CSC DATA PROCESSING PROTOCOL

This Data Processing Protocol (including the Appendixes attached hereto, the "**Protocol**") shall apply between:

The CSC entity that is a party to the Service Agreement ("**CSC**")	and	The entity that is procuring Services from CSC under the Service Agreement ("**Customer**")

This Protocol forms part of the Service Agreement in place between CSC and the Customer. This Protocol sets out the obligations and rights of the Customer and CSC in relation to Customer Data.

1. Introduction

a. Pursuant to the terms of the Service Agreement, the Customer wishes to engage CSC to provide the Services, in the course of which CSC will process personal data.

b. Definitions

The following terms have the meanings set forth below for this Protocol:

"**Administrative Purposes**" means the administration and management of this Protocol, resolution of disputes in connection with this Protocol, and compliance with obligations under applicable law.

"**CCPA Consumer**" means any California resident.

"**Competent Supervisory Authority**" means the data protection authority of the jurisdiction where the CSC entity that is a party to the Service Agreement is established.

"**CSC**" means Corporation Service Company (registration number: 0101330) and each of its subsidiaries including, but not limited to, Intertrust Group B.V. and each of Intertrust Group B.V.'s subsidiaries.

"**Customer Data**" means all personal data (as defined by applicable Data Protection Legislation) processed by CSC, in connection with, and for the duration of, the Service Agreement, but shall not include CCPA Consumer personal data.

"**Data Protection Legislation**" means (i) the EU General Data Protection Regulation 2016/679 ("**GDPR**"); (ii) the GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); (iii) the California Consumer Privacy Act (Civ. Code 1798.100-199) ("**CCPA**"); and (iv) the Switzerland Federal Act on Data Protection of 25 September 2020 (which came into force on 1 September 2023) ("**FADP**") together with all other legislation relating to privacy or the protection of individuals with regards to the processing of personal data and including any statute or statutory provision which amends, extends, consolidates or replaces the same, to the extent applicable to the parties. The terms "personal data", "data subject", "controller", "processor" and "process" (and its derivatives) shall have the meanings given to them in the applicable Data Protection Legislation.

"**Data Subject Request**" means a request from a data subject exercising his/her rights under Data Protection Legislation.

"**Data Transfer Agreement**" means an agreement incorporating the SCCs.

"**Information Security Program**" means CSC's program for Services which addresses: human resources security; network security; physical security; change management; vulnerability and patch management; backups, media handling and disposal; access control; incident management; business continuity and disaster recovery; secure development life cycle; and compliance with legal regulations and requirements applicable to CSC's provision of Services.

“**Running System**” means applications provided by CSC directly used by the Customer or as specified in any statement of work or Service Agreement.

“**SCCs**” means Module Two of the standard contractual clauses contained in the annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council and any amendment or replacement pursuant to Article 46(5) of the GDPR and incorporating the Swiss Addendum and/or UK Addendum where relevant.

“**Security Breach**” means a confirmed breach of CSC’s security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

“**Sensitive Data**” means special categories of personal data and criminal offences data, as defined in the GDPR and UK GDPR, in addition to any other information deemed sensitive under applicable Data Protection Legislation.

“**Service Agreement**” means the service agreement between CSC and Customer for the provision of the Services (including any statement of work or other contractual document entered into pursuant to such service agreement).

“**Services**” means the provision of (i) the Running System using server hardware and facilities shared with other CSC customers, which may be subcontracted from a third party and / or (ii) any other services provided by CSC to the Customer pursuant to the Service Agreement.

“**SOC Report**” or “**System and Organization Controls Report”** means an audit report which is prepared by an independent auditor in conformance with Statement on Standards for Attestation Engagements No. 18 (SSAE 18), as promulgated by the American Institute of Certified Public Accountants, or an equivalent or successor report.

“**Swiss Addendum**” means the Addendum set out at Appendix 5 that amends the SCCs for the purposes of any transfers of personal data subject to the FADP and any other relevant Swiss data protection laws or guidance that may be issued by the Federal Data Protection and Information Commissioner from time to time.

