FORCEPOINT DATA PROCESSING AND PROTECTION MEASURES

APPLICABLE TO FORCEPOINT PRODUCTS & SERVICES

1. Background

These Data Processing and Protection Measures (these "Measures") are subject to and incorporated by reference into the applicable Forcepoint Customer Agreement. Use of the Products or Services by Customer is deemed to be acceptance of the Forcepoint Customer Agreement and, by incorporation, these Measures. In the event of any conflict between the terms of the Forcepoint Customer Agreement and the terms of these Measures, the relevant terms of these Measures will prevail, unless otherwise specified below. The Standard Contractual Clauses and UK International Data Transfer Addendum will prevail in the event of any conflict between the terms of these Measures and the Standard Contractual Clauses or UK International Data Transfer Addendum, as applicable.

These Measures incorporate, as Annex II, **"**Forcepoint Technical And Organisational Security Measures**"** regarding Forcepoint's data security management practices.

These Measures will be effective for the Subscription Term or Maintenance Term of any Order placed under the Forcepoint Customer Agreement.

2. Definitions

Capitalized terms not specifically defined in these Measures will have the same meaning as provided for in the Forcepoint Customer Agreement(s) or applicable data protection legislation, such as CCPA, UK GDPR, or Article 4 of GDPR, e.g. for "processing", "controller", "processor", "personal data" and "data subject". All other capitalized terms have the respective meanings assigned to such terms in the Forcepoint Customer Agreement.

"**Affiliates**" means an entity controlling, controlled by, or under common control with Forcepoint, that may assist in the provisioning of the Products or Services.
"CCPA" means the California Consumer Privacy Act of 2018.
"Customer" means the Subscriber and/or Licensee as those terms are defined in the applicable Forcepoint Customer Agreements.
"Customer Data" means any data and/or information submitted by Customer to Forcepoint or accessed by Forcepoint through the provisioning and use of the Products or Services which may include, but is not limited to, (i) "End User Personal Data" 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 Customer by virtue of Customer's subscription or license to or use of the Products or Services.
"Data Processing and Protection Measures" means these commitments concerning Forcepoint's processing of Customer Data applicable to Forcepoint's Products and Services.
"**GDPR**" means the General Data Protection Regulation (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 or Maintenance Term.
"**Forcepoint Customer Agreement(s)**" means the terms and conditions governing the provision of the applicable Products or Services to Customers, which may consist of the following terms and conditions located at www.forcepoint.com/product-subscription-agreement, and/or the terms and conditions governing Products and Services provided to Licensees located at: https://www.forcepoint.com/network-security-products-license-agreement.
"Standard Contractual Clauses" means the applicable Data Protection Module of the Standard Contractual Clauses included in the European Commission's implementing decision 2021/914 of 4 June 2021 on Standard Contractual Clauses as agreed in these Measures.
"Sub-processor" means any Data Processor engaged by Forcepoint or an Affiliate.
"UK International Data Transfer Addendum" means the International Data Transfer Addendum **t**o the Standard Contractual Clauses attached to these Measures as Annex III.
"UK GDPR" means GDPR, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

3. Processing of Data

3.1. Access to and processing of Customer Data by Forcepoint Products and Services is done in accordance with the terms of the Forcepoint Customer Agreement and any reasonable and lawful directions received in writing from authorised personnel of Customers that obtained such Products and Services. For the avoidance of doubt, the placing of an Order by Customer isdeemed to be a general authorization for Forcepoint to process Customer Data in accordance with these Measures.

3.2. To the extent Customer Data includes Personal Data, Customer will at all times be deemed to be the Data Controller and Forcepoint will at all times be deemed to be the Data Processor within the meaning of the applicable data protection laws. Customer 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 Customer Data to Forcepoint (including providing any required notices and obtaining any required consents), and for its

decisions concerning the Processing and use of such Customer Data.

3.3. Forcepoint will promptly notify Customer about: (a) any legally binding request for disclosure of Customer Data by a law enforcement authority (where Customer is identified by name by the law enforcement authority and/or the response provided by Forcepoint will result in identifying Customer by name to the law enforcement authority) unless otherwise prohibited from doing so by law; (b) any request received for Customer Data directly from an individual regarding that individual's Personal Data (without responding to that request unless it has been otherwise authorised to do so); and (c) a complaint, communication or request relating to Customer's obligations under applicable data protection laws (including requests from a data protection authority with competent jurisdiction). Forcepoint will only process Customer Data in compliance with all applicable laws, including the UK, EU, or Member State law to which Forcepoint is subject.

3.4. Forcepoint will verify the legal basis of any government authority data requests and reject those Forcepoint has reason to believe are not valid.

