STURDY DATA PROCESSING AGREEMENT

Last Modified: November 20, 2025

This Sturdy Data Processing Agreement ("**DPA**") addresses the processing and transfer of Personal Data under the Master Services Agreement, order form, statement of work or other contract for the provision of Services ("**Services Agreement**") by SturdyAI Inc., acting on its own behalf and as agent for each SturdyAI Inc. Affiliate ("**Sturdy"**) for the counterparty that entered in to the Services Agreement ("**Customer**") (each a "**Party**" and collectively, the "**Parties**"). To the extent the terms of this DPA conflict with the Services Agreement with regard to the processing of Personal Data, the terms of this DPA shall prevail.

Article 1. Definitions

"Affiliate: means any entity that directly or indirectly controls, is controlled by, or is under common Control with the subject entity. "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Applicable Law(s)"** means as applicable and binding on Customer, Sturdy and/or the Services:

a. any law, statute, regulation, bylaw or subordinate legislation in force from time to time to which a Party is subject and/or in any jurisdiction that the services are provided to or in respect of;
b. the common law and laws of equity as applicable to the Parties from time to time;
c. any binding court order, judgment or decree; or
d. any applicable direction, policy, rule or order that is binding on a Party and that is made or given by any regulatory body having jurisdiction over a Party or any of that Party's assets, resources or business.

"**Appropriate Safeguards"** means legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time.

"**Customer Data"** means Personal Data received by Sturdy from or on behalf of Customer or Customer Affiliate in connection with the performance of Sturdy's obligations under this DPA, as set forth in **Annex A**, and the Services Agreement.

"**Data Protection Laws"** means any Applicable Law governing the privacy and security of personally identifiable information, such as:

a. the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**");
b. Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024 ("**EU AI Act**");
c. the Data Protection Act 2018 and any laws implementing the GDPR;
d. the GDPR, as it forms part of the law of England and Wales, Scotland and Northern Ireland (i.e., the "**UK GDPR**") as provided in the Data Protection Act 2018, and/or any corresponding or equivalent national laws or regulations;
e. the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 *et seq.*) , and as may be amended, supplemented, or otherwise modified from time to time, including by virtue of the California Privacy Rights Act ("**CPRA**")(collectively, the "**CCPA**";
f. Switzerland's Federal Act on Data Protection ("**FADP**"), as amended:
g. the laws of any country or other jurisdiction (including, without limitation, the United States and its states) that may apply to the Services, including the Virginia Consumer Data Protection Act

("**VCDPA**"), the Colorado Privacy Act ("**CPA**"), the Utah Consumer Privacy Act ("**UCPA**"), An Act Concerning Personal Data Privacy and Online Monitoring (Connecticut); and any laws replacing, amending, extending, re-enacting or consolidating any of the enumerated laws above from time to time.

"**Data Subject"** means the identified or identifiable person to whom the Personal Data relates.

"**Data Subject Request"** means a request made by a Data Subject to exercise any rights of Data Subjects under applicable Data Protection Laws.

"**Personal Data"** means:

a. all individually identifiable information created, collected, accessed, received or otherwise processed pursuant to the Services performed under the Services Agreement; and
b. any other information that applicable Data Protection Laws treat as "personal data" (or equivalent term, including without limitation, "personal information," "personally identifiable information," and "nonpublic personal information").

"**Personal Data Breach"** means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Personal Data or any other unlawful acquisition, use or handling of Personal Data.

"**Personnel"** means all persons engaged or employed from time to time by either Party in connection with the Services Agreement, including employees, consultants, contractors and permitted agents.

"**Services**" means the products or services Sturdy provides Customer under the Services Agreement.

"**Sub-processor"** means another processor engaged by Sturdy for carrying out processing activities in respect of the Customer Data on behalf of Customer.

Terms used but not defined in this DPA (e.g., "processing", "controller", "processor", "business", "service provider", "supervisory authority") shall have the same meaning as set forth in the Services Agreement and applicable Data Protection Laws.

In this DPA references to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including the any new Data Protection Laws from time to time) and the equivalent terms defined in such Applicable Laws, once in force and applicable.

