Fortra Data Processing Agreement ("DPA")

1. Scope of this DPA

1.1. This DPA is incorporated by reference into the Fortra Purchase Order Terms and Conditions or other applicable executed Services Agreement (each referred to as "Services Agreement") for provision of products or services ("Services") by service provider ("Vendor") to client ("Client" or "Fortra"). When providing the Services Vendor may Process Personal Data on behalf of the Client and the Parties agree to comply with the terms of this DPA.

1.2. In the event of any conflict between this DPA and the underlying Services Agreement, this DPA shall prevail. In the event of any conflict between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall prevail.

2. Definitions

In this DPA, the following terms shall have the following meanings:

2.1. "**Adequacy Decision**" means, as applicable, a decision from the European Commission, UK Government and/or Swiss Federal Council that a third country provides an adequate level of data protection.

2.2. "**CCPA**" means the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act effective 1 January 2023, and any subsequent amendments or implementing regulations.

2.3. "Client Data" means any data provided, processed, or stored by Vendor from Client.

2.4. "**Client Personal Data**" means any Personal Data Processed by Vendor on behalf of the Client pursuant to the Services Agreement.

2.5. "**Controller**" means an entity which alone or jointly with others, determines the purposes and means of the Processing of Personal Data, including any equivalent term under Data Protection Law.

2.6. "**Data Protection Law**" means, as applicable, any privacy and data protection laws and regulations including: (i) the GDPR and Member State laws implementing the GDPR; (ii) the UK GDPR and Data Protection Act 2018; (iii) the Swiss Federal Act on Data Protection ("**FADP**"); (iv) and the U.S. Privacy Laws, each as amended, updated or replaced from time to time.

2.7. "**Data Subject**" means an identified or identifiable individual.

2.8. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data.

2.9. **"NIS2"** means European Union's Network and Information Systems Directive, implementing regulations and any successor legislation in the EU, and similar applicable law(s) in other countries.

2.10. "**Personal Data**" means any information relating to a Data Subject, including any equivalent term under Data Protection Law.

2.11. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

2.12. "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether

or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

2.13. "**Processor**" means an entity which Processes Personal Data on behalf of a Controller, including any equivalent term under Data Protection Law.

2.14. "**Standard Contractual Clauses**" means, as applicable, (i) the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR ("**EU SCCs**"); and (ii) the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner's Office under S119A(1) of the Data Protection Act 2018 ("**UK Addendum**").

2.15. "**Sub-processor**" means any third party appointed by Vendor to Process the Client's Personal Data on behalf of the Client.

2.16. "**Supervisory Authority**" has the meaning or equivalent meaning given under Data Protection Law.

2.17. "**UK GDPR**" means the GDPR as incorporated into United Kingdom law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

2.18. "**U.S. Privacy Laws**" means (1) the CCPA and (2) the Colorado Privacy Act, Connecticut Data Privacy Act, the Delaware Personal Data Privacy Act, the Iowa Consumer Data Protection Act, the Montana Consumer Data Privacy Act, the Oregon Consumer Privacy Act, the Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, the Virginia Consumer Data Protection Act, and other similar comprehensive state privacy laws, in each case, that are or may become applicable to Vendor's Processing of Personal Data on behalf of Client.

2.19. Capitalized terms not defined in this DPA shall have the meaning given to those terms in the Services Agreement.

3. Scope of the Processing

3.1. The Parties agree that in relation to the Processing of the Client Personal Data, the Client is the Controller and Vendor is the Processor. If the Client is a Processor of the Client Personal Data Vendor shall be a sub-processor of the Client Personal Data. The terms of this DPA shall govern each scenario. In the event Vendor is deemed a sub-processor, Client shall be designated as the point of contact for the applicable Controller(s) and Vendor's notice to Client shall be deemed to satisfy its notice requirements under the applicable Data Protection Law as notice to the applicable Controller(s). Client shall be responsible for providing notice on behalf of Vendor to the applicable Controller(s). To the extent Vendor has provided notice to the Client, and Client fails to sufficiently provide notice on behalf of Vendor to the applicable Controller(s) and any Supervisory Authority determines that Vendor did not satisfy its notice requirements to the Controller(s), then (x) such nonsatisfaction shall not be deemed a material breach of this DPA or the Services Agreement by Vendor and (y) Client shall defend and indemnify Vendor for any deficiencies related to providing notices under applicable Data Protection Law to Controller(s) by Vendor acting as sub-processor.

