IRONSCALES – DATA PROCESSING ADDENDUM

Updated: January 1, 2025

This Data Processing Addendum ("**DPA**") forms an integral part of the End User License Agreement ("**Agreement**") between Customer and Ironscales. Customer and Ironscales may also be referred to herein each as a "**Party**" and collectively as the "**Parties**".

Customer shall qualify as the "Data Controller" and Ironscales shall qualify as the "Data Processor", as these terms are defined in Section 1 below. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions

a. "**Data Controller**" (which includes "business" as defined in CCPA), "**Data Processor**" (which includes "service provider" and "contractor" as defined in CCPA), "**Personal Data**" (or "personal data", both of which include similar terms in Data Protection Law, such as "personal information"), "**Personal Data Breach**", "**data subject**" (which includes other terms in Data Protection Law intended to refer to the individual person whose Personal Data are being processed), "**process**", "**processing**" shall have the meanings ascribed to them in the Data Protection Law.

b. **"EEA**" means those countries that are members of the European Economic Area.

c. "**Data Protection Law**" means, individually or collectively, the data protection and privacy laws and regulations that are in force and applicable to a Party's processing of Personal Data pursuant or in relation to the Agreement, including, where applicable, GDPR, EU/UK Data Protection Law, and CCPA; **"GDPR"** means Regulation 2016/679 of the European Parliament and of the Council 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), and any applicable laws of the European Union, their Member States, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement; **"CCPA"** means the California Consumer Privacy Act of 2018, the California Privacy Rights Act of 2020 and any binding regulations promulgated thereunder, in each case, as may be amended from time to time.

d. "**Services**" mean the Platform and any other ancillary services and products provided by Ironscales to Customer pursuant to an Order.

e. "**Security Measures**" mean commercially reasonable security-related policies, standards, and practices commensurate with the nature, size and complexity of Ironscales' business and the level of sensitivity of the data collected, handled and stored, including those set forth in Exhibit B of this DPA.

f. **"Standard Contractual Clauses"** and **"SCCs"** mean, as applicable to the processing, (i) the 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 from June 4th 2021, currently found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en ("**EU SCCs**") and (ii) the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf ("**UK Addendum**").

g. "**Sub-Processors**" and "**Subprocessors**" mean any affiliate, agent or assignee of Ironscales that may process Personal Data pursuant to the terms of the Agreement, and any unaffiliated processor engaged by Ironscales.

2. Compliance with Laws

a. Each Party shall comply with its respective obligations under the Data Protection Law. Without limiting the preceding sentence, Customer represents and warrants that it has obtained from Data Subjects and will maintain throughout the term of the Agreement all consents and permissions required by Data Protection Law for Ironscales' processing of such Data Subjects' Personal Data in accordance with the Agreement.
b. Ironscales shall provide reasonable cooperation and assistance to Customer in relation to Ironscales' processing of Personal Data in order to allow Customer to comply with its obligations as a Data Controller under the Data Protection Law.
c. Ironscales agrees to notify Customer promptly if it becomes unable to comply with the terms of this DPA and take reasonable and appropriate measures to remedy such non-compliance.

