inforcer

GLOBAL CLIENT DATA PROCESSING ADDENDUM

(INFORCER)

This Data Processing Addendum ("**DPA**") applies to the Processing of Client Personal Data (as defined below) by the **Supplier** in connection with the provision of the Services to the Client (each, as defined in the Agreement).

1. DEFINITIONS

1.1 Unless otherwise set out below, each capitalized term in this DPA shall have the meaning set out in the Agreement, and the following capitalized terms used in this DPA shall be defined as follows:

"**Adequate Jurisdiction**" means the UK, EEA or a country or territory deemed to provide adequate protection for the rights and freedoms of individuals, as set out in: (a) the Data Protection Act 2018 or regulations made by the UK Secretary of State under the Data Protection Act 2018; (b) with respect to Data Subjects in the EEA, a decision of the European Commission; and (c) with respect to Data Subjects in Switzerland, Annex 1 to the Ordinance.

"**Administration Data**" means:

(a) contact details relating to, and the content of correspondence with the Client's main account holder or administrator; and

(b) support enquiries submitted by the Client's authorized users in relation to the Services.

"**Agreement**" means the agreement entered into between the Client and the Supplier in respect of the provision of the Services, or such other terms as have been agreed between the Parties;

"**Approved Addendum**" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Approved Addendum;

"**Authorized Sub-processors**" means the Sub-processors listed in ANNEX 2, and any other Sub-processors appointed in accordance with paragraph 6;

"**Client**" means the entity identified in the Order Form;

"**Client Personal Data**" means the Personal Data described in ANNEX 1;

"**Controller Purposes**" means: (a) undertaking internal research and development to develop, test, improve and alter the functionality of the Supplier's products and services; (b) creating and using anonymized or aggregated datasets for evaluation, testing, benchmarking and improvement of the Supplier's products and services, provided that the Supplier shall not use Client Personal Data to train or fine-tune artificial intelligence or machine-learning models; and (c) administering the Supplier's relationship with the Client under the Agreement, including understanding the Client's use of the Services and supporting the Supplier's relationship with the Client;

"**Data Protection Laws**" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Client Personal Data in force from time to time as they may be amended or otherwise updated from time to time, including (without limitation): (a) the GDPR; (b) all federal and state laws relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States (the "**US Data Protection Laws**"); and (c) the Swiss Federal Act on Data Protection of 25 September 2020 ("**FADP**") and the Swiss Data Protection Ordinance of 31 August 2022 (the "**Ordinance**"), and any new or revised version of these laws that may enter into force from time to time (the "**Swiss Data Protection Laws**");

"**Data Subject**" means an individual to whom Personal Data relates;

"**Deidentified Data**" means data created using Client Personal Data that cannot reasonably be linked to such Client Personal Data, directly or indirectly;

"**DPA**" has the meaning given to it in the Background;

"**EEA**" means the European Economic Area;

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as defined in section 3 of the Data Protection Act 2018.

"**Member State**" means a member state of the EEA, being a member state of the European Union, Iceland, Norway, or Liechtenstein;

"**Objection**" has the meaning given in paragraph 6.5;

"**Parties**" means the Supplier and Client;

"**Personal Data**" means any data or information that (a) is linked or reasonably linkable to an identified or identifiable natural person or (b) is otherwise "personal data," "personal information," "personally identifiable information," or similarly defined data or information under Data Protection Laws;

"**Processing**" means any operation or set of operations (including storage) that is performed on Personal Data or on sets of Personal Data, whether or not by automated means. "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly;

"**Services**" means the applicable User Subscriptions and Support Services (if applicable) provided by the Supplier to the Client under the Agreement, as further set out in the Order Form and the Agreement;

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Client Personal Data Processed by the Supplier as a processor or service provider;

"**Standard Contractual Clauses**" or "**SCCs**" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 and available at https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en;

"**Sub-processor**" means a processor or service provider instructed to Process Personal Data on behalf of another processor or service provider;

"**Usage Data**" means:

(a) diagnostic, usage and performance information collected by the Supplier in relation to the Client's and its authorized users' use of the Services; and

(b) where the Services include the Security Services, threat risk detection heuristics and outcomes generated through analysis of Client Personal Data as part of the Services.

For the avoidance of doubt, where security telemetry, detection signals, threat data or performance metrics generated by the Supplier constitute Personal Data, such data shall be treated as Usage Data for the purposes of this DPA.

1.2 The terms "**business**", "**controller**", "**processor**", "**service provider**" and "**supervisory authority**" shall have the meanings given to them in the Data Protection Laws.