3.2. Each Party shall comply with its respective obligations under the Data Protection Law.

3.3. Vendor shall only Process the Client Personal Data on the written instructions of the Client, unless Vendor is legally required to do otherwise. In the latter case, Vendor shall inform the Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

3.4. Vendor shall not: (a) collect, retain, use, or disclose the Client Personal Data for any purpose other than as necessary for the specific purpose of performing the Services on behalf of the Client; (b) collect, retain, use or disclose the Client Personal Data for a commercial purpose other than providing the Services on behalf of the Client; (c) collect, retain, use or disclose the Client Personal Data outside of Vendor's direct business relationship with the Client; (d) combine the Client Personal Data with other Personal Data it receives other than as expressly permitted by Data Protection Law (except to contribute to improve its Services); or (e) sell Client Personal Data (for monetary or other valuable consideration) or share Client Personal Data with third parties for targeted or cross-context behavioral advertising.

3.5. The Processing of the Client Personal Data by Vendor comprises the subject matter, nature, purpose and duration determined in the relevant section of Schedule 1 to this DPA. The Processing relates to the types of Personal Data and categories of Data Subjects identified therein.

3.6. Vendor shall immediately inform the Client if, in its opinion, an instruction infringes the Data Protection Law.

4. Personnel Requirements

4.1. Vendor shall ensure that persons authorized to Process the Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Security of Processing

5.1. Vendor shall implement appropriate technical and organizational measures, taking into account the state of the art, the implementation costs and the nature, scope, circumstances, and purposes of the Processing of the Client Personal Data, as well as the respective likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of data security appropriate to the risk of the Client Personal Data and Client Data.

5.2. Vendor shall comply with the technical and organizational measures as specified in Schedule 2 to this DPA. Vendor may update such measures from time to time provided that any such updates do not diminish the level of security provided for in Schedule 2 of this DPA.

5.3. Vendor shall comply with all applicable technical and organizational measures that are required by NIS2, its implementing regulations and all similar laws worldwide. Vendor shall implement vendor management program measures that provide for appropriate security assessment of its third party vendors, promptly report security events (as defined under local law), pass through of NIS2 requirements to third party vendors applicable subcontractors, as well as any requirements from Services Agreement. Vendor shall report to Client any security events relating to Client Data as soon as aware of an actual or suspected event, but in no event more than 12 hours. Vendor shall fully cooperate with Client in investigation of a security event and provide all the information required by NIS2.

6. Engagement of Sub-processors

6.1. The Client hereby authorizes Vendor to engage Sub-processors in a general manner to Process the Client Personal Data. Upon written request from the Client, Vendor will provide a complete list of Sub-processors it engages.

6.2. Client shall notify of any objection of any sub-processors within 10 days of receiving the list. If the objection has not been resolved to the mutual satisfaction of the Parties within 30 days after receipt of the Client's objection either Party may terminate the Services Agreement (in whole or in part solely to the extent necessary to terminate access to the Services affected by the addition of the proposed Sub-processor), which shall be the Client's sole and exclusive remedy.

6.3. Vendor shall contractually impose obligations to comply with applicable Data Protection Law.

6.4. Vendor shall remain fully liable to the Client for the performance of the obligations of each Sub-processor with regards to the Services.

7. Support Obligations

7.1. Taking into account the nature of the Processing, Vendor shall assist the Client, insofar as this is possible, with technical and organizational measures to fulfil the Client's obligations to respond to requests for exercising Data Subjects' rights relating to the Client Personal Data. Vendor may respond to such requests directly to the Data Subject only upon prior written authorization of the Client. If a Data Subject directly contacts Vendor to exercise their Data Subject rights, Vendor shall forward this request immediately to the Client.