3. Processing Purpose and Instructions

a. The subject-matter of the processing, duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects, shall be as set out in **Exhibit A** to **Appendix 1** of this DPA.
b. The duration of the processing under the Agreement is determined by the Parties, as set forth in the Agreement.
c. Ironscales shall process Personal Data only to deliver the Services in accordance with Customer's written instructions (including Customer's Platform settings), the Agreement, the Documentation and the Data Protection Law, unless Ironscales is otherwise required by law to which Ironscales is subject (and in such a case, Ironscales shall inform Customer of that legal requirement before processing, unless that legal requirement prohibits such information disclosure).
d. Processing any Personal Data outside the scope of the Agreement will require prior written agreement between Ironscales and Customer by way of written amendment to the Agreement which may include additional fees that may be payable by Customer to Ironscales for carrying out such instructions.
e. The obligations in this Section 3e apply with respect to Personal Data that is subject to CCPA. To the extent that there is disclosure of Personal Data by Customer to Ironscales, including via the Services, the Parties agree that: (1) the Personal Data is provided by Customer only for the limited and specified purposes set out in the Agreement; (2) Ironscales shall comply with applicable obligations under CCPA and provide the same level of privacy protection as is required of Customer by CCPA; (3) Customer has the right to take reasonable and appropriate steps to help ensure that Ironscales uses the Personal Data in a manner consistent with Customer's obligations under CCPA; (4) Ironscales shall notify Customer if it makes a determination that it can no longer meet its obligations under CCPA; and (5) Customer has the right, upon written notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of the Personal Data by Ironscales. Customer shall inform Ironscales of any consumer (as defined in CCPA) request requiring Ironscales to stop or modify its processing of that consumer's Personal Data in connection with the Agreement. Upon notice of such a request, Ironscales shall promptly cease or modify its processing in accordance with CCPA's requirements. Where Ironscales is a service provider under CCPA, Ironscales agrees and certifies that it will not: (i) sell or share the Personal Data; (ii) retain, use, or disclose the Personal Data for any purpose, including a commercial purpose, other than the business purpose of performing the Services as set forth in the Agreement or as otherwise permitted by CCPA and the Agreement; (iii) retain, use, or disclose the Personal Data outside of the direct business relationship between Customer and Ironscales; or (v) combine the Personal Data with Personal Data that Ironscales receives from or on behalf of another person, or collects from its own interaction with consumers, provided that Ironscales may combine Personal Data to perform any business purpose permitted by the CCPA and the Agreement.

4. Reasonable Security and Safeguards

a. Ironscales shall maintain the Security Measures for the protection of the security, confidentiality and integrity of the Personal Data, and shall demonstrate compliance with such Security Measures upon Customer's written request within a reasonable time period and reasonable means. Upon Customer's request, Ironscales will assist Customer in ensuring compliance with the obligations pursuant to the information security requirements of Data Protection Law, taking into account the nature of the processing and the information available to Ironscales.
b. The Security Measures are subject to technical progress and development and Ironscales may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of Ironscales' platform.
c. Ironscales shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who have access to and process Personal Data. Ironscales shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Cooperation and Assistance

a. If Ironscales receives any requests from data subjects or applicable data protection authorities relating to the processing of Personal Data hereunder, including requests from individuals seeking to exercise their rights under Data Protection Law, Ironscales will promptly redirect the request to Customer unless required to do otherwise by Data Protection Law. Ironscales will not respond to such communication directly without Customer's prior written approval, unless legally compelled to do so. If Ironscales is required to respond to such a request, Ironscales will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so.
b. If Ironscales receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, Ironscales shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. Notwithstanding the foregoing, Ironscales will, to the extent permitted by applicable law, (i) cooperate with Customer with respect to any action taken pursuant to such order, demand or request, and (ii) ensure that confidential treatment will be accorded to such disclosed Personal Data.
c. Upon reasonable notice, Ironscales shall provide reasonable assistance to Customer in:
    i. allowing data subjects to exercise their rights under the Data Protection Law;
    ii. ensuring compliance with any notification obligations of Personal Data Breaches to the supervisory authority, as required under Data Protection Law;
    iii. Ensuring compliance with its obligation to carry out Data Protection Impact Assessments ("**DPIA**") or prior consultations with data protection authorities with respect to the processing of Personal Data. Any assistance to Customer with regard to DPIA or prior consultations will be solely at Customer's cost and expense.