4. Security of Data

4.1. Forcepoint agrees that it will implement appropriate technical and organisational security measures designed to prevent unauthorised or unlawful processing of, or accidental loss, destruction or damage to Customer Data, taking into account thestate of the art, the costs of implementation and the nature, scope, context and purposes of the processing. Technical and organisational security measures employed by Forcepoint include those described in Annex II (which may be amended by Forcepoint from time to time).

4.2. Forcepoint will 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 Customer Agreement will have access to Customer Data; (ii) ensure the reliability of any Forcepoint employees who have access to Customer Data; (iii) ensure that all employees involved in the processing of Customer Data have committed themselves to appropriate obligations of confidentiality and have undergone adequate training in the care, protection and handling of Personal Data; and (iv) notify Customer of any actual or reasonably suspected unauthorized or unlawful processing or any accidental loss, destruction, damage, alteration or disclosure of Customer Data (to the extent reasonably believed by Forcepoint to have targeted Customer Data) without undue delay and, where feasible, not later than 72 hours once it becomes aware of such an event and keep Customer informed of any related developments.

4.3. Forcepoint will take reasonable steps to ensure that Forcepoint contractors and Sub-processors' employees who access Customer Data are obligated to maintain the confidentiality and integrity of Customer Data.

5. Audit

5.1. Forcepoint will audit the security of its data processing facilities used to Process Customer 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 Customer's request, Forcepoint will provide Customer with a copy of the relevant certification(s), such as the Forcepoint Cloud ISO 27001 Certification, (such certification(s) being Forcepoint's confidential information) so that Customer can reasonably verify Forcepoint's compliance with its obligation to seek to take appropriate security measures in accordance with Section 4 and Annex II of these Measures.

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

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. Customer agrees that (i) such audits will not adversely affect Forcepoint's other customers or Forcepoint's provision of Products and Services; (ii) any such third party auditor must comply with Forcepoint's policies during such audit; and (iii) Customer willl 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 Customer is required to treat such Confidential Information.

5.5. Any audit provided for in this section will only consist of an audit of the architecture, systems and procedures relevant to the protection of Customer Data at locations where Customer Data is stored and/or the review by such auditor of Forcepoint's regularly-prepared records regarding its obligation to implement appropriate security measures, which in the case of Personal Data take into account the guidelines promulgated in Article 32 of the GDPR.

5.6. The parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with the specifications set out in this Section.

6. Sub-Processing

6.1. By placing its Order(s), Customer provides Forcepoint a general authorisation to engage third party Sub-processors as Forcepoint determines is necessary to assist with respect to the provisioning and use of Products and Services. 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 these Measures.

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 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 Customer Agreement

On termination of the Forcepoint Customer Agreement, Forcepoint will: (i) cease all Processing of Customer Data on behalf of Customer and upon request by Customer either (i) return to Customer (in a format accessible by Customer) all such Customer Data; or (ii) destroy or otherwise render inaccessible all Customer 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 Customer Agreement specify the applicable law, jurisdiction, and liability of the parties in relation to any disputes or claims arising in connection with the subject matter of these Measures.

9. International Transfers

9.1. With respect to Customer Personal Data that originates from Customers established in the European Union or United Kingdom and Processed by Forcepoint outside of the European Union or United Kingdom (as applicable), Forcepoint will take appropriate steps to ensure such Personal Data is Processed in accordance with applicable data protection laws. Customer will 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, Affiliates or Sub-processors is in compliance with applicable data protection laws.

9.2. Forcepoint and Sub-processors will comply with: (i) the Standard Contractual Clauses when transferring Customer Personal Data that is subject to GDPR to a third country that has not received an adequacy decision from the EU in accordance with GDPR; or (ii) the UK International Data Transfer Addendum when conducting a Restricted Transfer of Customer Personal Data that is subject to the UK GDPR to a third country that has not received an adequacy decision from the UK in accordance with the UK GDPR.

9.3. For the purpose of the Standard Contractual Clauses:

9.3.1. Module Two or Module Three will apply (as applicable);

9.3.2. In Clause 7, the optional docking clause will apply;

9.3.3. In Clause 9, Option 2 will apply, and the notice requirements for Subprocessor changes will be fulfilled by updating the list provided in Section 6.2 of these Measures;

9.3.4. In Clause 11, the optional language will not apply;

9.3.5. In Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law;

9.3.6. In Clause 18(b), disputes will be resolved before the courts of Ireland;

9.3.7. Annex I of the Standard Contractual Clauses is deemed completed with the information set out in Annex 1 to these Measures, as applicable; and

9.3.8. Annex II of the Standard Contractual Clauses is deemed completed with the information set out in Annex II to these Measures.

9.4. Subject to Section 6 of these Measures and pursuant to Clause 9 of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Forcepoint and its Affiliates may be retained as Sub-processors and may engage third-party Sub-processors in connection with the provision or use of the Products or Services.