7.2. Vendor shall notify the Client without undue delay of an actual Personal Data Breach involving the Client Personal Data. The notification shall contain a description of the:

a) nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

b) name and contact details of Vendor's contact point where more information can be obtained;

c) likely consequences of the Personal Data Breach; and

d) measures taken or proposed to be taken by Vendor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where it is not possible to provide such information at the same time, Vendor may provide the information in phases without undue further delay.

7.3. To the extent required by Data Protection Law, taking into account the nature of the Processing and the information available to Vendor, Vendor shall reasonably assist the Client in ensuring compliance with the security of Processing, breach notifications, data protection impact assessments and prior consultations with Supervisory Authorities at Client's cost, including providing items such as log data.

8. Deletion and Return of Client Personal Data

8.1. This DPA shall remain in effect for as long as Vendor Processes the Client Personal Data on behalf of the Client. Upon written request Vendor shall no later than 90 days after the date of cessation of any Service involving the Processing of the Client Personal Data, delete or return the Client Personal Data. If Vendor is required by law to maintain the Client Personal Data Vendor shall inform the Client of such requirement.

9. Audit

9.1. At the Client's cost, Vendor shall make available to the Client all information necessary to demonstrate compliance with the obligations laid down in this DPA and, to the extent required by Data Protection Law, allow for and contribute to audits, conducted by the Client or another auditor mandated by the Client. The Client may only exercise its right to audit once per calendar year and will not include access to premises or systems. Vendor and the Client will discuss and agree in writing the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any audit and the Client shall take all necessary steps to minimize the disruption to Vendor's business. The Client or relevant auditor shall not have any right to access any other of Vendor's customers Personal Data or any system not involved in the Processing of the Client's Personal Data. Any information obtained pursuant to an audit shall be deemed to be confidential information of Vendor.

10. International Transfers

10.1. Vendor shall ensure, as applicable, that any transfer of the Client Personal Data, subject to the GDPR, UK GDPR and/or FADP, outside of the EEA, UK and/or Switzerland to a third country without an Adequacy Decision complies with Data Protection Law.

10.2. If the Client transfers Client Personal Data which is subject to the GDPR, UK GDPR and/or FADP outside of the EEA, UK and/or Switzerland, as applicable, to Vendor in a third country without an Adequacy Decision the Parties agree to comply with module 2 and/or 3 of the Standard Contractual Clauses, as applicable, which are incorporated into this DPA by reference, as if they had been set out in full, and are populated in this clause 10. The Parties agree that for the purposes of the Standard Contractual Clauses the Client shall be the data exporter and Vendor shall be the data importer.

10.3. The Parties agree that execution or acceptance of the Services Agreement constitutes execution of the Standard Contractual Clauses to the extent required by Data Protection Law.

10.4. The Parties agree to complete the EU SCCs as follows in relation to the Client Personal Data subject to the GDPR: (i) any optional clauses are excluded; (ii) the Parties details shall be as set out in the Services Agreement and this DPA; (iii) the description of the transfer shall be as set out in the relevant section of Schedule 1 of this DPA; (iv) the competent Supervisory Authority shall be determined in accordance with clause 13 of the EU SCCs; (v) the data importer's technical and organizational security measures shall be in accordance with clause 5 of this DPA; (vi) the data importer has a general written authorization to appoint Sub-processors in accordance with clause 6 of this DPA; (vii) in Clause 17 (Option 1), the EU SCCs will be governed by the law of The Netherlands; and (viii) in Clause 18(b) disputes will be resolved before the courts of The Netherlands.

10.5. The Parties agree to complete the UK Addendum in relation to the Client Personal Data subject to the UK GDPR: (i) the version of the EU SCCs the UK Addendum is appended to shall be the version set out in this DPA and populated at clause 10.4; (ii) the start date shall be the date of the Services Agreement; (iii) the Parties details and Annex details shall be in accordance with clause 10.4; (iv) the competent Supervisory Authority shall be the Information Commissioner; and (v) the data importer shall have the right to terminate the UK Addendum.