“**UK Addendum**” means the International Data Transfer Addendum to the SCCs, as set out in Appendix 4, issued by the ICO under s119A(1) of the Data Protection Act 2018, version B1.0, in force 21 March 2022 and any updates or replacements as may be issued by the ICO from time to time.

2. General

a. The Customer and CSC shall comply with its obligations under applicable Data Protection Legislation in respect of personal data processed by it in connection with the provision of Services as described in Appendix 1 (Data Processing Particulars). Customer agrees to ensure that:

   i. it has the appropriate lawful basis under applicable Data Protection Legislation and has provided all necessary notices to allow CSC to process the Customer Data as envisaged in connection with the Services; and
   ii. The Customer Data is accurate, adequate, relevant and limited to what is necessary in relation to the processing that is envisaged under the Protocol.

b. The parties acknowledge that the status of the parties is a question of fact determined under Data Protection Legislation but agree that, subject to Clause 2(c) of this Protocol, CSC shall act as a processor of behalf of the Customer in respect of the Customer Data and the Customer shall act as a controller.

c. The parties anticipate that each shall act as independent controllers in relation to any processing of Customer Data for the Administrative Purposes.

d. To the extent that CSC receives or processes personal data of CCPA Consumers, CSC shall act as a service provider under the CCPA.

3. CSC's obligations as processor

a. CSC shall:

i. only process Customer Data: (a) to the extent necessary for CSC to provide the Services; and (b) in accordance with the terms of the Service Agreement, and any additional documented instructions of the Customer (save to the extent an instruction from Customer infringes applicable Data Protection Legislation, in which case CSC shall immediately notify the Customer unless such notification is prohibited by the relevant Data Protection Legislation);

ii. implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk relating to its processing of the Customer Data including those described in Appendix 2 (Security Requirements) of this Protocol, which CSC may amend from time to time;

iii. ensure that CSC personnel, who shall have access to Customer Data, shall only be permitted such access on a need-to-know basis, shall only access Customer Data as necessary for the purposes of performing the Services, shall comply with applicable Data Protection Legislation, and shall have entered into appropriate contractually binding confidentiality undertakings;

iv. notify the Customer through standard customer service or account management channels of a Security Breach without undue delay, and provide reasonable cooperation after becoming aware of a Security Breach;

v. provide reasonable cooperation and assistance to the Customer in relation to any Data Subject Request or in relation to a reasonable request, allegation or complaint by a competent authority or data subject, including notifying the Customer in writing without undue delay of receipt of any request (save to the extent prevented from doing so by applicable law);

vi. be entitled to recover any reasonable costs incurred in assisting the Customer in meeting its obligations under the applicable Data Protection Legislation;

vii. be entitled to process or transfer Customer Data in or to any jurisdiction including a jurisdiction outside the United Kingdom, European Economic Area or Switzerland including to any Sub-Processor (as defined below) or member of the CSC group of entities provided that such transfer is permissible under applicable Data Protection Legislation including in accordance with the transfer safeguards specified in Clause 8 of this Protocol; and

viii. Subject to Clause 7 of this Protocol and unless prohibited by applicable law, at the reasonable request of the Customer delete or return to the Customer all Customer Data on termination or expiry of the Service Agreement, provided, however, that: (a) CSC shall be authorized to keep a copy of such Customer Data to the extent required for legal or regulatory purposes as well as for the exercise or defense of legal claims; and (b) the foregoing obligation shall not extend to automatically generated computer or data storage system back-up or archival copies generated in the ordinary course of CSC's information system procedures ("**Archives**") where it is not commercially or technically feasible to implement the foregoing obligations regarding the Archives, provided that CSC shall make no further use of such Archives.

