be adopted. If so requested, Data Importer will provide Data Exporter with a description of the then current measures.

Graylog Security Addendum

This Graylog Security Addendum (CSA) sets forth the administrative, technical, and physical safeguards Graylog takes to protect Customer Content at Graylog. Graylog may update this CSA from time to time to reflect changes in Graylog's security posture, provided such changes do not materially diminish the level of security herein provided.

This CSA is made a part of Customer Terms of Service with Graylog. In the event of any conflict between the terms of the Agreement and this CSA, this CSA will control.

1. Purpose

    1.1. This CSA describes the minimum information security standards that Graylog maintains to protect Customer Content. Requirements in this CSA are in addition to any requirements in the Agreement.

    1.2. The CSA is reasonably designed to protect the confidentiality, integrity, and availability of Customer Content against anticipated or actual threats or hazards; unauthorized or unlawful access, use, disclosure, alteration, or destruction; and accidental loss, destruction, or damage in accordance with laws applicable to the provision of the Service.

2. Graylog Security Program

    2.1. Scope and Content. Graylog Security Program: (a) complies with industry recognized information security standards; (b) includes administrative, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Customer Content; and (c) is appropriate to the nature, size, and complexity of Graylog's business operations.

    2.2. Security Policies, Standards and Procedures. Graylog maintains security policies, standards, and procedures (collectively, Security Policies) designed to safeguard the processing of Customer Content by employees and contractors in accordance with this CSA.

2.3. Security Program Office. Graylog's Chief Technology Officer leads Graylog's Security Program and develops, reviews, and approves Graylog's Security Policies.

2.4. Security Program Updates. Graylog reviews, updates, and approves Security Policies once annually to maintain their continuing relevance and accuracy. Employees receive information and education about Graylog's Security Policies during onboarding and annually thereafter.

2.5. Security Training and Awareness. New employees are required to complete security training as part of the new hire process and receive annual and targeted training (as needed and appropriate to their role) thereafter to help maintain compliance with Graylog's Security Policies, as well as other corporate policies, such as the Graylog Code of Conduct. This includes requiring Graylog employees to annually re-acknowledge the Code of Conduct and other Graylog policies as appropriate. Graylog conducts periodic security awareness campaigns to educate personnel about their responsibilities and provide guidance to create and maintain a secure workplace.

3. Risk Management

3.1. Graylog has a security risk assessment program and management process to identify potential threats to the organization.

3.2. Graylog management rates and reviews identified, material risks to determine if existing controls, policies, and procedures are adequate. Risk mitigation plans are implemented as needed to address material gaps considering the nature of Graylog's business and the information it stores.

4. Change Management

4.1. Graylog deploys changes to the Services during maintenance windows, details of which are posted to the Graylog website or communicated to customers as set forth in the Specific Hosted Services Terms.

4.2. Graylog follows documented change management policies and procedures for requesting, testing, and approving application, infrastructure, and product related changes.

4.3. Changes undergo appropriate levels of review and testing, including security and code reviews, regression testing and user acceptance prior to approval for implementation.

4.4. Software development and testing environments are maintained and logically separated from the production environment.

5. Incident Response and Breach Notification

5.1. Graylog has an incident response plan and team to assess, respond, contain, and remediate (as appropriate) identified security issues, regardless of their nature (e.g., physical, cyber, product). Graylog reviews and updates the plan once annually to reflect emerging risks and "lessons learned."

5.2. Graylog notifies Customers without undue delay after becoming aware of a Data Breach. As used herein, Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Content under the applicable Agreement, including Personal Data as defined under the General Data Protection Regulation (EU) 2016/679 (GDPR), while being transmitted, stored, or otherwise processed by Graylog.

5.3. In the event of a Data Breach involving Personal Data under the GDPR, if customer reasonably determines notification is required by law, Graylog will provide reasonable assistance to the extent required for the Customer to comply with applicable data breach notification laws, including assistance in notifying the relevant supervisory authority and providing a description of the Data Breach.

6. Governance and Audit

6.1. Graylog conducts internal control assessments on an ongoing basis to validate that controls are designed and operating effectively. Issues identified from assessments are documented, tracked, and remediated as appropriate.

6.2. Third party assessments are performed to validate ongoing governance of control operations and effectiveness. Issues identified are documented, tracked, and remediated as appropriate.

7. Access and User Management

7.1. Graylog implements reasonable controls to manage user authentication for employees or contractors with access to Customer Content, including without limitation, assigning each employee or contractor with unique and/or time limited user authorization credentials for access to any system on which Customer Content is accessed and prohibiting employees or contractors from sharing their user authorization credentials.

7.2. Graylog allocates system privileges and permissions to users or groups on a “least privilege” principle and reviews user access lists and permissions on a quarterly basis, at minimum.

7.3. New users must be pre-approved before Graylog grants access to Graylog corporate networks and systems. Pre-approval is also required before changing existing user access rights.

7.4. Graylog promptly disables application, platform, and network access for terminated users upon notification of termination.

8. Password Management and Authentication Controls

8.1. Authorized users must identify and authenticate to the network, applications and platforms using their user ID and password. Graylog’s enterprise password management system requires minimum password parameters.

8.2. SSH key authentication and enterprise password management applications are utilized to manage access to the production environment.

8.3. Two-factor authentication (2FA) is required for remote access and privileged account access for Customer Content production systems.

9. Encryption and Key Management

9.1. Graylog uses industry-standard encryption techniques to encrypt Customer Content in transit. The Graylog System is configured by default to encrypt user data files using transport layer security (TLS) encryption for web communication sessions.