10. Assistance

To the extent technically feasible and consistent with its responsibilities related to the sale of its Products and Services to Customer, Forcepoint will assist Customer through appropriate technical and organisational measures to comply with Customer's Data Controller responsibilities as set forth in Chapter III of GDPR Reg EU 2016/679.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: Customer as defined in the Measures, and Customer's affiliates established within the European Economic Area and Switzerland using the Products or Services (or the United Kingdom for purposes of the UK International Data Transfer Addendum) in accordance with the Forcepoint Customer Agreement

Address: . . As provided in the relevant Forcepoint Customer Agreement.

Activities relevant to the data transferred under these Clauses:

Customer Personal Data is 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 Services and associated technical support;
- Forcepoint Product and Services management and development;
- the conduct of Forcepoint's business activities.

Signature and date: .....

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Forcepoint (as defined in the relevant Forcepoint Customer Agreement).

Address: As provided in the relevant Forcepoint Customer Agreement

Contact person's name, position and contact details:

Forcepoint
Attention: Data Protection Officer
10900-A Stonelake Blvd., Quarry Oaks 1, Suite 350
Austin, TX 78759, USA

Email: Privacy@forcepoint.com

Activities relevant to the data transferred under these Clauses:

Customer Personal Data is 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 Services and associated technical support;
- Forcepoint Product and Services management and development;
- the conduct of Forcepoint's business activities

Signature and date: .....

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

Through their use of Forcepoint Products and Services, 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 Customer 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 Customers.*Categories of personal data transferred*

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

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. Forcepoint does not expect to receive sensitive data from the Data Exporter.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Customer Personal Data may be transferred for the purposes of the management and administration of customer/client services on a continuous basis.

Nature of the processing

Customer Data is 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 Services and associated technical support;
- Forcepoint Product and Services management and development;
- the conduct of Forcepoint's business activities.

Purpose(s) of the data transfer and further processing

Customer 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 Services and associated technical support;
- Forcepoint Product and Services management and development;
- the conduct of Forcepoint's business activities.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Forcepoint will only keep the Data Exporter's Personal Data it collects, as long as necessary, for the purpose or purposes (i) for which it was collected; (ii) of performing or fulfilling contractual obligations; (iii) of complying with law; and/or (iv) of responding to legal actions.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
A list of Forcepoint's current Sub-processors, along with a description of their services, can be found at: https://www.forcepoint.com/sites/default/files/resources/files/datasheet-forcepoint-sub-processors-list-en.pdf. Forcepoint's sub-processor's will only keep the Data Exporter's Personal Data it collects, as long as necessary, for the purpose or purposes (i) for which it was collected; (ii) of performing or fulfilling contractual obligations; (iii) of complying with law; and/or (iv) of responding to legal actions.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

ANNEX II

FORCEPOINT TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Forcepoint implements various technical and organizational measures designed to ensure a level of security appropriate to the risks posed to Customer Data. Such measures seek to prevent unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of access to Customer Data.Consistent with industry standard and guidelines set forth in applicable data protection laws, such measures include:

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 Customer Data is accessed, 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] will also 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 Customer Data cannot be read, copied or modified, or removed without authorization. This will 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 Customer 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 Customer 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 Customer 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 accomplishedby:

- 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 oftime;
- logging or otherwise evidencing input authorization; and
- electronic recording of entries.

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

Availability Control
Forcepoint implements suitable measures to ensure that Customer 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.

Sub-processors

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

ANNEX III
UK INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This UK International Data Transfer Addendum to the EU Commision Standard Contractual Clauses (the "UK International Data Transfer Addendum") has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The Effective Date as stated in the applicable Forcepoint Customer Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Customer (as defined in the Measures) Main address (if a company registered address): As provided in the applicable Forcepoint Customer Agreement Official registration number (if any) (company number or similar identifier):	Full legal name: Forcepoint (as defined in the applicable Forcepoint Customer Agreement) Main address (if a company registered address): As provided in the applicable Forcepoint Customer Agreement Official registration number (if any) (company number or similar identifier):
Key Contact	Job Title: As provided on the relevant Order Contact details including email: As provided on the relevant Order	Job Title: Data Protection Officer Contact details including email: privacy@forcepoint.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: As of the Effective Date of the applicable Forcepoint Customer Agreement Reference (if any): The Standard Contractual Clauses as referenced and agreed to in the Measures to which this UK International Data Transfer Addendum is attached as Annex III.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Annexes of the Standard Contractual Clauses (other than the Parties), and which for this Addendum is set out in:

Annex IA: List of Parties: As included in Annex I.A. to the Measures.
Annex IB: Description of Transfer: As included in Annex I.B. to the Measures.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As included in Annex II to the Measures
Annex III: List of Sub processors (Modules 2 and 3 only): As described in the Measures.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this UK International Data Transfer Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Mandatory Clauses of this UK International Data Transfer Addendum, being the template Addendum B.1.0 issued by the U.K. Information Comissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.