4. CCPA Processing Obligations

a. To the extent that CSC receives or processes personal data of CCPA Consumers, CSC shall act as a service provider under the CCPA.

b. CSC shall:

   i. only process CCPA Consumer personal data in order to provide the Services and as required by applicable Data Protection Legislation; not retain, use or further disclose CCPA Consumer personal data for its own commercial purpose or for any purpose outside of the direct business relationship with Customer or the business purpose covered by the services; not sell, disclose, share or provide access to CCPA Consumer personal data for monetary or other valuable consideration; and not further collect CCPA Consumer personal data except as necessary to perform the services.

   ii. implement appropriate technical and organizational measures and cooperate with the Customer in the fulfilment of the Customer's obligations to respond to requests by CCPA Consumers for disclosure of information or information practices and for deletion of personal information as permitted by the CCPA.

   iii. promptly and in any event within ten (10) days of the date of a Customer request for deletion of personal data about a CCPA Consumer who has made demand on Customer for deletion, delete and procure the deletion of all copies of CCPA Consumer personal data, provided however, that CSC may retain personal data to the extent permitted by the CCPA and only to the extent and for such period as required by applicable Data Protection Legislation, provided that CSC shall ensure the confidentiality of all such personal data and shall ensure that such personal data is only processed as necessary for the purpose(s) specified in the applicable Data Protection Legislation requiring its storage and for no other purpose.

c. CSC certifies that CSC understands its obligations and the restrictions on its use of CCPA Consumer personal data under this Protocol and the CCPA and agrees to adhere to such obligations and restrictions.

5. **Audit**

a. To the extent required by Data Protection Legislation, CSC shall maintain a record of its processing activities and provide such cooperation and information to the Customer as is reasonably necessary for the Customer to demonstrate compliance with Data Protection Legislation. Such cooperation shall include permitting the Customer, at its sole cost and expense, to audit CSC's compliance with this Protocol provided that (unless expressly required otherwise by any competent authority):

   i. reasonable notice of not less than thirty (30) days is given of any proposed audit and the parties shall, acting reasonably, agree the scope and parameters of any such audit;

   ii. to the extent the audit scope is covered in any audit carried out for CSC by an independent third party auditor within eighteen (18) months prior to the Customer's audit request and there have been no material changes to the controls audited, CSC may share the report to the extent relevant to the Customer and the disclosure of such report shall be deemed to satisfy the audit request made by the Customer;

   iii. such audit shall be conducted during regular business hours, subject to CSC's policies and may not unreasonably interfere with CSC's business activities;

   iv. the audit shall be subject to CSC's duties of confidentiality owed to any of its customers or employees and shall not extend to CSC's subcontractors (including any Sub-Processors); and

   v. the rights granted in this Clause 5 may not be exercised more than once in any calendar year.

6. Review of Controls

Upon written request from Customer at any time during the term of the Service Agreement, CSC shall provide to Customer relevant information on it information security controls, which shall constitute CSC's Confidential Information.

7. Third Party Relationships

a. CSC shall be permitted to appoint third parties to process Customer Data on its behalf ("**Sub-Processors**"), and to disclose Customer Data to the Sub-Processors in accordance with this Protocol, provided that CSC ensures that (a) such processing is subject to a written contract or other legal act with such Sub-processors containing data protection obligations no less onerous than those set out in this Protocol and (b) CSC shall remain liable for the acts and omission of any such Sub-processors with respect to the processing of Customer Data.

b. CSC shall notify the Customer of intended changes concerning the addition or replacement of Sub-Processors ("**New Sub-Processors**") by updating its website ("**CSC's Notification**").

   i. If the Customer has any reasonable objection to the appointment of New Sub-Processors on the grounds that such New Sub-Processor: (a) would put the Customer in breach of its obligations under the Data Protection Legislation (or any other applicable law); or (b) is a direct competitor of the Customer, the Customer shall notify CSC of this objection in writing within a reasonable period after CSC's Notification pursuant to this clause 7(b)(i). In the event of such an objection by the Customer, CSC shall work with Customer to address its objections and if the Customer's objections have not been addressed within a reasonable period from the date of CSC's Notification, CSC shall notify the Customer of its option to terminate the Service Agreement in accordance with termination clause of the Service Agreement in respect to the affected Services which cannot be provided by CSC without the use of the New Sub-Processor.

   ii. If the Customer does not object to the New Sub-Processor within the time period stipulated in clause 7(b)(i) then the Customer will be deemed to have authorized the appointment of the New Sub-Processor.