2. INTERACTION WITH THE AGREEMENT

2.1 This DPA is incorporated into and forms an integral part of the Agreement. This DPA supplements and (in case of contradictions) supersedes the Agreement with respect to any Processing of Client Personal Data, except to the extent an Order Form expressly provides greater protection for Client Personal Data, in which case the Order Form shall prevail.

2.2 The Parties certify that they understand the requirements in this DPA and will comply with them.

3. ROLE OF THE PARTIES

3.1 The Parties acknowledge and agree that:

(a) save as set out at paragraph 3.1(b), the Supplier Processes Client Personal Data as a processor or service provider in the performance of its obligations under the Agreement

and this DPA and Client acts as a controller or business; and

(b) for the purposes of the GDPR and Swiss Data Protection Laws the Supplier Processes Usage Data and Administration Data as a controller for the Controller Purposes.

4. INSTRUCTIONS FOR DATA PROCESSING

4.1 The details of the Processing of Client Personal Data under the Agreement and this DPA (including subject matter, duration, nature and purpose of the Processing, categories of Client Personal Data and Data Subjects) are described in the Agreement and in ANNEX 1.

4.2 The Supplier will only Process Client Personal Data under the documented instructions provided by the Client and in accordance with Data Protection Laws, other than in respect of its Processing of Usage Data and Administration Data for the Controller Purposes.

4.3 The Agreement and this DPA shall constitute the instructions to the Supplier for the Processing of Client Personal Data by the Supplier. The Client may issue further written instructions in accordance with this DPA.

4.4 Without limiting the foregoing, the Supplier is prohibited from:

(a) selling Client Personal Data or otherwise making Client Personal Data available to any third party for monetary or other valuable consideration;

(b) sharing Client Personal Data with any third party for cross-context behavioral advertising;

(c) retaining, using, or disclosing Client Personal Data for any purpose other than for the business purposes specified in the Agreement or as otherwise permitted by Data Protection Laws;

(d) retaining, using, or disclosing Client Personal Data outside of the direct business relationship between the Parties, unless permitted by Data Protection Laws; and

(e) except as otherwise permitted by Data Protection Laws, combining Client Personal Data with Personal Data that the Supplier receives from or on behalf of another person or persons, or collects from the Supplier's own interaction with the applicable Data Subject.

4.5 The Supplier will:

(a) limit access to Client Personal Data to its personnel who have a business need to have access to such Client Personal Data and shall ensure that such personnel are subject to confidentiality obligations with respect to Client Personal Data;

(b) comply with its obligations under and provide the same level of privacy protection as is required by Data Protection Laws; and

(c) inform Client if it decides it can no longer meet its obligations under Data Protection Laws.

5. COMPLIANCE AND NOTICE

5.1 The Client shall comply with its obligations under Data Protection Laws and shall ensure that:

(a) any instructions to the Supplier in relation to the Processing of Client Personal Data comply with Data Protection Laws;

(b) it has provided all applicable notices to Data Subjects required under the Data Protection Laws in relation to the Processing of Client Personal Data in accordance with the Agreement and this DPA; and

(c) to the extent required, it has obtained consent from Data Subjects in each case as required for the lawful Processing of Client Personal Data required under the Data Protection Laws in accordance with the Agreement and this DPA.

6. SUB-PROCESSORS

6.1 The Supplier may Process Client Personal Data anywhere that the Supplier or its Sub-processors maintain facilities, subject to the remainder of this paragraph 6.

6.2 Client generally authorizes the Supplier to engage any of the Sub-processors listed in ANNEX 2, as amended in accordance with paragraph 6.4.

6.3 The Supplier shall enter into a written agreement with each Authorized Sub-processor imposing data protection obligations that, in substance, are no less protective of Client Personal Data than the Supplier's obligations under this DPA and shall remain liable to the Client for any failure of an Authorized Sub-processor to fulfil its obligations under that agreement or Data Protection Laws.

6.4 The Supplier shall provide the Client with ten (10) days' notice of any proposed changes to the Authorized Sub-processors it uses to Process Client Personal Data (including any addition or replacement of any Authorized Sub-processors), including any information reasonably necessary to enable the Client to assess the Authorized Sub-processor and exercise its right to object.

6.5 If the Client objects to the Supplier's use of a new Authorized Sub-processor it shall provide the Supplier with written notice of the objection within fifteen (15) days after the Supplier has provided notice to the Client as described in paragraph 6.4 (an "**Objection**").