Article 2. <u>Roles</u>

1. This DPA applies to Sturdy's processing of Personal Data in Sturdy's provision of the Services and defines the principles and procedures that Sturdy shall adhere to in its role as a data processor. The Parties agree that this DPA outlines Customer's complete processing instructions for Study under the Services Agreement.

2. For purposes of this DPA, Customer and Sturdy agree that Customer is the controller (or "business" as that term is defined by the CCPA) of Customer Data and Sturdy is a processor of Customer Data (or "service provider" as set forth in the CCPA).

Article 3. U.S.-Specific Processing Requirements

The Parties agree that Data Protection Laws also include any United States federal and state laws applicable to the processing of Personal Data. Sturdy acknowledges that it shall act as a "service provider" or "contractor" where such term is defined under applicable Data Protection Laws and comply with all such obligations under applicable U.S. Data Protection Laws. Sturdy shall not: (i) sell or share (as defined under U.S. Data Protection Laws) Customer Data; (ii) collect, retain, use, or disclose Customer Data for any purpose other than providing the services specified in the agreement(s) between Customer and Sturdy; (iii) collect, retain, use, or disclose Customer Data outside of the direct business relationship between Customer and Sturdy; or (iv) combine Customer Data with Personal Data that Sturdy obtains from other sources or that Sturdy collects itself. Sturdy acknowledges that the Personal Data Customer discloses is provided for a "business purpose" (as defined under Data Protection Laws), including those business purposes outlined in this DPA. Sturdy understands that Customer may exercise any right of a controller or "business" under Data Protection Laws including, but not limited to, any right that (a) permits Customer to take reasonable and appropriate steps to ensure that Sturdy uses Customer Data consistent with Customer's business purpose (b) stops or remediates Sturdy's unauthorized use or misuse of Customer Data, upon notice to Sturdy. Without unreasonable delay, Sturdy shall notify Customer if it can no longer meet its obligations under the U.S. Data Protection Laws. Sturdy certifies that it understands the prohibitions outlined in this Article 3 and will comply with them.

Article 4. Scope of Personal Data Processing

1. Customer determines the scope of Customer Data to which Customer provides Sturdy access to perform the Services. Accordingly, the collection, processing and/or use of Personal Data may relate to the categories of data presented in **Annex A** to this DPA.

Article 5. Data Processing Instructions

1. Sturdy shall:

   a. process the Customer Data only (i) on written instructions from Customer, as further specified in this DPA, or (ii) where required to do so under applicable Data Protection Laws to which Sturdy is subject. Customer hereby acknowledges that by virtue of using the Services, it gives Sturdy instructions to process and use Customer Data in order to provide the Services in accordance with the Services Agreement and as further described in **Annex A;**

   b. ensure that persons authorized to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory or contractual obligation of confidentiality;

   c. take all applicable measures required of Sturdy as a data processor pursuant to applicable Data Protection Laws, as further specified in Article 10 below;

   d. respect the conditions referred to in Article 7 for engaging another processor of Customer Data to provide the Services;

   e. provide Customer reasonable assistance in the fulfilment of Customer's obligations to respond to Data Subject requests, as applicable and required by Data Protection Laws;

   f. assist Customer in ensuring compliance with the obligations pursuant to applicable Data Protection Laws, taking into account the nature of processing and the information available to Customer;

g. return or provide an opportunity for Customer to retrieve or otherwise securely delete all Customer Data after the end of the provision of Services. At Customer's written request, Sturdy shall delete any Personal Data except for (i) secure back-ups deleted in the ordinary course of business according to an established data retention policy, and (ii) retention as required by Applicable Law;

h. make available to Customer information reasonably necessary to demonstrate compliance with this DPA and Applicable Law;

i. ensure that only Personal Data which is strictly necessary for the legitimate conduct of the processing is collected and processed. Further, Sturdy shall provide information on the processing of Customer Data required by Data Protection Laws. Where required, Sturdy shall communicate the essential content of this DPA to the Data Subjects;

j. inform Customer if, in Sturdy's opinion, any written instruction from Customer infringes Data Protection Laws, provided that Sturdy shall have no obligation to independently inspect or verify Customer's use or processing of Personal Data; and

k. inform Customer of and provide reasonable assistance in meeting Customer's obligations in regard to any Personal Data Breach of Customer Data, in accordance with Article 11 below.

