FORCEPOINT DATA PROCESSING AGREEMENT

FOR THE PROVISION OF FORCEPOINT PRODUCTS

1. Background

This Data Processing Agreement is subject to and is incorporated by reference into the Forcepoint Subscription Agreement. Use of the Products by a Subscriber shall be deemed to be acceptance of the Forcepoint Subscription Agreement and, by incorporation, this Data Processing Agreement. In the event of any conflict between the terms of the Forcepoint Subscription Agreement and the terms of this Data Processing Agreement, the relevant terms of this Data Processing Agreement shall prevail. In the event of any conflict between the terms of this Data Processing Agreement and its Exhibits, the relevant terms of this Data Processing Agreement shall prevail. This Data Processing Agreement shall be effective for the Subscription Term of any Order placed under the Forcepoint Subscription Agreement.

2. Definitions

"**Data Controller**", "**Data Processor**", "**Process/Processing**" and "**Personal Data**" have the meanings given to them in EU Data Protection Law;

"Data Processing Agreement" means this agreement between Subscriber and Forcepoint concerning the Processing of Personal Data as part of provision by Forcepoint of the Products to Subscriber;

"**EU Data Protection Law**" means the General Data Protection Regulation ("GDPR") (EU 2016/679) on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data, and any subsequent amending or replacing European legislation governing the Processing of Personal Data by Forcepoint during the Subscription Term

"**Forcepoint Affiliates**" means an entity controlling, controlled by, or under common control with Forcepoint, that may assist in the provision of the Product(s);

"**Forcepoint Subscription Agreement**" means the terms and conditions governing the provision of the Products to Subscribers located at www.forcepoint.com/product-subscription-agreement.

"Standard Contractual Clauses" means the agreement executed by and between Subscriber and Forcepoint LLC and attached hereto as Exhibit 2 pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses (Controller to Processor) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection and any amendments thereto which are necessary to comply with EU Data Protection Law.

"Sub-processor" means any Data Processor engaged by Forcepoint or a Forcepoint Affiliate.

"**Subscriber Data**" means Personal Data as defined under GDPR, which shall include (i) "End User Personal Information" as defined in the Forcepoint Privacy Policy available at https://www.forcepoint.com/company/privacy-policy; and

(ii) Personal Data given or made accessible to Forcepoint by the Subscriber by virtue of Subscriber's subscription to or use of the Product(s);

All other capitalized terms have the respective meanings assigned to such terms in the Forcepoint Subscription Agreement.

3. Processing of Data

3.1 To the extent that Forcepoint Processes or has access to Subscriber Data in the course of providing Product(s) to Subscriber, it will: (i) Process such Subscriber Data solely as a Data Processor on behalf of Subscriber, who will at all times be deemed to be the Data Controller for the purpose of the applicable data protection laws; (ii) Process the Subscriber Data in accordance with the terms of the Forcepoint Subscription Agreement together with any reasonable and relevant lawful instructions received in writing from authorised personnel of Subscriber from time to time which may be specific instructions or instructions of a general nature as set out in the Forcepoint Subscription Agreement or as otherwise agreed between Subscriber and Forcepoint during the term of the Forcepoint Subscription Agreement; and (iii) promptly notify the Subscriber about: (a) any legally binding request for disclosure of the Subscriber Data by a law enforcement authority (where Subscriber is identified by name by the law enforcement authority and/or the response provided by Forcepoint will result in identifying the Subscriber by name to the law enforcement authority) unless otherwise prohibited from doing so by law; (b) any request received for the Subscriber Data directly from the individual to whom the Subscriber Data relates (without responding to that request unless it has been otherwise authorised to do so); and

(c) a complaint, communication or request relating to Subscriber's obligations under applicable data protection laws (including requests from a data protection authority with competent jurisdiction).

3.2 Subscriber is responsible for compliance with its obligations as Data Controller under applicable data protection laws, in particular for justification of and liability for any transmission of Subscriber Data to Forcepoint (including providing any required notices and obtaining any required consents), and for its decisions concerning the Processing and use of Subscriber Data.

3.3 Forcepoint will only process Subscriber Data in compliance with all applicable laws including the EU or Member State law to which Forcepoint is subject, including the EU General Data Protection Regulation (GDPR).

4. Security of Data

4.1 Forcepoint agrees that it shall implement appropriate technical and organisational security measures to seek to prevent unauthorised or unlawful processing of, or accidental loss, destruction or damage to Subscriber Data, taking into account the guidelines promulgated in Article 32 of the GDPR. The technical and organisational security measures are more particularly described in Exhibit 1 (which may be amended by Forcepoint from time to time).