8. International transfers

Where the Customer transfers Customer Data that is subject to the GDPR, UK GDPR or FADP to CSC and CSC is located in a territory outside the United Kingdom, European Economic Area or Switzerland (as applicable) which is treated as a third country under the GDPR, UK GDPR or FADP and which has not been deemed to provide an adequate level of protection of personal data pursuant to the applicable Data Protection Legislation ("**Third Country**"), the Customer agrees that, unless there is an alternative valid basis for ensuring that the transfer is lawful under Data Protection Legislation as notified by CSC, the SCCs (as interpreted in accordance with and supplemented by Appendices 3, 4 and 5) shall be deemed to be incorporated into this Protocol and represent a relevant Data Transfer Agreement in relation to such transfer.

i. Where CSC transfers Customer Data to a Sub-processor located in a Third Country, CSC and the Sub-processor shall enter into a Data Transfer Agreement. If any conflict arises between the Protocol and the Data Transfer Agreement, the provisions of the Data Transfer Agreement shall prevail in respect of the transferred Customer Data.

ii. Upon a change in Data Protection Legislation or law, updates to the SCCs required by a competent authority or such change in law shall be deemed automatically incorporated into this Protocol and, to extent such amendments need explicit confirmation, the parties acknowledge it may be necessary for CSC to unilaterally amend this Protocol which shall be deemed effective upon written notice to the Customer. The Customer shall provide reasonable co-operation including executing all necessary documents to facilitate such changes in order to comply with Data Protection Legislation.

9. Remedies and liability

Each Party's liability to the other shall be governed by the terms of the Service Agreement.

10. **Applicable Law and Jurisdiction**
    The processing of Customer Data under this Agreement shall be governed by the governing law of the Service Agreement. Any action related to this Protocol, or the execution thereof shall be governed by the terms of the Service Agreement, including terms about the competent court.

11. **Termination**
    This Protocol shall terminate automatically upon the termination of the Service Agreement.

12. **Notices**
    Unless agreed otherwise between parties, any notice permitted or required under this Protocol shall be sent by email to the email address stipulated in the Service Agreement and then confirmed in writing, and shall be deemed given two (2) hours after the time the email was sent, unless the sender receives an automated message that the email has not been delivered.

13. **Miscellaneous**
    Subject to changes required under applicable law under Clause 8, any amendment to this Protocol shall be published on the website of CSC. Neither party may assign its rights or obligations under this Protocol without the written consent of the other party, with such consent not to be unreasonably withheld. If any part of this Protocol is held invalid or unenforceable, the validity of the remaining provisions shall not be affected. In the event of a conflict or inconsistency between this Protocol and the provisions of the Service Agreement and/or any other related agreements between the Parties existing at the time of this Protocol, the provisions in this Protocol shall prevail.

APPENDIX 1 (DATA PROCESSING PARTICULARS)

Data subjects

The personal data processed concern the following categories of data subjects:

Natural persons who are (i) prospects, customers, business partners and vendors of the Customer, (ii) employees and contact persons of prospects, customers, business partners and vendors of the Customer, (iii) employees, agents, advisors, and freelancers of the Customer, and (iv) any other users authorized by the Customer to use the Services.

Categories of data

The personal data processed concern the following categories of personal data:

The Customer may submit personal data to CSC, the extent of which is determined and controlled by the Customer in its sole discretion. Personal data may include, but is not limited to, the following categories: full name, title, position, employer, contact information (company, phone, email, fax, physical address), and identification data, professional life data, connection data, and localization data.

Sensitive Data (if appropriate)

The personal data transferred concern the following Sensitive Data:

In certain circumstances, Customer may upload information into CSC's web-based system. That Customer Data could include Sensitive Data of which the customer is the controller.

Processing operations

The personal data processed will be subject to the following basic processing activities:

- Receiving data, including collection, accessing, retrieval, recordings and data entry.
- Holding data, including storage, organization and structuring.
- Protecting data, including restricting, encrypting and security testing.
- Returning data to the data exporter.
- Erasing data, including destruction and deletion.