6.6 In the event of an Objection, the Supplier will use reasonable endeavors to make available to the Client a change in the Services, or will recommend a commercially reasonable change to the Services to prevent the applicable Authorized Sub-processor from Processing the Client Personal Data.

6.7 If the Supplier is unable to make available such a change in accordance with paragraph 6.6 within a reasonable period of time, which shall not exceed thirty (30) days, the Supplier may terminate

the Agreement by providing not less than thirty (30) days' written notice to Client. During such notice period, the Supplier may suspend the affected portion of the Services.

7. DEIDENTIFIED DATA

7.1 If the Supplier receives Deidentified Data from or on behalf of Client, or creates Deidentified Data, the Supplier shall:

(a) take reasonable measures to ensure the information cannot be associated with a Data Subject;

(b) publicly commit to Process the Deidentified Data solely in deidentified form and not to attempt to reidentify the information; and

(c) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and Data Protection Laws.

8. DATA SUBJECT RIGHTS REQUESTS

8.1 The Supplier will notify Client without undue delay of any request received by the Supplier or any Authorized Sub-processor from a Data Subject to assert their rights under Data Protection Laws in relation to Client Personal Data Processed by the Supplier, other than in respect of the Supplier's Processing of Usage Data and Administration Data for the Controller Purposes (a "**Data Subject Request**") and:

(a) as between the Supplier and Client, Client will have sole discretion in responding to the Data Subject Request;

(b) the Supplier shall not respond to the Data Subject Request without Client's prior consent, save that the Supplier may advise the Data Subject that their request has been forwarded to Client; and

(c) the Supplier will provide Client with reasonable assistance as necessary for Client to fulfil its obligation under Data Protection Laws to respond to Data Subject Requests in respect of Client Personal Data.

8.2 Client shall promptly inform the Supplier of any request received by the Client from a Data Subject to assert their rights under the GDPR and Swiss Data Protection Laws in relation to Usage Data or Administration Data Processed by the Supplier for the Controller Purposes.

9. SECURITY AND AUDITS

9.1 The Supplier will implement and maintain appropriate technical and organizational data protection and security measures designed to ensure security of Client Personal Data, taking into account the risks that are presented by the Processing, including those measures set out in ANNEX 3.

9.2 Client may take reasonable and appropriate steps to:

(a) ensure that the Supplier uses Client Personal Data in a manner consistent with Client's obligations under Data Protection Laws; and

(b) upon reasonable notice, stop and remediate unauthorized use of Client Personal Data.

9.3 Client may audit the Supplier's compliance with this DPA in respect of its Processing of Client Personal Data. The Parties agree that all such audits will be conducted:

(a) not more than annually, unless more frequent audits are required by a supervisory or other regulatory authority with jurisdiction over the Processing of Client Personal Data or otherwise under Data Protection Laws;

(b) upon reasonable written notice to the Supplier;

(c) only during the Supplier's normal business hours; and

(d) in a manner that does not materially disrupt the Supplier's business or operations.

9.4 With respect to any audits conducted in accordance with paragraph 9.3:

(a) Client may engage a third-party auditor to conduct the audit on its behalf, save that the Supplier may reasonably object to the engagement of a third-party auditor if such third-party auditor is a competitor of the Supplier; and

(b) the Supplier shall not be required to facilitate any such audit unless and until the Parties have agreed in writing the scope and timing of such audit.

9.5 Client shall promptly notify the Supplier of any non-compliance discovered during an audit.

9.6 The results of the audit shall be the Supplier's confidential information.

9.7 The Supplier shall provide to Client upon request, or may provide to Client in response to any audit request submitted by Client to the Supplier, either of the following:

(a) data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, or by a publicly certified auditing Supplier; or

(b) such other documentation reasonably evidencing the implementation of the technical and organizational data security measures in accordance with industry standards.

9.8 If an audit requested by Client is addressed in the documents or certification provided by the Supplier in accordance with paragraph 9.7, and:

(a) the certification or documentation is dated within twelve (12) months of Client's audit request; and

(b) the Supplier confirms that there are no known material changes in the controls audited,

Client agrees to accept that certification or documentation in lieu of conducting a physical audit of the controls covered by the relevant certification or documentation.

10. SECURITY INCIDENT

10.1 The Supplier will notify Client in writing without undue delay after becoming aware of any Security Incident, and reasonably cooperate in any obligation of Client under Data Protection Laws to make any notifications, such as to individuals or supervisory or other regulatory authorities.

10.2 The Supplier will take reasonable steps to contain, investigate, and mitigate any Security Incident, and will send Client timely information about the Security Incident, including, but not limited to, the nature of the Security Incident, the measures taken to mitigate or contain the Security Incident and the status of the investigation.