4.2 Forcepoint shall also: (i) ensure that only its employees, agents or sub-processors who may be required by Forcepoint to assist it in performing any obligations imposed by the Forcepoint Subscription Agreement will have access to the Subscriber Data; (ii) ensure the reliability of any employees who have access to the Subscriber Data; (iii) ensure that all employees involved in the processing of the Subscriber Data have undergone adequate training in the care, protection and handling of Personal Data; and (iv) notify Subscriber of any actual or reasonably suspected unauthorised or unlawful processing or any accidental loss, destruction, damage, alteration or disclosure of the Subscriber Data (to the extent reasonably believed by Forcepoint to have targeted Subscriber Data) without undue delay once it becomes aware of such an event and keep Subscriber informed of any related developments.

4.3 Forcepoint shall take reasonable steps to ensure that Forcepoint employees, contractors or sub-processors who access Subscriber Data are obligated to maintain the confidentiality and integrity of Subscriber Data.

5. Audit

5.1 Forcepoint shall audit the security of its data processing facilities used to Process the Subscriber Data. This audit will be performed annually in accordance with ISO 27001 standards (including for purposes in addition to complying with Section 4).

5.2 Upon Subscriber's request, Forcepoint will provide Subscriber with a report of the relevant audit (such report being Forcepoint's confidential information) so that Subscriber can reasonably verify Forcepoint's compliance with its obligation to seek to take appropriate security measures in accordance with Section 4 and Exhibit 1 of this Data Processing Agreement.

5.3 In addition, upon request in writing by Subscriber and at Subscriber's sole expense, Forcepoint and Subscriber will appoint a mutually agreed upon auditor who is internationally approved by the ISO 27001 certification auditing body so that Subscriber can reasonably verify Forcepoint's compliance with its obligation to seek to take appropriate security measures in accordance with Section 4 and Exhibit 1 of this Data Processing Agreement.

5.4 Any such audit will take place during regular business hours and no more frequently than once in any consecutive twelve-month period, and on a mutually agreed upon date, time, location and duration. Subscriber agrees that (i) such audits shall not adversely affect other Subscribers of Forcepoint or Forcepoint's provision of Products; (ii) any such third party auditor shall comply with Forcepoint's policies during such audit; and (iii) Subscriber shall ensure that any such third party auditor treat all of Forcepoint's Confidential Information disclosed to such third party auditor as a result of such audit in the same manner Subscriber is required to treat such Confidential Information.

5.5 Any audit provided for in this section shall only consist of an audit of the architecture, systems and procedures relevant to the protection of Personal Data at locations where Personal Data is stored and/or the review by such auditor of Forcepoint's regularly-prepared records regarding its obligation to seek to take appropriate security measures in accordance with Exhibit 1 of this Data Processing Agreement.

6. Sub-Processing

6.1 By accepting the Forcepoint Customer Agreement, using the Products, or placing its Order(s), Customer provides Forcepoint a general authorisation to engage third party sub-processors as Forcepoint determines necessary to assist in the provision of Products. Forcepoint will ensure such Sub-processors are required to comply with data protection obligations, which are no less onerous than the data protection obligations of Forcepoint contained within this Data Processing Agreement.

6.2 Customer may review a current list of sub-processors engaged by Forcepoint to process Customer Data at (https://www.forcepoint.com/sites/default/files/resources/files/datasheet-forcepoint-sub-processors-list-en.pdf).

6.3 If Customer has a reasonable basis to object to Forcepoint's use of a Sub-processor, Customer may terminate the Forcepoint Customer Agreement and this Data Processing Agreement by providing written notice to Forcepoint.

6.4 For the avoidance of doubt, no refund will be due from Forcepoint in the event of termination by Customer pursuant to Section 6.3

7. Consequences of termination of the Forcepoint Subscription Agreement

On termination of the Forcepoint Subscription Agreement, Forcepoint shall: (i) cease all Processing of Subscriber Data on behalf of Subscriber and upon request by Subscriber either (i) return to Subscriber (in a format accessible by Subscriber) all such Subscriber Data; or (ii) destroy or otherwise render inaccessible all Subscriber Data (as far as technically possible and except as may be required by law).

8. Disputes and liability

For the avoidance of doubt, the relevant provisions of the Forcepoint Subscription Agreement shall apply in relation to the applicable governing law, jurisdiction and liability of the parties in relation to any disputes or claims arising in connection with the subject matter of this Data Processing Agreement.