Duration of the processing

The duration of the provision of the Services.

APPENDIX 2 (SECURITY REQUIREMENTS)

RULES AND PROCEDURES. CSC shall have a documented a set of rules and procedures regulating the management, protection and distribution of systems and information, including Customer Data. Such rules and procedures shall comply with the requirements set forth in this Protocol and Data Protection Legislation. CSC's Information Security Program will contain administrative, technical, and physical safeguards reasonably designed to maintain confidentiality, integrity, and availability of Customer Data; protect against anticipated threats to the security of Customer Data; protect against unauthorized access to or use of Customer Data; and delete Customer Data from the Running System upon request.

SECURITY POLICY. CSC will maintain and enforce written information security policies and procedures and incident response programs required to comply at a minimum with (i) all applicable privacy regulations and (ii) industry standards in accordance with the security requirements contained in this Appendix 2. Such security requirements are intended to provide reasonably appropriate safeguards against accidental, unauthorized, and unlawful destruction, loss, exfiltration, alteration, theft, exposure, disclosure, acquisition, or access to Customer Data.

ORGANIZATIONAL SECURITY. CSC shall establish organizational requirements ensuring proper competence and training of CSC personnel. CSC shall maintain a process to detect changes in the job function, employment status and other changes that may require changes to the network access or permission rights of CSC personnel. When an individual is terminated, CSC shall promptly disable such individual's access to all CSC's systems and Customer Data. CSC shall use commercially reasonable efforts to ensure that its personnel: (1) do not attempt to obtain access to any programs or data beyond the scope of the access granted and (2) otherwise comply with the requirements of this Protocol. CSC shall at all times remain liable for any actions or omissions of its personnel or third-party contractors that would constitute a breach of this Protocol.

SPECIFIC SECURITY PRACTICES. CSC shall do the following:

a. Have trained, full-time employees assigned to information security roles, who are responsible for the implementation, operation and maintenance of the Enterprise Security Program;
b. Require, as applicable based on employment positions, that relevant employees receive regular security awareness training;
c. Review and revise the Information Security Program regularly to reflect changes in operational status;
d. Ensure the data center used to provide Services maintain a physical security plan commensurate with industry standards;
e. Investigate employee backgrounds as applicable based on employment role, require that employees sign a confidentiality agreement, and revoke access to Services for terminated employees;
f. implement and maintain a vulnerability and patch management procedures;
g. maintain processes for testing, approving and applying patches; and
h. at its sole cost and expense, CSC shall perform, no less than once in every twelve (12) month period, a vulnerability threat assessment test or penetration test on the Services production network using industry standard threat assessment tools and methods.

ASSET MANAGEMENT. CSC shall maintain reasonable controls to protect CSC hardware and software assets that contain Customer Data.

PHYSICAL AND ENVIRONMENTAL. CSC shall maintain reasonable controls to protect the physical security of Customer Data maintained by CSC. Physical access to facilities shall be restricted through use of access control procedures for authorized users (e.g., badge access, turnstile entry doors, security guards at the entrance, and security alarms, as appropriate). Servers and computer equipment shall be secure from environmental hazards, and CSC shall maintain reasonable environmental controls based on the nature of the facility (e.g., climate control, smoke/heat detectors, fluid/water sensors and backup generators, as appropriate).

ACCESS CONTROL. The logical access process shall restrict user (local or remote) access based on user job function for applications, databases and remote users. User access recertification to determine access and privileges shall be performed periodically. Procedures for onboarding and off boarding users in a timely manner shall be documented, including prompt removal of access from staff whose employment is terminated. CSC will maintain and implement access control procedures that address:

(a) Account creation and password policies designed to reduce unauthorized access;
(b) Sharing credentials with unauthorized personnel;
(c) Management of access for employee terminations or transfers; and
(d) Session timeouts.

COMMUNICATION AND CONNECTIVITY. CSC shall implement controls over its communication network to safeguard Customer Data. All Customer Data from the Running System shall be stored and maintained in a manner that allows for its return upon request from Customer.