6. Use of Sub-Processors

a. Customer provides a general authorization to Ironscales to appoint (and permit each Sub-Processor appointed in accordance with this section to appoint) Sub Processors in accordance with this section.
b. Ironscales may continue to use those Sub Processors already engaged by Ironscales as at the date of this Agreement, subject to Ironscales in each case as soon as practicable meeting the obligations set out in this section. A list of Ironscales' current Sub Processors can be viewed at List of Sub-Processors.

c. Ironscales may appoint new Sub-Processors provided that Ironscales provides seven (7) days' prior notice (email and Platform notices sufficing) and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable grounds relating to the appointment of the Sub-Processor, specifically any non-compliance with Data Protection Law. In the event of such objections, Ironscales shall either refrain from using such Sub-Processor in the context of the processing of Personal Data or shall notify Customer of its intention to continue to use the Sub-Processor. Where Ironscales notifies Customer of its intention to continue to use the Sub-Processor in these circumstances, Customer may, by providing written notice to Ironscales, terminate the Agreement immediately.
d. With respect to each Sub-Processor, Ironscales shall ensure that the engagement between Ironscales and the Sub Processor is governed by a written contract including terms which offer at least the same level of protection as those set out in this DPA and meet the requirements of Data Protection Law pertaining to Ironscales use of Sub-Processors.
e. Ironscales will be responsible for any acts, errors or omissions by its Sub-Processors which cause Ironscales to breach any of its obligations under this Addendum. Where the preceding sentence is inconsistent with or would cause a violation of the terms of any Data Protection Law, it shall be interpreted to be modified to the minimum extent necessary to avoid such inconsistency or violation.

7. Personal Data Breach

a. Within any notification period prescribed by applicable law (but in any case within two (2) business days of becoming aware of a Personal Data Breach), Ironscales will notify Customer of the Personal Data Breach and will provide relevant information relating to the Personal Data Breach as reasonably requested by Customer.
b. Ironscales shall make reasonable efforts to identify the cause of such Personal Data Breach and take those steps as Ironscales deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach. Furthermore, Ironscales will cooperate and assist the Customer in mitigating, where possible, the adverse effects of any Personal Data Breach.

8. Security Assessments and Audits

a. Subject to Section 8b, Ironscales shall, no more than once a year, upon Customer's written request and subject to obligations of confidentiality, allow its data processing procedures and documentation to be inspected by Customer (or its designee) during regular business hours in order to ascertain compliance with this DPA; and (ii) Ironscales shall cooperate in good faith with audit requests by providing access to relevant knowledgeable personnel and documentation. Notwithstanding anything to the contrary, nothing in this DPA will require Ironscales either to disclose to Customer (and/or its authorized auditors), or provide access to: (i) any data of any other customer of Ironscales; (ii) Ironscales' internal accounting or financial information; (iii) any trade secret of Ironscales; or (iv) any information that, in Ironscales' sole reasonable discretion, could compromise the security of any of Ironscales' or its customers' or suppliers' information, systems or premises or cause Ironscales to breach obligations under any applicable law or its obligations to any third party.
b. Where sufficient to satisfy the purpose of a Customer request under Section 8a, Ironscales may satisfy the requirements set out in this section by providing Customer with a copy of a written report so that Customer can reasonably verify Ironscales' compliance with its obligations under this DPA.

9. International Data Transfers

a. Ironscales may transfer and process Personal Data of Data Subjects ("**Transfer**") anywhere in the world where Ironscales, its Affiliates, or their respective Sub-Processors maintain data processing operations, subject to the following: (i) the Transfer is for the purpose of Ironscales carrying out its obligations under the Agreement, or is required under applicable laws; and (ii) the Transfer is done in accordance with this Section 9 and Data Protection Law.

b. Neither Party shall transfer or permit to be transferred any Personal Data that is (i) subject to GDPR, EU/UK Data Protection Law, or other Data Protection Law that imposes requirements on the international transfer of Personal Data governed by such law; and (ii) provided by or on behalf of the other Party to a territory outside of the European Economic Area (EEA), the UK, or other applicable jurisdiction unless it has taken such measures as are necessary to ensure the transfer complies with EU Data Protection Law or other appliable Data Protection Law. Such measures may include transferring the Personal Data to a recipient in a country that the European Commission or UK has decided provides adequate protection for Personal Data, or to a recipient in the United States that has certified compliance with, as applicable to the Personal Data being transferred, the EU-U.S. Data Privacy Framework ("**DPF**), UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF, or transfer frameworks promulgated by other applicable Data Protection Law (collectively, "**Transfer Frameworks**"), or to a recipient with whom the Party has established appropriate alternative transfer mechanisms such as entering into Standard Contractual Clauses deemed adequate under EU/UK Data Protection Law.