10.3 The Supplier's notification of or response to a Security Incident under this paragraph 10 will not be construed as an acknowledgement by the Supplier of any fault or liability with respect to the Security Incident.

11. INTERNATIONAL TRANSFERS

11.1 Where the Services are provided by Inforcer Ltd (as identified in the Order Form):

(a) the Supplier shall not transfer any Client Personal Data to a recipient outside of the UK unless:

(i) the recipient is in an Adequate Jurisdiction; or

(ii) the transfer is governed by an agreement incorporating standard data protection clauses approved under Section 119A of the Data Protection Act 2018; and

(b) if the Client is not in an Adequate Jurisdiction, the Approved Addendum shall, as further set out in ANNEX 4, apply to and form part of this DPA in relation to the transfer of any Client Personal Data from the Supplier (as data exporter) to the Client (as data importer).

11.2 The Standard Contractual Clauses shall, as further set out in ANNEX 4, apply to and form part of this DPA in respect of any transfer of Client Personal Data from the Client (as data exporter) to the Supplier (as data importer) to the extent that the Services are provided by Inforcer, Inc (as identified in the Order Form) and one of the following applies:

(a) the GDPR applies to the Client's Processing of Client Personal Data when it makes the transfer;

(b) Applicable Data Protection Laws that apply to the Client when making that transfer (the "**Exporter Data Protection Laws**") otherwise prohibit such transfer in the absence of a transfer mechanism implementing adequate safeguards in respect of the Processing of

that Client Personal Data, and entering into the Standard Contractual Clauses would reasonably satisfy any requirement under Exporter Data Protection Laws to implement such safeguards; or

(c) the transfer is an "onward transfer" as defined in the SCCs.

11.3 The parties agree that execution of the Agreement shall, where applicable, have the same effect as signing the Standard Contractual Clauses and Approved Addendum.

11.4 For the avoidance of doubt, any governing law, jurisdiction or supervisory authority specified in ANNEX 4 applies solely to the Standard Contractual Clauses, the Approved Addendum and the international transfer mechanisms incorporated into ANNEX 4. It does not amend or replace the governing law, jurisdiction or dispute-resolution provisions applicable to the Agreement, as set out in the terms and conditions incorporated there in, or, where applicable, the US Addendum.

12. COSTS

12.1 The Client shall pay to the Supplier on demand all costs and expenses incurred by the Supplier in connection with:

(a) implementing any changes to the Services under paragraph 6.6;

(b) facilitating and contributing to any audits of the Supplier under paragraph 9;

(c) facilitating and contributing to any audits of the Supplier conducted by a supervisory authority;

(d) responding to queries or requests for information from the Client relating to the Processing of Client Personal Data;

(e) any assistance provided by the Supplier to the Client with its fulfilment of its obligations to respond to Data Subjects' requests for the exercise of their rights under Data Protection Laws; and

(f) any assistance provided by the Supplier to the Client with any data protection impact assessments or prior consultation with any supervisory authority of the Client.

13. DURATION AND TERMINATION

13.1 This DPA shall commence on the Effective Date and, notwithstanding any termination of the Agreement, will remain in effect until, and automatically expire upon, the later of (a) the Supplier's deletion of all Client Personal Data as described in this DPA; and (b) termination of the Supplier's Processing of Usage Data and Administration Data for the Controller Purposes.

13.2 The Supplier shall:

(a) if requested to do so by the Client within sixty (60) days of the date of termination or expiry of the Agreement (the "**Retention Period**"), return by secure file transfer a copy of the Client Personal Data then held in the Services and reasonably available for export, in a commonly used format reasonably determined by the Supplier; and

(b) upon expiry of the Retention Period, delete Client Personal Data from its active production systems, except to the extent that this DPA expressly permits or requires continued retention of specific categories of Personal Data, including threat-related data retained pursuant to the Security Services retention provisions. Client Personal Data contained within point-in-time recovery, disaster recovery, long-term retention or other immutable backup systems may remain retained until expiry of the applicable backup retention cycle. Such backup copies shall be maintained solely for disaster recovery, security, legal compliance and business continuity purposes and shall be automatically overwritten or deleted in accordance with Supplier's backup retention policies.

ANNEX 1

DETAILS OF PROCESSING

Part 1A – List of Parties

	Supplier	**Client**
Role	Data Exporter Controller in respect of Usage Data and Administration Data Processed for the Controller Purposes Processor / service provider in respect of Client Personal Data	Data Importer Controller / business
Contact person	Taylor Mullings – Chief Legal Officer taylor.mullings@inforcer.com	*As set out in the Order Form*
Activities relevant to the transfer	The performance of the Services under the Agreement.	The receipt of the Services under the Agreement.