2. Where Sturdy engages another Sub-processor for carrying out specific processing activities on Customer's behalf as part of the Services, the same data protection obligations as set out in this DPA shall be imposed on that Sub-processor applicable by way of a contract, or other legal act under Applicable Law. Sturdy shall engage any such Sub-processor in accordance with the terms of Article 7 below.

Article 6. Customer Obligations.

Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired the Personal Data, including providing any required notices to, and obtaining any necessary consent from, its clients, Data Subjects, employees or contractors who qualify as end-users for the Services. Should Customer learn that it has provided Personal Data that may not be shared pursuant to a consent or data privacy notice, Customer shall promptly notify Sturdy in writing, at privacy@sturdy.ai. Customer acknowledges and agrees that Sturdy shall not be liable for the Processing of any Personal Data (including Customer Data) in which Customer (i) failed to obtain consent from the relevant Data Subject to process such Personal Data or (ii) possess a lawful basis to process such Personal Data. Additionally, Customer shall comply with (a) the obligations of a data controller, "business," or equivalent term (as these terms are defined under Applicable Laws) under all applicable Data Protection Laws; (b) all terms of the Services Agreement; and (c) all terms of this DPA.

Article 7. Sub-processing

1. Subject to the terms of this Article 7, Customer consents to Sturdy engaging Sub-processors for the processing of Customer Data.

2. Customer hereby acknowledges and expressly agrees that (i) Sturdy may engage the Sub-processors listed in **Annex C**, (ii) Sturdy is entitled to retain its Affiliates as Sub-processors, and (iii) Sturdy or any such Sturdy Affiliate may respectively engage any third parties to process Customer Data on Sturdy's behalf in connection with the provision of Services. Sturdy (and each Sturdy Affiliate) may continue to use those Sub-processors already engaged by Sturdy or any Sturdy Affiliate as of the date of this DPA. If customer wished to be notified of new Sub-processors it can subscribe to notification by sending an email to privacy@sturdy.ai.

3. Customer may object to Sturdy's use of a new Sub-processor by notifying Sturdy promptly in writing within (30) thirty days of receipt of Sturdy's notification of a new Sub-processor. If Customer objects within

this time frame, Sturdy will make a reasonable effort to provide the Service in order to comply with the Customer's request. If Sturdy cannot comply with the customer's request within (60) sixty days of said request, then Customer may terminate the Service. Sturdy will refund any prepaid fees remaining on their subscription, on a pro-rata basis from the date of termination.

4. Sturdy will ensure that Sub-processors are bound by written agreement(s) that require Sub-processors to process Customer Data only as authorized by Sturdy and provide the same level of data protection required of Sturdy under this DPA.

5. Sturdy remains responsible at all times for compliance with this DPA as applicable. Where the Sub-processor fails to fulfill its obligations under any written agreement, Sturdy shall remain fully liable to Customer for the performance of the Sub-processor's obligations.

Article 8. Onward and International Data Transfer

In the event Customer requests Sturdy to transfer Customer Data across national borders, and without prejudice to the Data Subject's rights, Sturdy agrees to consult with Customer to ensure the lawful export of Customer Data through an Appropriate Safeguard, including those safeguards in **Annex D**. If a listed Appropriate Safeguard is, or becomes applicable under new Data Protection Laws, it shall be deemed to be signed by Sturdy and Customer by execution of the Services Agreement and is incorporated into this DPA by reference. Applicable Appropriate Safeguards shall be hereby effective upon the commencement of any transfer of Personal Data by either Party.

Article 9. Assistance with Data Subject Requests

1. Sturdy will make available to Customer the Personal Data of Customer's Data Subjects and the ability to fulfill requests by Data Subjects to exercise one or more of their rights under applicable Data Protection Laws in a manner consistent with the Services. Sturdy shall comply with reasonable requests to assist with Customer's response to Data Subjects.

2. If Sturdy receives a request from Customer's Data Subject to exercise one or more of their rights under applicable Data Protection Laws, will redirect the Data Subject to make their request directly to Customer.

Article 10. Technical and Organizational Controls and Security

Sturdy shall maintain the technical and organizational controls and security measures for the protection of Customer Data as set forth in this DPA, including **Annex B**. Sturdy may update its security practices and other security documentation without notice provided that the measures implemented during any term of Service shall in no event provide less protection than those included as of the effective date of such term.