c. With respect to EU/UK Data Protection Law, currently (and subject to change as described in Section 9.a), Ironscales transfers Personal Data to and processes Personal Data in the following countries outside of the European Economic Area and the UK pursuant to the following transfer mechanisms:

<table>
<tr><th>Ironscales Entity</th><th>Import Countries</th><th>Statutory Mechanism for Transfers by Import Country</th></tr>
<tr><td>Ironscales, Inc. (US Delaware corporation)</td><td>United States of America
State of Israel
United Kingdom</td><td rowspan="3">US: Ironscales adherence to the Transfer Frameworks (see Ironscales' DPF listing at https://www.dataprivacyframework.gov/list)
Israel: EU adequacy decision 2011/61/EU
UK: EU adequacy decision 2021/1772</td></tr>
<tr><td>Ironscales Global Ltd. (UK entity)</td><td>United Kingdom
State of Israel
United States of America</td></tr>
<tr><td>Ironscales Ltd. (Israeli company)</td><td>State of Israel
United States of America
United Kingdom</td></tr>
<tr><td>Sub-Processor Entities</td><td>See List of Sub-Processors</td><td>As stated in data privacy agreements with Sub-Processors</td></tr>
</table>

d. If a Transfer Framework is determined to be inadequate or unlawful for any reason, with the Parties will implement a lawful alternative mechanism that will ensure such Transfers are lawful, including, where EU/UK Data Protection

Law applies, the appropriate Standard Contractual Clauses. Customer will cooperate with Ironscales as necessary to ensure any such lawful alternative Transfer mechanism is implemented in accordance with Data Protection Law. Without limiting the preceding sentence, if the DPF is determined to be inadequate or unlawful for any reason, the Parties shall be deemed to enter into the Standard Contractual Clauses, as supplemented and interpreted in Appendix 1, in which event the Customer shall be deemed to be the Data Exporter and Ironscales shall be deemed to be Data Importer (as these terms are defined therein), and the Parties' signatures to the Agreement shall be deemed sufficient for purposes of accepting their respective obligations under and fulfilling any signature requirements in the Standard Contractual Clauses.

10. Data Retention and Destruction

Upon Customer's written request, Ironscales will delete all Personal Data in its possession as provided in the Agreement except to the extent Ironscales is required (in which case Ironscales will implement reasonable measures to prevent the Personal Data from any further processing that is not required) or permitted (in which case Ironscales will limit its processing to such permitted purposes) under applicable law to retain the Personal Data. The terms of this DPA will continue to apply to such retained Personal Data for as long as it is retained.

11. General

a. Any claims brought under this DPA will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement.
b. In the event of a conflict or inconsistency among the Agreement (and any document referred to therein), this DPA, and, if applicable, the Standard Contractual Clauses, the order of precedence in respect of the Processing of Customer Personal Data shall be: the SCCs, the DPA, and then the Agreement.
c. Any changes to this DPA shall be done upon the mutual written agreement of Customer and Ironscales, provided that neither party shall unreasonably withhold its agreement to such change, if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, and further provided that such change does not: (i) seek to alter the categorization of Ironscales as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party's rights to use or otherwise process Personal Data; or (iii) have a material adverse impact on Customer.
d. Interpretation. In this DPA, its Appendix, and the Exhibits and Annexes to the Appendix, unless the context requires otherwise:
    1. any reference to any statute, regulation, instrument or statutory provision shall be construed as a reference to the same as from time to time replaced, amended, extended, re-enacted, or implemented in local legislation;
    2. any reference to a "person" includes any individual, company, corporation, partnership, limited partnership, limited liability partnership, firm, joint venture, association, organization, trust, state or state agency (in each case whether or not having separate legal personality);
    3. the headings used in this DPA are for convenience only and shall not be used for purposes of construction or interpretation;
    4. references to "Appendices", "Exhibits", "Annexes", "Sections", and "clauses" are, unless otherwise stated, references to the Appendices, Exhibits, Annexes, Sections, and clauses to this DPA, as applicable;
    5. any word following the terms "including", "include", "in particular", "such as", "for example" or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms;

6. if any provision in this DPA is ineffective or void, this shall not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. In case a necessary provision is missing, the parties shall add an appropriate one in good faith; and
7. if applicable, the Appendices and its Exhibits form part of this DPA and will have the same force and effect as if expressly set out in the body of this DPA.