Part 1B - List of Parties

	Supplier	**Client**
Role	Data Importer Controller in respect of Usage Data and Administration Data Processed for the Controller Purposes Processor / service provider in respect of Client Personal Data	Data Exporter Controller / business
Contact person	Taylor Mullings – Chief Legal Officer taylor.mullings@inforcer.com	*As set out in the Order Form*
Activities relevant to the transfer	The performance of the Services under the Agreement.	The receipt of the Services under the Agreement.

Part 2 - Description of Processing

Categories of Data Subjects	Client's authorized users, and any other Data Subjects whose data the Client or its authorized users submits, transfers, loads or otherwise provides to the Supplier via the Services, including the Client's customers and employees.
Categories of Personal Data	• Name, email address, work site address, phone number, job role and title, and home address; • User ID; • Service usage information; • Feedback and support requests submitted by authorized users of the Services; and • Any Personal Data the Client or its authorized users submits, transfers, loads or otherwise provides to the Supplier via the Services, including contact information, job role, requests, comments and opinions of authorized users or Data Subjects. Where the Services include the Security Services, the following categories of Personal Data will also be processed: • unified audit log entries; • Entra ID sign in and audit logs; • Defender and Purview logs; • mailbox and message-trace metadata; • conditional access and identity protection state;
	• role and group assignments; • device compliance state; • secure score signals; and • other security telemetry derived from Microsoft Graph.
Special categories of Personal Data	None
Frequency of Transfer	Continuous
Nature of the Processing	• Collection, storage, and retrieval of data submitted by the Client in connection with their use of the Services; and • Monitoring and improvement of the Services.
Purpose(s) of the data transfer and further Processing	Provision of the Services to the Client in accordance with the Agreement Administration and management of the relationship with the Client under the Agreement Undertaking internal research and development to develop, test, improve and alter the functionality of the Supplier's products and services Creating and using anonymized or aggregated datasets for evaluation, testing, benchmarking and improvement of the Supplier's products and services

Duration	Personal Data is retained for the period necessary to provide the Services and in accordance with the retention periods described in the Agreement and this DPA. In the case of Security Services: • Operational security data, including security logs, event data and other telemetry collected through the Security Services, is retained on a rolling basis and is generally deleted sixty (60) days after collection. • Behavioural analysis, learned security context, behavioural baselines, risk profiles and similar outputs derived from operational security data are retained only while the underlying operational security data remains available and therefore generally follow the same rolling sixty (60) day retention period. • Where a threat has been identified, raised or investigated through the Security Services, the associated threat-related data, including threat records, interpreted indicators and Personal Data reasonably necessary to investigate, understand, report on, respond to and maintain a historical record of the threat, may be retained for up to five (5) years, notwithstanding the shorter retention periods applicable to operational security data. For the avoidance of doubt, the retention of threat-related data under this clause may continue after termination or expiry of the Agreement for the periods specified above.
Sub-Processor (if applicable)	Transfers to Sub-processors are carried out as set out in ANNEX 2.

Part 3 – Competent Supervisory Authority

The Parties agree that the Competent Supervisory Authority shall be the supervisory authority determined in accordance with Clause 13 of the SCCs.

ANNEX 2
SUB-PROCESSORS

Sub-processor	Purpose	Data description	Data Location
Microsoft	Microsoft provides the Microsoft 365 productivity and collaboration suite, including email, file storage, authentication, and communication tools.	All personal data may be processed for identity management, collaboration, communication, security monitoring, and general business operations.	Global: Data centres located in ANZ | EU | UK | US
Intercom	Intercom provides live chat and in-app messaging to support Client onboarding and support interactions.	Personal data is processed only as necessary to deliver support, respond to queries, and maintain a record of communication.	US
ApplicatieLink B.V.	PSA ticket creation middleware solution software	It processes any PII included in a ticket created by an alert within the Software, which may include name, job title, User ID, email address, phone number, address.	EU
Inforcer Inc.; Inforcer Pty Ltd	Provision of intragroup support services. Performance of threat monitoring, investigation, triage and incident response.	Personal data contained in support tickets or as otherwise provided by the Client in connection with requesting support (which may include name, job title, User ID, email address, phone number, address). Entra ID sign in and audit logs, Defender and Purview logs, mailbox and message-trace metadata, conditional access and identity protection state, role and group assignments, device compliance state, secure score signals, other security telemetry derived from Microsoft Graph, security incident / ticket information.	US, Australia
Anthropic PBC	Analysis of and generation of insights and reports in respect of security threats and business and operational matters	Entra ID sign in and audit logs, Defender and Purview logs, mailbox and message-trace metadata, conditional access and identity protection state, role and group assignments, device compliance state, secure score signals, other security telemetry derived from Microsoft Graph, security incident / ticket information, and business and operational data contained in reports, documents or other materials submitted for analysis.	US