CHANGE MANAGEMENT. Changes to CSC's system, network, applications, data files structures, other system components and physical/environmental changes shall be monitored, controlled and reviewed through a formal change control environment. To that end, CSC shall implement and maintain a change management program for Services which requires that:

(a) Changes are made within a formal change control program that tracks, documents, tests, and approves change requests prior to implementation.
(b) Proposed Services system changes are reviewed so as to not compromise the security of the Services environment.
(c) Segregation of development, test and production environments is practiced.

ENCRYPTION. Customer Data shall be encrypted while in transit over the Internet. Laptops and removable storage devices that contain Customer Data shall be encrypted. Key management procedures shall be employed that assure the confidentiality, integrity, and availability of cryptographic key material.

SYSTEM DEVELOPMENT. CSC shall have an established software development lifecycle ("**SDLC**") for the purpose of defining, acquiring, developing, enhancing, modifying, testing, or implementing information systems. The SDLC methodology shall include version control and release management procedures. SDLC shall contain security activities that foster development of secure SDLC methodology and shall include requirements for documentation and be managed by appropriate access controls. Software vulnerability assessments shall be conducted on an on-going basis internally or using external experts and any critical findings identified shall be remediated in a timely manner. Where Customer Data is used in a test environment, the level of control shall be consistent with production controls. Production data shall be sanitized before use in non-production environments. Developer access to production environments shall be restricted by policy.

BUSINESS CONTINUITY AND DISASTER RECOVERY. Formal business continuity plans shall be in place. CSC has a disaster recovery facility that is geographically remote from its primary data center, along with required hardware, software, and Internet connectivity, in the event CSC production facilities at the primary data center were to be rendered unavailable. CSC has disaster recovery plans in place and tests them at least once per year.

BACK-UP AND OFFSITE STORAGE. CSC shall have a defined back-up policy and associated procedures for performing back-up of data in a scheduled and timely manner. Effective controls shall be established to safeguard backed-up data (on-site and off-site). CSC shall also ensure that Customer Data is securely transferred or transported to and from back-up locations and conduct periodic tests to ensure that data may be safely recovered from backup devices.

APPENDIX 3

SCCs

The terms of the SCCs, including the clauses and optional provisions such as those as set out in Part 1 (Options Applicable to the SCCs) of this Appendix 3 and the Appendix Information set out in Part 2 (Appendix Information to the SCCs) of this Appendix 3, are incorporated and brought into effect here by reference for the purposes of this Protocol.

Part 1: Options Applicable to the SCCs

The Parties agree that the options set out below shall apply to these SCCs.

Options	Module Two
Clause 7 (Docking Clause)	Applicable
Clause 11 *(Option)*	Not Applicable
Clause 9a (Prior Authorisation or General Authorisation)	General Authorisation
Clause 9a (Time period)	in a reasonable period of time
Clause 17 Governing Law	As determined in clause 10 of this Protocol
Clause 18 Choice of Forum and Jurisdiction	As determined in clause 10 of this Protocol

Part 2: Appendix Information to the SCCs

ANNEX I

A. LIST OF PARTIES

Exporter(s):

Name: Customer
Address: As set out in the Service Agreement
Contact person's name, position and contact details: As set out in the Service Agreement
Role (controller/processor): Controller

Importer(s):

Name: CSC
Address: As set out in the Service Agreement
Contact person's name, position and contact details: As set out in the Service Agreement
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Activities relevant to the data transferred under these Clauses:

See Appendix 1 (Data Processing Particulars).

Categories of data subjects whose personal data is transferred

See Appendix 1 (Data Processing Particulars).

Categories of personal data transferred

See Appendix 1 (Data Processing Particulars).

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Appendix 1 (Data Processing Particulars).

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

Continuous basis.

Nature of the processing

See Appendix 1 (Data Processing Particulars).

Purpose(s) of the data transfer and further processing

See Appendix 1 (Data Processing Particulars).

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

See Appendix 1 (Data Processing Particulars).