Appendix 1

EU/UK/Swiss to US Data Transfer Clauses

Preamble: This Appendix 1 shall only apply under the conditions specified in Section 9.d of the DPA.

1. Application and Interpretation of the Standard Contractual Clauses

(A) Subject to the Preamble above, for any Transfers of Customer Personal Data from the European Economic Area and its member states, the United Kingdom and/or Switzerland (collectively, "**Restricted Countries**") to Ironscales in a country which does not ensure an adequate level of protection (within the meaning of and to the extent governed by the Data Protection Laws of the Restricted Countries) (collectively, "**Third Country**"), such transfers shall be governed by this Appendix 1. For clarity, for transfers from the United Kingdom and Switzerland, references in the SCCs shall be interpreted to include applicable terminology for those jurisdictions (e.g., "Member State" shall be interpreted to mean "United Kingdom" for transfers from the United Kingdom).

(B) Where the valid Transfer Framework is the Standard Contractual Clauses, Ironscales is entering into the Standard Contractual Clauses with Customer as set out in this Section 1 and in accordance with the applicable terms of this Section 1. The following terms of this Section 1(B) shall apply to all SCCs applicable to the parties.

a. Each Party agrees to transfer and process Customer Personal Data from the Restricted Countries in accordance with the EU SCCs and UK Addendum respectively and as applicable, which are incorporated into this DPA by reference. Each Party is deemed to have executed the applicable SCCs by entering into the DPA, and the details set forth in this Section 1 and Exhibit A, shall apply for the purposes of Table 1 of the UK Addendum.
b. If a Subprocessor is a Data Importer (as that term is used in the applicable SCCs), Ironscales shall enter into the appropriate standard contractual clauses with Customer on behalf of such Data Importer. If that is not possible, Ironscales will inform Customer in writing and will procure such Data Importer's agreement to such standard contractual clauses as an additional Data Importer. Customer or Ironscales will, upon request of a Data Subject, provide the Data Subject with a copy of documentation of such mechanism(s) and this DPA.
c. The Parties agree that the nature of the Processing is such that Customer is the Controller and Ironscales is the Processor; therefore, the applicable clauses of the Standard Contractual Clauses shall be those with general applicability (i.e., those clauses that are not identified as being applicable to any specific module(s)) and the clauses identified in the EU SCCs as "Module TWO: Transfer controller to processor" clauses.
d. If the UK SCCs apply to the processing under this DPA, they shall be interpreted in accordance with the UK Addendum and the applicable details set forth in this Section 1(B). For purposes of Table 2 of the UK Addendum, the versions of the Approved EU SCCs that apply shall be determined by Section 1(B)c above.

(C) The terms in this Section 1(C) apply to the applicable SCCs as described in Sections 1(B) c and d, including (i) the election of specific terms and/or optional clauses as described in more detail in subsections a - i below, and (ii) for purposes of the UK SCCs (except to the extent the UK SCCs modify them).