ANNEX 3

TECHNICAL AND ORGANIZATIONAL MEASURES

Part 1

Security

The Supplier has developed a suite of policies setting out the technical and organizational measures it has implemented to prevent the unauthorized use, access, destruction, disclosure or amendment of Personal Data.

These policies include:

1. Governance and Policies

1.1 The Supplier assigns personnel with responsibility for the determination, review and implementation of security policies and measures.

1.2 The Supplier:

(a) has documented the security measures it has implemented in a security policy and/or other relevant guidelines and documents; and

(b) reviews its security measures and policies on a regular basis to ensure they continue to be appropriate for the data being protected.

1.3 The Supplier establishes and follows secure configurations for systems and software and ensures that security measures are considered during project initiation and the development of new IT systems.

2. Breach response

The Supplier has an incident response plan that has been developed to address data breach events. The plan is tested and updated at least annually.

3. Intrusion, anti-virus and anti-malware defenses

3.1 The Supplier's IT systems used to Process Personal Data have or will have appropriate data security software installed on them, including as follows:

(a) Inbound and outbound traffic passes through firewalls that are monitored and protected by intrusion detection / prevention systems that allow traffic flowing through the firewalls to be logged.

(b) IT systems have antivirus, anti-spyware and anti-malware software installed. Such software is updated regularly and performs ongoing scans for threats and malicious programs.

(c) The Supplier performs regular, and at least monthly vulnerability scans.

(d) The Supplier collects, maintains, reviews and audits event logs.

(e) The Supplier monitors all traffic leaving the organization and unauthorized use of encryption.

4. Access controls

4.1 The Supplier limits access to Personal Data by implementing appropriate access controls, including:

(a) limiting administrative access privileges and use of administrative accounts;

(b) changing all default passwords before deploying operating systems, assets or applications;

(c) requiring authentication and authorization to gain access to IT systems (i.e. require users to enter a user ID and password before they are permitted access to IT systems);

(d) only permitting user access to Personal Data which the user needs to access for his/her job role or the purpose for which they are given access to the Supplier's IT systems (i.e. the Supplier implements measures to ensure least privileged access to IT systems);

(e) having appropriate procedures for controlling the allocation and revocation of Personal Data access rights. For example, having in place appropriate procedures for revoking employee access to IT systems when they leave their job or change role;

(f) enforcing password policies that require users to use strong passwords, in accordance with SOC II Type II, including a combination of upper and lower case letters, numbers (non sequential) and special characters;

(g) use of multi-factor authentication;

(h) automatic timeout and locking of user terminals if left idle;

(i) access to IT systems is blocked after multiple failed attempts to authenticate;

(j) monitoring and logging access to IT systems; and

(k) monitoring and logging amendments to data or files on IT systems.

5. Availability and Back-up Personal Data

5.1 The Supplier has a documented disaster recovery plan that ensures that key systems and data can be restored in a timely manner in the event of a physical or technical incident. The plan is tested and updated at least annually.

5.2 The Supplier regularly backs up information on IT systems and keeps back-ups in separate locations. Back-ups are tested at least annually.

6. Segmentation of Personal Data

6.1 The Supplier:

(a) separates and limits access between network components and, where appropriate, implements measures to provide for separate Processing (storage, amendment, deletion, transmission) of Personal Data collected and used for different purposes; and

(b) does not use live data for testing its systems.

7. Disposal of IT equipment

7.1 The Supplier has in place Processes to securely remove all Personal Data before disposing of IT systems.

7.2 The Supplier uses appropriate technology to purge equipment of data and/or destroy hard disks.

8. Encryption

8.1 The Supplier uses encryption technology to protect Personal Data at rest and in transit, including:

(a) applying AES-256 encryption to data at rest and TLS 1.2 or higher to data in transit; and

(b) encryption of portable devices used to Process Personal Data.

8.2 Encryption keys are stored separately from the encrypted information and are subject to appropriate security measures.