9.2. Graylog relies on policy controls to help ensure sensitive information is not transmitted over the Internet or other public communications unless it is encrypted in transit.

9.3. Graylog uses encryption key management processes to help ensure the secure generation, storage, distribution, and destruction of encryption keys.

10. Threat and Vulnerability Management

10.1. Graylog continuously monitors for vulnerabilities that are acknowledged by vendors, reported by researchers, or discovered internally through vulnerability scans, Red Team activities or personnel identification.

10.2. Graylog documents vulnerabilities and ranks them based on severity level as determined by the likelihood and impact ratings assigned by TVM. Graylog assigns appropriate team(s) to conduct remediation and track progress to resolution as needed.

10.3. For systems containing Customer Content, an external vendor conducts security penetration tests on the corporate environments at least annually to detect network and application security vulnerabilities. Critical findings from these tests are evaluated, documented and assigned to the appropriate teams for remediation.

11. Logging and Monitoring

11.1. Graylog continuously monitors application, infrastructure, network, data storage space and system performance.

11.2. Graylog reviews key reports daily and follows up on events as necessary.

12. Secure Development

12.1. Graylog's Software Development Life Cycle (SDLC) methodology governs the acquisition, development, implementation, configuration, maintenance, modification, and management of software components.

12.2. For major product releases, Graylog uses a risk-based approach when applying its standard SDLC methodology, which may include such things as performing security architecture reviews, open source security scans, dynamic application security testing, network vulnerability scans and external penetration testing in the development environment. Graylog performs security code review for critical features if needed; and performs code review for all features in the development environment. Graylog scans packaged software to ensure it is free from trojans, viruses, malware, and other malicious threats.

12.3. Graylog utilizes a code versioning control system to maintain the integrity and security of application source code. Access privileges to the source code repository are reviewed periodically and limited to authorized employees.

12.4. The SDLC methodology does not apply to free Graylog Content or to Third Party Content, including any made available on Graylog Marketplace.

13. Network Security

13.1. Graylog uses industry standard technologies to prevent unauthorized access or compromise of Graylog's network, servers, or applications, which include such things as logical and physical controls to segment data, systems, and networks according to risk. Graylog monitors demarcation points used to restrict access such as firewalls and security group enforcement points.

13.2. Remote users must authenticate with two-factor authentication prior to accessing Graylog networks containing Customer Content.

14. Vendor Security

14.1. Graylog assesses risks associated with new vendors prior to onboarding and thereafter manages them through its risk management program.

14.2. Confidential Information is shared only with those who are subject to appropriate confidentiality terms with Graylog.

14.3. Graylog uses a risk-based approach to verify on-going vendor compliance with Graylog's Security Policies.

15. Physical Security

15.1. Graylog grants physical access to Graylog based on role. Graylog removes physical access when access is no longer required, including upon termination.

15.2. Personnel must carry, and visitors must wear, identity badges when in Graylog facilities. Visitors must always be accompanied. Graylog logs visitor access to Graylog facilities.

16. Disaster Recovery Plan

16.1. Graylog has a Business Continuity / Disaster Recovery Plan to manage significant disruptions to Graylog operations and infrastructure. Graylog management updates and approves the Plan annually.

16.2. Graylog personnel perform annual disaster recovery tests. Test results are documented and corrective actions are noted.

16.3. Data backup, replication and recovery systems/technologies are deployed to support resilience and protection of Customer Content.

16.4. Backup systems are configured to encrypt backup media.

17. Asset Management and Disposal

17.1. Graylog maintains and regularly updates an inventory of infrastructure assets.

17.2. Documented, standard build procedures are utilized for installation and maintenance of production servers.

17.3. Documented data disposal policies are in place to guide personnel on the procedure for disposal of Customer Content.

17.4. Upon expiration or termination of the Agreement, Graylog will return or delete Customer Content in accordance with the terms of the Agreement. If deletion is required, Customer Content will be securely deleted, except that Customer Content stored electronically in Graylog's backup or email systems may be deleted over time in accordance with Graylog's records management practices.

18. Human Resources Security

18.1. Graylog personnel sign confidentiality agreements and acknowledge Graylog's Acceptable Use Policy during the new employee onboarding process.

18.2. Graylog conducts background verification checks for potential Graylog personnel with access to Customer Content in accordance with relevant laws and regulations. The background checks are commensurate to an individual's job duties.

19. CSA Proof of Compliance

19.1. Security Audits. At least once a year, Graylog undergoes a security audit by an independent third party that attests to the effectiveness of the controls Graylog has in place to safeguard the systems and operations where Customer Content is processed, stored, or transmitted (e.g., System and Organizational Control (SOC 2), Type 2) audit in accordance with the Attestation Standards under Section 101 of the codification standards (AT 101). Upon request, Graylog will supply Customer with a summary copy of Graylog's annual audit reports, which will be deemed Confidential Information under the Agreement.

ANNEX III

TO THE STANDARD CONTRACTUAL CLAUSES

Exhibit B

List of Sub-Processors

Name of the Subprocessor	Purpose of the Processing	Contact Details
AWS	Cloud Provider	https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
Okta	Single Sign On / Identity Management	https://www.okta.com/trustandcompliance/
Hubspot	CRM & Customer Service Software	https://legal.hubspot.com/dpa
PostHog	Activity Analytics for Performance Analysis and Product Improvement	https://posthog.com/privacy
Quickbooks	Customer Billing	https://quickbooks.intuit.com/uk/data-processing-agreement/