9. International Transfers

9.1 With respect to Subscriber Data that originates from Subscribers established in the European Union and is Processed by Forcepoint outside of the European Union, Forcepoint shall ensure that it has taken appropriate steps to ensure Subscriber Data is Processed in accordance with applicable data protection laws. Subscriber shall execute such further documents and do any and all such further things as may be necessary to ensure that any international transfers and subsequent Processing of Personal Data by Forcepoint, Forcepoint Affiliates or their Sub-processors is in compliance with applicable data protection laws.

9.2 With respect to Subscriber Data that originates from Subscribers established in the European Union and is Processed by Forcepoint LLC in the United States of America, Section 10 below will apply.

10. Application of Standard Contractual Clauses

10.1 The Standard Contractual Clauses will apply only to Subscriber Data that (i) is transferred from the European Economic Area and/or Switzerland to a processor established in a third country that has not been determined to offer personal data protection laws commensurate with EU Data Protection Laws, either directly or via onward transfer, and (ii) is Processed by Forcepoint LLC.

10.2 For the purpose of the Standard Contractual Clauses and this Section 10, the Data Exporter shall be (i) Subscriber and (ii) all Subscriber Affiliates (as defined in the Forcepoint Subscription Agreement) established within the European Economic Area and Switzerland using the Products in accordance with the Forcepoint Subscription Agreement, and the Data Importer shall be Forcepoint LLC.

10.3 Subject to Section 6 of this Data Processing Agreement and pursuant to Clause 5(h) of the Standard Contractual Clauses, Subscriber acknowledges and expressly agrees that (a) Forcepoint LLC's Affiliates may be retained as Sub-processors; and (b) Forcepoint LLC and Forcepoint LLC's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Products.

10.4 Subject to Section 6 of this Data Processing Agreement, Forcepoint LLC shall make information available to Subscriber regarding sub-processors currently engaged by Forcepoint LLC to Process Personal Data in connection with the provision of the Products.

10.5 Subject to Section 6, if Subscriber has a reasonable basis to object to Forcepoint LLC's use of a new Sub-processor, Subscriber may terminate the Subscription Agreement and this Data Processing Agreement by providing written notice to Forcepoint.

10.6 The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the specifications set out in Section 5 of this Data Processing Agreement.

EXHIBIT I

FORCEPOINT ORGANISATIONAL SECURITY MEASURES

The following contains the description of all of the technical and organizational security measures Forcepoint implements in accordance with Clause 5 of the Data Processing Agreement aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of Processing:

Access Control of Processing Areas
Forcepoint implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the Personal Data are Processed or used. This is accomplished by:

- establishing security areas;
- protection and restriction of access paths;
- securing the decentralized telephones, data processing equipment and personal computers;
- establishing access authorizations for employees and third parties, including the respective documentation;
- regulations on access card-keys;
- restriction on access card-keys;
- all access to the data center where personal data are hosted is logged, monitored, and tracked; and
- the data center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems
Forcepoint implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:

- identification of the terminal and/or the terminal user to the Forcepoint systems;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- User IDs are monitored and access revoked when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of identification codes and secure tokens;
- strong password requirements (minimum length, use of special characters, re-use etc.);
- protection against external access by means of a state-of-the-art industrial standard firewall whose connection to the intranet [if applicable] shall in addition be safeguarded by a VPN connection;
- dedication of individual terminals and/or terminal users, identification characteristics exclusive to specific functions; and
- all access to data content on machines or computer systems is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems
Forcepoint commits that the persons entitled to use its data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by:

- employee policies and training in respect of each employee's access rights to the Personal Data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the Personal Data;
- effective and measured disciplinary action against individuals who access Personal Data without authorization;
- release of data to only authorized persons;
- control of files, controlled and documented destruction of data; and
- policies controlling the retention of back-up copies.

Transmission Control
Forcepoint implements suitable measures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that

it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged. This is accomplished by:

- use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- use of 128bit SSL-encryption for all http-connections;
- implementation of secure two-factor VPN connections to safeguard the connection to the internet, if applicable;
- encryption of Personal Data by state-of-the-art encryption technology;
- constant monitoring of infrastructure (i.e. ICMP-Ping at network level, disk space examination at system level, successful delivery of specified test pages at application level); and
- monitoring of the completeness and correctness of the transfer of data (end-to-end integrity check).

Input Control

Forcepoint implements suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed. This is accomplished by:

- an authorization policy for the input of data into hosted service, as well as for the reading, alteration and deletion of stored data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of user codes (passwords and tokens);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user ID's that have not been used for a substantial period of time;
- logging or otherwise evidencing input authorization; and
- electronic recording of entries.