9. Transmission or transport of Personal Data

9.1 Appropriate controls are implemented by the Supplier to secure Personal Data during transmission or transit, including:

(a) encryption in transit using TLS 1.2 or higher;

(b) logging Personal Data when transmitted electronically;

(c) logging Personal Data when transported physically; and

(d) ensuring physical security for Personal Data when transported on portable electronic devices or in paper form.

10. Device hardening

10.1 The Supplier ensures that default passwords that are provided by hardware and software producers are not used.

11. Asset and Software management

11.1 The Supplier maintains an inventory of IT assets and the data stored on them, together with a list of owners of the relevant IT assets.

11.2 The Supplier:

(a) documents and implements rules for acceptable use of IT assets;

(b) requires network level authentication and uses client certificates to validate and authenticate systems;

(c) deploys automated patch management tools and software update tools for operating systems and software;

(d) proactively monitors software vulnerabilities and promptly implements any out of cycle patches; and

(e) permits the use of only the latest versions of fully supported web browsers and email clients.

11.3 The Supplier stores all API keys securely, including as follows:

(a) the Supplier does not store API keys on client side;

(b) the Supplier does not publish API key credentials in online code repositories (whether private or not); and

(c) the Supplier uses API key management tools to retrieve and manage credentials.

12. Physical security

12.1 The Supplier implements physical security measures to safeguard Personal Data. This may include:

(a) Deployment of appropriate building security, including visitor logs, ID card access for staff, logs of staff access to buildings, and CCTV.

(b) Deployment and enforcement of appropriate policies to ensure that Personal Data is printed only where this is necessary for a person to perform his/her job role.

(c) Sensitive Personal Data or large amounts of Personal Data held in hardcopy are kept securely, e.g. in locked rooms or filing cabinets. Generally, steps are taken to ensure that access to hardcopy Personal Data is limited in the same way it would be on an electronic IT system i.e. access is limited to those individuals where it is necessary for them to have access in order for them to perform their job role.

(d) Hardcopy documents containing Personal Data are only taken off site where necessary for a person's job role.

(e) When travelling or working away from the office, hard copy documents and portable devices containing Personal Data are kept secure e.g. never left in a car or unsecured in a public place.

(f) Paper records which contain confidential information (including Personal Data and sensitive Personal Data) are shredded after use.

13. Staff training and awareness

13.1 The Supplier's agreements with staff and contractors and employee handbooks set out its personnel's responsibilities in relation to information security.

13.2 The Supplier carries out:

(a) regular (and at least annual) staff training on data security and privacy issues relevant to their job role and ensures that new starters receive appropriate training before they start their role (as part of the onboarding procedures); and

(b) appropriate screening and background checks on staff.

13.3 The Supplier communicates and enforces information security responsibilities/access that apply before, during, and after termination or any change in employment status. This includes disabling accounts immediately when an employee is terminated or leaves.

13.4 Staff are subject to disciplinary measures for breaches of the Supplier's policies and procedures relating to data privacy and security.

14. Selection of service providers and commission of services

14.1 The Supplier assesses service providers' ability to meet their security requirements before engaging them.

14.2 The Supplier has, or will have, written contracts in place with service providers which require them

to implement appropriate security measures to protect the Personal Data they have access to and limit the use of Personal Data in accordance with the Supplier's instructions.

14.3 The Supplier conducts annual audits of vendors (including sub-processors) that have access to data either through physical inspection or by reviewing vendors' security accreditation (such as ISO 27001 or SOC II) reports.

14.4 The Supplier's incident response protocol and agreements with material vendors provide for the audit of vendors (and sub-processors) following receipt of any notice of a security incident from that vendor.

15. Assistance with Data Subject Rights Requests

15.1 The Supplier has implemented appropriate policies and measures to identify and address Data Subject rights requests including:

(a) the data Processed on behalf of the Client is stored separately from data Processed by the Supplier on behalf of others or for its own purposes;

(b) the Supplier maintains accurate records to enable it to identify quickly all Personal Data Processed on behalf of the Client; and

(c) back-ups of Personal Data Processed by the Supplier on behalf of the Client are retained and overwritten in accordance with the Supplier's applicable back-up, disaster recovery and business continuity processes. Following termination or expiry of the applicable Agreement, Client Personal Data shall be deleted from the Supplier's active production systems in accordance with the Supplier's retention procedures. Personal Data may continue to be retained in secure back-up and disaster recovery systems for the duration of the applicable recovery cycle. Such back-up copies shall be logically isolated, protected by appropriate technical and organisational security measures, used only where reasonably necessary for disaster recovery, business continuity, security, legal or regulatory purposes, and automatically deleted or overwritten when the applicable backup retention or recovery cycle expires. Where Personal Data is restored from a back-up, any deletion, rectification or restriction requests previously applied to that Personal Data shall be re-applied without undue delay.