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Transfers to Sub-processors will occur where necessary for the provision of the Services in accordance with the Protocol.

C. COMPETENT SUPERVISORY AUTHORITY

The data protection authority of the jurisdiction where the CSC entity that is a party to the Service Agreement is established.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Appendix 2 (Security Requirements)

ANNEX III – LIST OF SUBPROCESSORS

A list of CSC’s Sub-processors can be found on its website.

APPENDIX 4

UK ADDENDUM

The terms of the UK Addendum, including the clauses and the Appendix Information set out in Parts One to Three of this Appendix 4, are incorporated and brought into effect here by reference for the purposes of this Protocol.

Part 1: Parties

Start date	Date of the Service Agreement.	
The Parties	**Exporter:** Customer - as defined in the Service Agreement	**Importer:** CSC – as defined in the Service Agreement.
Parties' Key Contacts **(Full name, job title and contact details)**	As set out in the Service Agreement	As set out in the Service Agreement

Part 2: Selected SCCs, Modules and Selected Clauses

Addendum SCCs	☒ The version of the SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Date of the Service Agreement.

Part 3: Appendix Information

As set out in Part One of Appendix 3 (SCCs).

Part 4: Ending this Addendum when the approved UK Addendum changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum: ☐ Importer ☐ Exporter ☒ neither Party

APPENDIX 5

SWISS ADDENDUM

The SCCs shall be read and amended to the extent necessary that they operate for transfers of personal data subject to the FADP and fulfil the intention to provide the appropriate safeguards as required by relevant Data Protection Legislation in Switzerland. Those amendments are incorporated and brought into effect here by reference for the purposes of this Protocol.

Part 1: Transfers subject to FADP and the GDPR

The Parties agree that the amendments set out below shall apply to the SCCs when transfers of personal data are subject to both the FADP and the GDPR.

SCCs Reference	Amendments
Clause 8.7 (Sensitive data)	The term 'sensitive data' shall include data on the intimate sphere, health or racial origin, trade union, political, religious or ideological views or activities, administrative and criminal proceedings and sanctions and social security measures.
Clause 13a (Supervision) and Annex I.C	The Swiss Federal Data Protection and Information Commissioner shall hold the position of "competent supervisory authority" in parallel with: (a) the *Autoriteit Persoongegevens* where the data exporter is established in the Netherlands; or (b) one of the other EU national data protection authorities that may be competent authorities where the data exporter is established in another Member State.
Clause 18(c) (Choice of Forum and Jurisdiction)	The term "Member State" as used in the SCCs must not be interpreted in such a manner as to exclude data subjects in Switzerland from the possibility of bringing legal proceedings against the Data Exporter and/or Data Importer in their place of habitual residence where that habitual residence is in Switzerland

Part 2: Transfers subject solely to the FADP

The Parties agree that the amendments set out below shall apply to the SCCs when transfers of personal data are subject solely to the FADP.

SCCs Provision	Amendments
"Regulation (EU) 2016/679"	References to Regulation (EU) 2016/679 shall be understood as references to FADP and its implementing ordinance and their corresponding provisions, as applicable.
Clause 8.7 (Sensitive data)	The term 'sensitive data' shall include data on the intimate sphere, health or racial origin, trade union, political, religious or ideological views or activities, administrative and criminal proceedings and sanctions and social security measures.
Clause 13a (Supervision) and Annex I.C	The Swiss Federal Data Protection and Information Commissioner shall hold the position of "competent supervisory authority".
Clause 17 (Governing Law)	The SCCs shall be governed by Swiss law or the law of a country that allows and grants rights as a third-party beneficiary.
Clause 18(b) (Choice of Forum and Jurisdiction)	Any dispute arising from the SCCs shall be resolved by the courts of a jurisdiction of the Parties' choice.
Clause 18(c) (Choice of Forum and Jurisdiction)	The term "Member State" as used in the SCCs must not be interpreted in such a manner as to exclude data subjects in Switzerland from the possibility of bringing legal proceedings against the data exporter and/or data importer in their place of habitual residence where that habitual residence is in Switzerland.