Article 11. Personal Data Breach

1. Notice Requirement. Sturdy shall notify Customer without unreasonable delay after becoming aware of a Personal Data Breach relating to Customer Data.

2. Notice to Supervisory Authorities. Sturdy shall also ensure it complies with Applicable Laws concerning Personal Data Breaches and with its obligations to notify any supervisory authority as required by Applicable Law.

3. Public Statement. Customer shall not issue any public statements regarding Sturdy or engage in any correspondence with a supervisory authority on behalf of Sturdy unless Sturdy has first agreed, in

writing, to the issuance of the public statement or correspondence. Customer shall notify Sturdy in advance of any written statements it makes to Supervisory Authorities regarding Sturdy, unless otherwise prohibited by Applicable Law.

4. No Admission of Fault. Sturdy's obligation to report or respond to a Personal Data Breach under this Article is not and will not be construed as an acknowledgement by Sturdy of any fault or liability of Sturdy with respect to such Personal Data Breach.

Article 12. DPIA; Records of Processing Activities

1. If a data protection impact assessment is required pursuant to Data Protection Laws (including Article 35 of the GDPR), Sturdy shall cooperate and provide reasonable assistance to Customer in the performance of such assessment(s), to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Sturdy.

2. Sturdy shall maintain all applicable records of data processing activities required by Article 30(2) of the GDPR and other applicable Data Protection Laws.

Article 13. Audit right

1. Customer may carry out audits of Sturdy's processing of Customer Data as required by Data Protection Laws, subject to Customer:

a. giving Sturdy at least thirty (30) days prior written notice of such audit being required by Customer;

b. ensuring that all information obtained or generated by Customer or its auditor(s) in connection with such audits is kept strictly confidential and saved for disclosure to a supervisory authority or as otherwise required by Applicable Law;

c. ensuring that such audit is undertaken during normal business hours, with minimal disruption to Sturdy's business, Sub-processors' business, or the business of other clients of Sturdy; and

d. providing, at no charge to Sturdy, a full copy of all findings of the audit.

2. Third-Party Auditors. Customer may use a third-party auditor with Sturdy's written agreement, which shall not be unreasonably withheld. Prior to any third-party audit, such auditor shall be required to execute an appropriate confidentiality agreement with Sturdy.

3. Notice of Failure to Comply. After conducting an audit under this Article 13 or after receiving an audit report from Sturdy, Customer must notify Sturdy, in writing, of the specific manner, if any, in which Sturdy does not comply with any of the security, confidentiality, or data protection obligations in this DPA or Data Protection Laws, if applicable. Any such information will be deemed confidential information of Sturdy. Upon such notice, Sturdy will use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations.

Article 14. Counterparts, Modification, Supplementation, and Term

1. Counterparts. Should any provisions of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained herein.

2. Modification. The Parties may modify or supplement this DPA, with notice to the other Party, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement Appropriate Safeguards such as Standard Contractual Clauses, (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40 and 42 of the GDPR or similar provisions in applicable Data Protection Laws, or (v) to comply with any request or requirement imposed by an applicable third-party data controller.

3. Supplementation. Without prejudice to this DPA, either Party may from time to time provide additional information and detail about how it will execute this DPA in its product-specific technical, privacy, or policy documentation.

4. Term. This DPA shall expire upon the later of (a) the termination of the Services Agreement, (b) cessation of any processing of Customer Data by Sturdy on behalf of Customer, or (c) delivery of written notice of termination of the Services Agreement from one Party to the other.

5. Liability and Indemnity. This DPA is subject to the limitations of liability and indemnity set forth in the Services Agreement.

Article 15. Governing Law.

1. This DPA and any disputes or claims arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) are governed by, and construed in accordance with, Idaho and controlling United States federal law or, if required under Data Protection Laws, the governing law required by such Data Protection Laws.

2. This DPA is subject to the governing law and exclusive jurisdiction set forth in the Services Agreement.

Executed by the Authorized Representatives

SturdyAI, Inc.	**Controller:**_____
Signature:	**Signature:**
Name: Nathaniel Hazelton	Name:_____
Title: Data Privacy Officer	Title:_____
	Date:

ANNEX A TO DATA PROCESSING AGREEMENT

Details of Personal Data Processing

Purpose(s) of Processing
The Personal Data is to be processed for purposes of supporting Customer operations and services in accordance with the Services Agreement.