ANNEX 4
INTERNATIONAL TRANSFERS

PART 1
Supplier as Data Exporter and Client as Data Importer

The Approved Addendum shall be completed as follows:

Table 1: Parties	As set out in Part 1A of ANNEX 1
Table 2: Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum: • Module 4 in operation; • Clause 7 option is not used • Clause 11 option is not used • personal data received from the data importer is combined with personal data collected by the data exporter
Table 3: Appendix Information	As set out in ANNEX 1
Table 4: ending the Addendum	Either Party

PART 2
Client as Data Exporter and Supplier as Data Importer

1. EU SCCS

1.1 The Standard Contractual Clauses shall be completed as follows:

Modules and options

Module	**Clause 7 option**	**Clause 9 option and time period**	**Clause 11(a) option**	**Clause 17 option and governing law**	**Clause 18 jurisdiction**
Module 1	Not used	n/a	Not used	Option 1, Ireland	Ireland
Module 2	Not used	As set out in section 6.4 of the DPA	Not used	Option 1, Ireland	Ireland

Appendix Information

Annex I.A	As set out in Part 1B of ANNEX 1
Annex I.B	As set out in Part 2 of ANNEX 1
Annex I.C	The supervisory authority determined in accordance with Clause 13 of the SCCs.
Annex II	As set out in ANNEX 3

2. UK ADDENDUM

2.1 This paragraph 2 (UK Addendum) shall apply to any transfer of Client Personal Data from the Client to the Supplier, to the extent that (i) the UK Data Protection Laws apply to the Client when making that transfer; or (ii) the transfer is an "onward transfer" as defined in the Approved Addendum.

2.2 As used in this paragraph 2, "**UK Data Protection Laws**" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

2.3 The Approved Addendum will form part of this DPA with respect to any transfers referred to in paragraph 2.1, and execution of this DPA shall have the same effect as signing the Approved Addendum.

2.4 The Approved Addendum shall be deemed completed as follows:

Table 1: Parties	As set out in Part 1B of ANNEX 1
Table 2: Addendum EU SCCs	The Approved EU SCCs as incorporated into this DPA in accordance with paragraph 11 and this ANNEX 4.
Table 3: Appendix Information	As set out in ANNEX 1 and ANNEX 3.
Table 4: ending the Addendum	Either Party

3. TRANSFERS UNDER THE LAWS OF OTHER JURISDICTIONS

3.1 With respect to any transfers of Personal Data referred to in clause 11.2(b) (each a "**Global Transfer**"), the SCCs shall not be interpreted in a way that conflicts with rights and obligations provided for in the Exporter Data Protection Laws.

3.2 For the purposes of any Global Transfers, the SCCs shall be deemed to be amended to the extent necessary so that they operate:

(a) for transfers made by the Client to the Supplier, to the extent the Exporter Data Protection Laws apply to the Client's Processing when making that transfer; and

(b) to provide appropriate safeguards for the transfers in accordance with the Exporter Data

Protection Laws.

3.3 The amendments referred to in paragraph 3.2 of this ANNEX 4 include (without limitation) the following:

(a) references to the "**GDPR**" and to specific Articles of the GDPR are replaced with the equivalent provisions under the Exporter Data Protection Laws;

(b) references to the "**Union**", "**EU**" and "**EU Member State**" are all replaced with reference to the jurisdiction in which the Exporter Data Protection Laws were issued (the "**Exporter Jurisdiction**");

(c) the "**competent supervisory authority**" shall be the applicable supervisory authority in the Exporter Jurisdiction; and

(d) Clauses 17 and 18 of the SCCs shall refer to the laws and courts of the Exporter Jurisdiction respectively.

3.4 Where, at any time during Supplier's Processing of Client Personal Data under this DPA, a transfer mechanism other than the SCCs is approved under the Exporter Data Protection Laws with respect to transfers of Client Personal Data by the Client to the Supplier, the Parties shall promptly enter into a supplementary agreement that:

(a) incorporates any standard data protection clauses or another transfer mechanism formally adopted by the relevant authority in the Exporter Jurisdiction;

(b) incorporates the details of Processing set out in ANNEX 1; and

(c) shall, with respect to the transfer of Personal Data subject to the Exporter Data Protection Laws, take precedence over this DPA in the event of any conflict.

3.5 Where required under the Exporter Data Protection Laws, the Client shall file a copy of the agreement entered into in accordance with paragraph 3.4 with the relevant national authority.