Instructional Control

Forcepoint ensures that Personal Data may only be Processed in accordance with the Forcepoint Subscription Agreement together with any reasonable and relevant instructions received in writing from authorised personnel of the Subscriber from time to time which may be specific instructions or instructions of a general nature as set out in the Forcepoint Subscription Agreement or as otherwise agreed between the Subscriber and Forcepoint during the term of the Forcepoint Subscription Agreement. This is accomplished by binding policies and procedures for Forcepoint's employees.

Availability Control

Forcepoint implements suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy: reporting data is stored on hardware with redundant disks subsystem backed up in real time with off-site replication backups.

Separation of Processing for different Purposes

Forcepoint implements suitable measures to ensure that data collected for different purposes can be processed separately. This is accomplished by:

- access to data is separated through multiple diverse applications for the appropriate users; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is Processed separately.

Subprocessors

Forcepoint engages various sub processors in connection with its cloud infrastructure. Forcepoint ensures that it has robust contractual provisions in place to ensure compliance by such sub processors with the organizational security measures outlined herein.

EXHIBIT 2

STANDARD CONTRACTUAL CLAUSES[1]

TO APPLY TO THE TRANSFERS OF SUBSCRIBER DATA BY SUBSCRIBERS OR THEIR AFFILIATES LOCATED WITHIN THE EEA OR SWITZERLAND ("EXPORTERS") TO FORCEPOINT LLC OR TO ANY SUB-PROCESSORS APPOINTED BY FORCEPOINT ("IMPORTERS") WHERE SUCH IMPORTERS ARE PROCESSING THE DATA OUTSIDE OF THE EEA OR SWITZERLAND.

THIS EXHIBIT 2 IS TO BE READ IN CONJUNCTION WITH THE DATA PROCESSING AGREEMENT BETWEEN FORCEPOINT AND THE SUBSCRIBER TO WHICH IT IS APPENDED.

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

.....

Address:

.....

Tel.:_____; fax:_____; e-mail: _____

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Name of the data importing organisation: Forcepoint LLC .....

Address: 10900-A Stonelake Blvd., 3rd Floor, Austin, TX 78759, USA.....

Tel.:1-800-723-1166; fax: 1-858-458-2950; e-mail:privacy@forcepoint.com

Other information needed to identify the organisation:

1 The Standard Contractual Clauses issued in accordance with Article 26(2) of Directive 95/46/EC remain in effect pending updating by the EU to comport with the requirements of GDPR.

……

(the data **importer**)

each a “party”; together “the parties”,

have agreed on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1 – Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 – Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 – Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 – Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be

transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 – Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 – Liability

5. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

7. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7 – Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the

data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 – Cooperation with supervisory authorities

3. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

4. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

5. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 – Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 – Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause. Subject to the preceding sentences, these Clauses should be read in conjunction with any data processing agreement and/or subscription agreement between the data exporter(s) or its affiliates and Forcepoint or Forcepoint's affiliates.

Clause 11 – Subprocessing

6. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

7. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the

data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

8. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

9. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 – Obligation after the termination of personal data processing services

10. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

11. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and (ii) all Affiliates (as defined in the Forcepoint Subscription Agreement) of Subscriber established within the European Economic Area and Switzerland using the Products in accordance with the Forcepoint Subscription Agreement.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Forcepoint LLC is a provider of on-premise and cloud products which processes Personal Data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The individuals from whom the Data Exporter collects Personal Data through its use of the Forcepoint Products.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Through their use of Forcepoint Products, Data Exporter may submit personal data to Forcepoint, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include but is not limited to the categories of Personal Data listed below:

- ***Forcepoint Subscriber ID information*:** Customer ID (i.e. the ID used to identify which customer send files to ThreatScope), User ID or Visitor ID (the ID used to identify client IP visiting the file), network user name, first name, last name, company name, country, and email address.
- ***Communication information*:** email metadata, including email addresses of sender and recipient, sender email in SMTP transaction and email subject.
- ***Traffic data*:** proxy log, web traffic logs, apache browsing logs, browsing and diagnostic logs, IP addresses, URL information, website session data and files submitted by Forcepoint Subscribers.

Special categories of data (if appropriate)

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

NA

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Subscriber Product Data are transferred for the purposes of the management and administration of customer/client services, including but not limited to:

- administration of orders and accounts;
- providing Forcepoint Products and associated technical support;
- Forcepoint Product management and development;
- the conduct of Forcepoint's business activities.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see Exhibit 1 to the Data Processing Agreement between the Data Exporter or its affiliate and Forcepoint International Technology Limited.