Processing Operations
The Personal Data processed will be subject to the basic processing activities as applicable and as described in the Services Agreement and below:

- Continuous transfer of Customer Data (which may be anonymized) to provide actionable insights on Customer's business practices, including personnel retention.

Types of Personal Data
The following Personal Data may be processed by Sturdy and its Affiliates on behalf of Customer or Customer Affiliates. The Personal Data processed includes the following:

- Personal Data relating to individuals which is provided by Customer, such as Personal Data related to Customer personnel, business contact details, and connection data.

Sensitive Data (if appropriate).
The Personal Data processed concern the following categories of data:

- None. N/A.

Categories of Data Subjects to Whom the Personal Data Relates

- Customer may submit Personal Data to Sturdy, the extent of which is determined and controlled by Customer in its sole discretion. This may include, but is not limited to Personal Data relating to the following categories of data subjects:
    - Customer's employees, users, clients, agents, subcontractors, and customers.

ANNEX B TO DATA PROCESSING AGREEMENT

TECHNICAL AND ORGANIZATIONAL MEASURES

Sturdy maintains commercially reasonable and risk-based administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of Customer Data ("**TOMs**"). The following provides high-level summary of those safeguards. This Annex B is not intended to be an exhaustive list, as Sturdy continually improves its security position in response to changes in business and emerging threats.

- **Change Management**: Sturdy maintains logs that document all changes to the information technology operating environment, such as the addition of a server, modifying of code/configurations, or any and all changes affecting production equipment.

- **Encryption**: Sturdy encrypts all Customer Data, both at rest and in transit. All Sturdy backups utilize full Advanced Encryption System ("AES").

- **Information Security Program**: Sturdy maintains a comprehensive written information security program including administrative, technical, and physical safeguards to protect Customer Data.

- **Multi-Factor Authentication**: Sturdy enforces multi-factor authentication for all users with administrative privileges or elevated accounts.

- **Password Management**: All Sturdy users are required to use strong passwords with multi-factor authentication in place. In addition, all passwords for administrative accounts are maintained in a key vault with multi-factor authentication in place.

- **Patch Management**: Sturdy maintains and pushes critical security updates for all equipment immediately upon vendor release.

- **Physical Safeguards**: All Sturdy locations and data centers employ a full-time security guard, and maintains an access control system with clearance badges. In addition, Sturdy has established security areas with restriction of access paths.

- **Risk Assessment & Penetration Testing**: Sturdy performs annual information security risk assessments with penetration testing, as well as annual phishing awareness training.

- **Scanning**: Sturdy performs vulnerability scans of all devices connected to its network by executing real-time anti-virus scans and malware scans, as well as full-time use of intrusion detection and penetration systems. Sturdy also scans all emails for potentially malicious content and provides Sturdy users the ability to report and quarantine as desired.

- **Training & Awareness**: Sturdy mandates its employees complete annual security and incident response training and maintains an ongoing awareness progress to keep employees apprised of new requirements and threats.

- **Sturdy Policies**: Sturdy will act in accordance with its existing policies and procedures governing the handling of Personal Data including, but not limited to, Sturdy's Privacy Policy (as amended from time to time) which shall be incorporated into these TOMs by reference.

ANNEX C TO DATA PROCESSING AGREEMENT

SUB-PROCESSOR LIST

As set forth in Article 6 of the DPA, Customer agrees to Sturdy engaging any Sub-processor listed below.

Due to the nature of our business, Sturdy may add, replace or remove Sub-processors. You may subscribe to notifications by emailing privacy@sturdy.ai. If you elect to be notified, we will notify you at least 30 days prior to making a change.

Sub-processor Names and Addresses	**Location(s) of Processing**	**More Information**	**Applicable Service**
Amazon Web Services, Inc. Address: 410 Terry Avenue North Seattle WA 98109	United States	https://aws.amazon.com	Cloud Hosting, authentication, authorization and cognitive services.
Microsoft, Inc. Address: One Microsoft Way Redmond, WA 98052-6399	United States	https://www.microsoft.com	Cloud hosting and cognitive services.
OpenAI, Inc. Address: 1455 3rd Street San Francisco, CA 94158	United States	https://openai.com	AI Cognitive Services

ANNEX D TO DATA PROCESSING AGREEMENT

APPROPRIATE SAFEGUARDS

The Parties agree that the processing of Personal Data under or in connection with the DPA shall be in accordance with the applicable Appropriate Safeguards listed below ("**Appropriate Safeguards List**").