10.6. The Parties agree to comply with EU SCCs as populated in clause 10.4 of this DPA in relation to the Client Personal Data subject to the FADP, and as amended as follows: (i) the competent Supervisory Authority shall be the Federal Data Protection and Information Commissioner; (ii) the term 'Member State' will not be interpreted to exclude Data Subjects in Switzerland from initiating legal proceedings in Switzerland; and (iii) references to the 'GDPR' in will be understood as references to the FADP.

10.7. The following additional safeguards are designed to further support the use of the Standard Contractual Clauses by the Parties: (a) Vendor represents that it has not, as of the effective date of this DPA, received any requests under Section 702 of the U.S. Foreign Intelligence Surveillance Act for the Personal Data of residents of EEA, UK, Switzerland or any such other country; (b) Vendor shall provide the Client with notice if it becomes unable to comply with the Standard Contractual Clauses; and (c) if Vendor receives a request for any Client Personal Data from any third party, including a government or law enforcement authority or under Section 702 of the Foreign Intelligence Surveillance Act, Vendor will make commercially reasonable efforts to assert available defenses against making the disclosure and will minimize the scope of any legally required disclosure to only that which is strictly necessary to meet the disclosure obligation.

Schedule 1

Data Processing Instruction

Nature of the Processing	The nature of the Processing involves, but is not limited to, collecting, using, storing, and transferring Client Personal Data.
Purposes of the Processing	For the purposes of providing the Services pursuant to the Services Agreement.
Types of Personal Data including Special Category Personal Data	• Data Exporter may submit Client Data, 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 following categories of Client Data: • As outlined in the Services Agreement.
Categories of Data Subjects	Data Exporter may submit Client Data to the Solution(s), 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 Client Data relating to the following categories of data subjects: • As outlined in the Services Agreement.
Frequency and Duration of the Processing	On a continuous basis for the duration of the Services Agreement.

Schedule 2

Appendix 2

Technical and Organizational Measures

The relevant measures are marked below by a tick in the respective box:

1. Organization Control

- ❑ Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release of data
- ❑ Regular training of employees in data protection matters
- ❑ Appointment of a data protection officer
- ❑ Four-eye-principle
- ❑ _____

2. Access Control of Persons

- ❑ Establishing access authorizations for employees and third parties, including the respective documentations
- ❑ Identity cards, codecard passes, or biometric passes
- ❑ Security locks or electronic locks
- ❑ Restrictions on keys / key codes
- ❑ Security alarm system
- ❑ Constructional measures (fencing, locked doors, locked windows)
- ❑ Specific safety areas with own access control ("closed shops")
- ❑ _____

3. Access Control to Data

- ❑ Access authorization system with specific authorization levels for employees and third parties
- ❑ Pseudonymization and encryption of data
- ❑ Functional and / or time restricted use of terminals and / or terminal users and identification characteristics
- ❑ Guidelines for the creation of secure passwords
- ❑ Automatic screen lock after a certain period of time
- ❑ Logging of events (monitoring of break-in attempts)
- ❑ Logging and analysis of use of the files
- ❑ Protection of internal networks against unauthorized access (e.g. by firewalls)
- ❑ _____

4. Transmission Control

- ❑ Authentication of the authorized personnel both for release and receipt of data
- ❑ Logging of releases and log analysis
- ❑ Encryption of the data in transmission or transport
- ❑ Electronic signature
- ❑ Control of completeness and correctness
- ❑ Implementation of a remote maintenance concept
- ❑ _____

5. Input Control

- ❑ Logging and log analysis of data processing
- ❑ Electronic signature
- ❑ _____

6. Availability Control

- ❑ Execution of a risk and weak point analysis
- ❑ Separation of functions between IT department and other departments
- ❑ Keeping all used software up-to-date (e.g. by updates, patches, fixes, etc.)
- ❑ Existence of an emergency plan (backup contingency plan)
- ❑ Generating backup copies in regular intervals and separate and safe storage
- ❑ Set up of the server in a separately secured server room or datacenter
- ❑ Fire protection measures
- ❑ Emergency power generator
- ❑ Data mirroring
- ❑ _____

7. Separation Control

- ❑ Storage of the data in separated data collectors (physical separation)
- ❑ Authorization policy (logical separation)
- ❑ Multi-Client capability
- ❑ Separation of test data and productive data
- ❑ _____