a. Where the Standard Contractual Clauses identify a clause as an option, the optional clause shall apply (including with respect to Table 2 of the UK Addendum) unless otherwise expressly agreed by Customer and Ironscales in this Data Protection Agreement or its Exhibits.
b. The optional Clause 7 in Section I of the SCCs is incorporated, and Ironscales' Affiliates may accede to this DPA and the SCCs under the same terms and conditions as Ironscales, subject to any variations made by mutual agreement of Customer and Ironscales. The foregoing shall apply with respect to Table 2 of the UK Addendum;
c. For purposes of Clause 9 of the SCCs, Option 2 ('General written authorization') is selected and the process and time period for the addition or replacement of Subprocessors shall be as described in Section 6 of the DPA. The foregoing shall apply with respect to Table 2 of the UK Addendum;
d. For purposes of Clause 13 of the SCCs, Annex I.C to this Appendix 1 shall apply. Ironscales shall maintain accurate records of the applicable Member State(s) and competent supervisory authority, which shall be made available to Customer on request;
e. For purposes of Clause 14(c) and 15 of the SCCs, Exhibit A, Annex IV (Additional Safeguards for Third Countries) applies for each applicable Third Country in which Customer Personal Data is or may be Processed by Ironscales. Ironscales shall update Exhibit A, Annex IV by notice to Customer whenever a material change to the relevant laws and practices of Third Countries occurs;
f. Except as provided in subpart g below, (i) for purposes of Clause 17, Option 1 shall apply and the Parties agree that the law of the Republic of Ireland shall govern, and (ii) for purposes of Clause 18(b) of the EU SCCs, the Member State for purposes of governing law and jurisdiction shall be the Republic of Ireland.
g. For purposes of the UK Addendum, Part 2, Section 15(m) of the UK Addendum shall apply in lieu of Clause 17 of the EU SCCs, and Part 2, Section 15(n) of the UK Addendum shall apply in lieu Clause 18(b) of the EU SCCs;
h. Exhibit A of this DPA sets forth the information required for completion of the Appendix to the Standard Contractual Clauses; in particular, (List of the Parties), (Description of the Transfer), (Competent Supervisory Authorities), (Technical and Organisational Measures), and (List of Subprocessors). The foregoing shall apply with respect to Table 3 of the UK Addendum; and
i. With respect to Table 4 of the UK Addendum, either party may terminate the UK Addendum pursuant to Section 19 of the UK Addendum if, after a good faith effort by the parties to amend this DPA to account for the approved changes and any reasonable clarifications to the UK Addendum, the parties are unable to come to a mutual agreement.

2. The parties agree that, if authorized to use the Services pursuant to the Agreement, Customer's Affiliates are, within the scope of their use of the Services, intended third-party beneficiaries of the SCCs and its provisions will inure to the benefit of the Customer Affiliates, which will be entitled to enforce the SCCs as if each were a signatory to the DPA.

EXHIBIT A TO THE STANDARD CONTRACTUAL CLAUSES

The information in this Exhibit A contains the relevant information needed to complete Annexes I – III of the Standard Contractual Clauses.

Annex I.A of the SCCs (List of the Parties)

Data exporter: The data exporter is the Customer specified in the Agreement.

Data importer: The data importer is Ironscales as specified in the Agreement.

Annex I.B of the SCCs (Description of Transfer)

Data subjects: Data subjects whose personal data are transferred include the data exporter's representatives and end-users and may include (i) individuals attempting to communicate or transfer Personal Data to users of the Ironscales Services, and (ii) the following types of data subjects:

- Customer's employees and other users and the businesses and individuals with whom they correspond via email or other communications processed by Ironscales' Services;
- Employees, contractors and temporary workers (current, former, prospective) of data exporter or data controller;
- Dependents of the above;
- Data exporter's or data controller's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, visitors, etc.) and other data subjects that are users of data controller's products or services; or
- The data exporter's partners, stakeholders or individuals who communicate or otherwise interact with employees of the data exporter or data controller and use or interact with communication tools provided by the data exporter where the contents of such communications are processed by the Ironscales Services.

Categories of data: The personal data transferred that is included in e-mail, documents and other data in an electronic form in the context of the Services. Ironscales acknowledges that, depending on Customer's use of the Ironscales' Services, Customer may elect to include personal data from any of the following categories in the personal data:

- First name
- Last name
- Address
- Phone number
- Email address
- Authentication data (for example, user name, password, security questions and authentication codes, audit trail);
- Social media identifiers;
- Unique identification numbers and signatures (for example, employee number, student number, patient number, signature, unique identifiers in non-essential cookies or similar technologies);

- Pseudonymous identifiers;
- Location data (for example, mobile ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Email content and correspondence, including:
    - Headers
    - Links
    - Attachments
    - Photos
    - Videos
    - Audio and other files
    - Metadata
    - IP addresses
    - Payment information
    - Business information;

  or
- Any other personal data identified in Article 4 of GDPR or special categories of personal data (aka sensitive data) identified in Article 9 of GDPR that Customer provides to Ironscales for processing by the Services.