1. Definitions

1.1. "**Standard Contractual Clauses**" or "**SCCs**" means: (a) as to data subjects of the European Economic Area ("**EEA**") and Switzerland, the clauses included in Commission Decision 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 and any replacement, amendment or restatement of the foregoing issued by the European Commission ("**EU SCCs**") attached hereto as Schedule 1; and (b) as to data subjects of the United Kingdom, the clauses included in Commission Decision 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 and any replacement, amendment or restatement of the foregoing issued by the European Commission together with the International Data Transfer Addendum ("**Addendum**") to the EU Commission Standard Contractual Clauses issued by the UK's Information Commissioner's Office ("**ICO**") attached hereto as Schedule 2.

2. International Personal Data Transfers – Where a Customer, acting as a data exporter, transfers Personal Data to Sturdy, acting as a data importer, the Parties hereby agree to abide by the Appropriate Safeguards List, as follows:

2.1. Transfers from the ("EEA") and Switzerland: Schedule 1 shall apply to the transfer of any Personal Data by Customer (acting as a data exporter) located in the EEA to Sturdy or Sturdy Affiliate or Sub-processor (acting as a data importer) located outside the EEA or Switzerland. The Parties agree the EU SCCs shall also govern transfers of Personal Data to and from Switzerland and the term "Member State" referenced in the EU SCCs shall include Switzerland.

2.2. Transfers from the United Kingdom: Schedule 2 shall apply to the transfer of any Personal Data by Customer (acting as a data exporter) located in the United Kingdom to Sturdy or Sturdy Affiliate or Sub-processor (acting as a data importer) located outside the United Kingdom.

2.3. **Other Applicable Jurisdictions:** Where Customer is located in another jurisdiction not explicitly referenced or covered in the DPA or this Appropriate Safeguards List that require the transfer of Personal Data outside the borders of the country where the data was collected, the Party responsible for collecting the Personal Data will ensure the data subject has (i) received notice that their Personal Data will be transferred abroad and (ii) consented to such transfer of their Personal Data in accordance with applicable Data Protection Laws.

SCHEDULE 1

FOR DATA SUBJECTS OF THE EEA AND SWITZERLAND

STANDARD CONTRACTUAL CLAUSES (MODULES TWO AND THREE)

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

The entity identified as "Customer" in the DPA and Services Agreement and any Customer Affiliate (the data **exporter**)

And

The entity identified as "Sturdy" in the DPA and any Sturdy Affiliate or authorized Sub-processor (as defined in the DPA) for whom Sturdy is authorized as an agent to enter these Standard Contractual Clauses

(the data **importer**)

each a 'party'; together 'the parties',

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

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these

Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
ii. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
v. Clause 13;
vi. Clause 15.1(c), (d) and (e);
vii. Clause 16(e);
viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for

in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 –Optional

Docking Clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and

organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures

to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of Sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the

data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of subprocessors at least [Specify time period] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data Subject Rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the

instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to: (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13; (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards12;
iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). For Module Three: The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation for Module Three: , if appropriate in consultation with the controller. The data exporter

shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or the data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in the case of access by public authorities

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. For Module Three: The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). For Module Three: The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. For Module Three: The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
ii. the data importer is in substantial or persistent breach of these Clauses; or
iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing Law

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State in which the data exporter is established.

Clause 18

Choice of Forum and jurisdiction

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of EU Member State in which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

Data exporter(s): The data exporter is the entity identified as "Customer" in the Services Agreement and the DPA and any Customer Affiliate.

Data importer(s): The data importer is the entity identified as "Sturdy" in the DPA or a Sturdy Affiliate or authorized Sub-processor (as defined in the DPA) for whom Sturdy is authorized as an agent to enter these Standard Contractual Clauses.