Sensitive data transferred: Any special categories of data provided by Customer in the course of its usage of the Services, in particular such special categories of data as may be included in the contents of email communications processed by the Services. With respect to such sensitive data, data importer shall take the safeguards specified in its technical and organisational measures set forth in the DPA.

Processing operations: The personal data transferred will be subject to the following processing activities, which apply to Ironscales' Subprocessors unless stated otherwise:

a. Duration and Frequency of Personal Data Processing. The duration of the personal data processing shall be for the term designated under the Agreement and the DPA. The frequency of the personal data processing is continuous during the term of the Agreement.

b. Nature and Purpose of the Personal Data Processing. The scope, nature and purpose of the data importer's processing of personal data are described in the Agreement and this DPA.

e. Customer Personal Data Retention, Deletion or Return. Upon expiration or termination of the Agreement or this DPA, data importer shall provide all Customer data including personal data to Customer in a format reasonably acceptable to Customer and data importer will delete Customer data including personal data, each in accordance with the terms of the Agreement and the DPA.

Subprocessors: For purposes of Annex IB of the SCCs and solely in accordance with the Clause 9 of the SCCs, the data importer may use the Subprocessors identified in the DPA to provide services that process personal data on data importer's behalf.

Annex I.C of the SCCs

Competent supervisory authority: the supervisory authority that shall act as competent supervisory authority shall be determined in accordance with the terms of Clause 13(a) of the Clauses, taking account of the facts and circumstances of the data exporter's establishment and the data exporter's appointment of a representative, if any, pursuant to Article 27(1) of Regulation (EU) 2016/679.

Annex II to the Standard Contractual Clauses (Technical and Organisational Measures)

Description of the technical and organizational security measures implemented by the data importer, including for purposes of Annex II of the SCCs (Technical and Organisational Measures of the data importer):

1. **Personnel**. Data importer's personnel will not process Customer personal data without authorization. Personnel are obligated to maintain the confidentiality of any such Customer personal data and this obligation continues even after their engagement ends.

2. **Technical and Organization Measures.** The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer data and personal data in accordance with the requirements of the DPA, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth Exhibit B of the DPA.

Annex III to the Standard Contractual Clauses (Subprocessors)

Ironscales is authorized to engage Subprocessors in accordance with the Agreement and the DPA. Where required for purposes of Annex III of the SCCs (List of Subprocessors), the list of Subprocessors is set forth in Section 6 of the DPA, as updated from time to time.

Annex IV to the Standard Contractual Clauses (Additional Safeguards)

By the terms of this Annex IV, Ironscales provides additional safeguards to Customer and additional redress to the data subjects to whose personal data processed by Customer and Ironscales relates.

This Annex supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses.

1. **Challenges to Orders**. In the event Ironscales receives an order from any third party for compelled disclosure of any personal data that has been transferred under the Standard Contractual Clauses, Ironscales shall:

a. use reasonable efforts to redirect the third party's request, order or demand directly to Customer;

b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and

c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable Member State law.

For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2. **Indemnification of Data Subjects**. Subject to Sections 3 and 4, Ironscales shall indemnify a data subject for any material or non-material damage to the data subject caused by Ironscales' disclosure of personal data of the data subject that has been transferred under the Standard Contractual Clauses in response to an order from a non-EU/EEA government body or law enforcement agency (a "Relevant Disclosure"). Notwithstanding the foregoing, Ironscales shall have no obligation to indemnify the data subject under this Section 2 to the extent the data subject has already received compensation for the same damage, whether from Ironscales or otherwise.