Signatures: The Parties agree that by signing the Services Agreement to which the DPA and these Standard Contractual Clauses are incorporated by reference, such act will constitute a signature of these Standard Contractual Clauses to the extent applicable under the DPA and permitted by Applicable Law.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred.

- The personal data transferred concern the categories of data subject set forth in Annex A of the DPA under the header "Categories of Data Subjects to Whom Personal Data Relates."

Categories of personal data transferred.

- The personal data transferred concern the categories of data set forth in Annex A of the DPA under the header "Types Personal Data."

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.

- The personal data transferred concern the sensitive data set forth in Annex A of the DPA under the header "Sensitive Data."

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

- The frequency of the transfer shall be on a continuous basis as necessary to perform the obligations of the Services Agreement (as defined in the DPA).

Nature of the processing

- The personal data transferred will be subject to the following basic processing activities (please specify): The processing operations are defined in Annex A of the DPA under the heading "Processing Operations."

Purpose(s) of the data transfer and further processing

- The personal data transferred will be subject to the following basic processing activities (please specify): The processing operations are defined in Annex A of the DPA under the heading "Purpose(s) of Processing."

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

- The Personal Data will be retained solely for as long as necessary to complete any processing necessary to provide the Services under the applicable Services Agreement (as defined in the DPA).

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

- As set forth in Article 7 of the Agreement and including, without limitation, Annex C to the DPA.

……..

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

- England, as to data subjects of the United Kingdom (UK) and UK GDPR, and the EU Member State where the data exporter is established, as to data subjects of the European Economic Area (EEA), Switzerland and GDPR.

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

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.
Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.
[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
Measures for user identification and authorisation
Measures for the protection of data during transmission
Measures for the protection of data during storage
Measures for ensuring physical security of locations at which personal data are processed
Measures for ensuring events logging
Measures for ensuring system configuration, including default configuration
Measures for internal IT and IT security governance and management Measures for certification/assurance of processes and products
Measures for ensuring data minimisation
Measures for ensuring data quality
Measures for ensuring limited data retention
Measures for ensuring accountability
Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

- As set forth in Article 10 of the DPA and including, without limitation, Annex B to the DPA.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

- As set forth in Article 7 of the DPA and including, without limitation, Annex C to the DPA.

SCHEDULE 2

FOR DATA SUBJECTS OF THE UK

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The start of this Addendum is hereby, effective upon the commencement of any transfer of Personal Data to countries outside the United Kingdom.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: The entity identified as "Customer" in the DPA and the Services Agreement. Trading name (if different): As set forth in the Services Agreement , if applicable. Main address (if a company registered address): As set forth in the Services Agreement. Official registration number (if any) (company number or similar identifier): As set forth in the Services Agreement.	Full legal name: The entity identified as "Sturdy" in the DPA and any Sturdy Affiliate or authorized third party for whom Sturdy is authorized as an agent to enter this Addendum. Trading name (if different): N/A. Main address (if a company registered address): 1775 W State St #195, Boise, ID 83702 Official registration number (if any) (company number or similar identifier): N/A.
Key Contact	Full Name (optional): N/A. Job Title: Contact details for the data exporter are specified in the Services Agreement. Contact details including email: Contact details for the data exporter	Full Name (optional): N/A. Job Title: Contact details for the data importer are specified in the Services Agreement. Contact details including email: Contact details for the data importer

	are specified in the Services Agreement.	are specified in the Services Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

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	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	☒	☒	☐ Option Not Exercised	General Authorisation	At least 30 days in advance	
3	☒	☒	☐ Option Not Exercised	General Authorisation	At least 30 days in advance	
4						

Table 3: Appendix Information

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

Annex 1A: List of Parties: Data exporter(s): The data exporter is the entity identified as "Customer" in the Services Agreement and DPA, and each Customer Affiliate.

Data importer(s): The data importer is the entity identified as “Sturdy” in the DPA, or a Sturdy Affiliate or authorized Sub-processor (as defined in the DPA) for whom Sturdy is authorized as an agent to enter the SCCs and this Addendum.
Annex 1B: Description of Transfer: As set forth in Annex A to the DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Article 10 of the DPA and including, without limitation, Annex B to the DPA.
Annex III: List of Sub processors (Modules 2 and 3 only): As set forth in Article 7 of the DPA and including, without limitation, Annex C to the DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.