3. **Conditions of Indemnification**. Indemnification under Section 2 is conditional upon the data subject establishing, to Ironscales' reasonable satisfaction, that:

a. Ironscales engaged in a Relevant Disclosure;

b. the Relevant Disclosure was the basis of an official proceeding by the non-EU/EEA government body or law enforcement agency against the data subject; and

c. the Relevant Disclosure directly caused the data subject to suffer material or non-material damage.

The data subject bears the burden of proof with respect to conditions a. though c.

Notwithstanding the foregoing, Ironscales shall have no obligation to indemnify the data subject under Section 2 if Ironscales establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

4. **Scope of Damages**. Indemnification under Section 2 is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Ironscales' violation of the GDPR.

5. **Exercise of Rights**. Rights granted to data subjects under this Annex may be enforced by the data subject against Ironscales irrespective of any restriction in the Standard Contractual Clauses. The data subject may only bring a claim under this Annex on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Annex are personal to the data subject and may not be assigned.

6. **Notice of Change**. In addition to the Standard Contractual Clauses, Ironscales agrees and warrants that it has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the data exporter and its obligations under this Appendix or the Standard Contractual Clauses and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Appendix or the Standard Contractual Clauses, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of personal data and/or terminate the contract.

7. **Termination**. This Annex shall automatically terminate if the European Commission, a competent Member State supervisory authority, or an EU or competent Member State court approves a different lawful transfer mechanism that would be applicable to the data transfers covered by the Standard Contractual Clauses (and if such mechanism applies

only to some of the data transfers, this Annex will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Annex.

EXHIBIT B TO THE STANDARD CONTRACTUAL CLAUSES

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

During the term of the processing of Customer personal data, Ironscales will employ the following technical and organizational measures for the processing and security of Customer personal data:

1. Implement appropriate environmental and physical security measures to prevent unauthorized access to restricted information and the systems managing it.
2. Manage and restrict access to only the resources necessary for users (application, database, network, and system administrators) to perform authorized functions. Ironscales should document all the user types and their related permissions.
3. Require multi-factor authentication and encryption that meet security standards for any remote access to Confidential Information and Customer's network.
4. Use a secure method for securing authentication information (Username and password) by acceptable security standards. Below are the some of the key parameters for Password Requirements:
    - Passwords must be at least eight characters in length. Longer is better.
    - User shall change password at least in every 180 days.
    - New passwords cannot be the same as the previous four passwords.
    - Passwords must contain both uppercase and lowercase characters (e.g., a-z and A-Z).
    - Passwords must contain at least one number (e.g., 0-9).
    - Users shall not use easy to guess passwords such as company name, names of pets, spouse, favorites, vendor supplied default passwords, etc.
5. Separate virtually Customer's information from any other customer or Subprocessor's own applications and information, including but not limited to the public internet or any system used by Subprocessor. Information shall be protected using appropriate tools and measures, including but not limited to access control, firewall, anti-virus applications.
6. Not transfer and store Customer's information on removable devices, laptops, smartphones, tablets, etc., unless agreed upon in advance with Customer in writing. Ironscales shall implement security measures such as using strong encryption (AES-256 and above) to protect all of Customer's information stored on mobile devices.
7. Regularly install the most recent system and security updates to systems that used to access, process, manage, or store Customer's information.
8. Employ appropriate measures of identification and access controls to any of the Ironscales's systems and Customer's information. Ironscales should save log files of all access to Customer's information and shall be provided to Customer upon request.
9. Use only the mutually agreed upon facilities and connection methodologies to remotely connect to Customer's network. Any connection to Customer's information sources using a remote connection is conditioned on prior approval.
10. Transfer of Confidential Information between Customer and the Ironscales will be implemented by using secure file transfer platform.
11. Be responsible to architecture reviews, conduct penetration tests and/or code review to the Ironscales's systems at least once a year, or more than once, if there is any change in its systems. The penetration tests shall be conducted by a third party. Customer shall be entitled to receive the reports of such penetration tests upon its demand.

12. Without limiting the preceding measures, Ironscales is SOC 2 Type II certified. Customer shall be entitled to receive the SOC 2 Type II report upon written request