IRONSCALES

End User License Agreement

THIS END USER LICENSE AGREEMENT ("**AGREEMENT**") CONSTITUTES A BINDING CONTRACT BETWEEN IRONSCALES INC. IRONSCALES LTD., AND THEIR AFFILIATES AND SUBSIDIARIES (COLLECTIVELY, "**IRONSCALES**"), AND THE AUTHORIZED USER (AS DEFINED BELOW) AND/OR THE LEGAL ENTITY IDENTIFIED IN THE ORDER (COLLECTIVELY, "**CUSTOMER**").

TAKING ANY STEP TO SET-UP, CONFIGURE AND/OR INSTALL THE PLATFORM SHALL CONSTITUTE CUSTOMER'S ACCEPTANCE OF THE TERMS OF THIS AGREEMENT. IF CUSTOMER DOES NOT AGREE WITH ALL THE TERMS OF THIS AGREEMENT, IT AND ANYONE ON ITS BEHALF MUST CEASE ALL USE OF THE PLATFORM.

1. **DEFINITIONS**

1.1 "**Affiliate**" means all entities which are controlling, controlled by or under common control with a party. For purposes of this Agreement, "control" means possessing, directly or indirectly, the power to direct or cause the direction of the management, policies or operations of an entity, whether through ownership or voting securities, by contact or otherwise.

1.2 "**Authorized Users**" means the user(s) who have been granted access to manage and administer the Platform on behalf of Customer.

1.3 "**Customer Data**" means any data made available to Ironscales by Customer through or in connection the use of Platform and this Agreement, including but not limited to content of emails, attachments and other links provided via Customer's email servers and other communication platforms, which are processed by the Platform.

1.4 "**Documentation**" means the standard documentation and user manuals of the Platform, as made available to Customer from time to time.

1.5 **"Order**" means the order issued for Customer's use of the Platform, and any other ancillary services and products provided by Ironscales.

1.6 "**Partner**" means a reseller or distributor authorized by Ironscales to market, distribute, sell, operate, and/or support the Platform.

1.7 **"Platform**" means Ironscales' messaging security platform and anti-phishing solution, as further detailed and licensed under the applicable Order (or Partner Order).

1.8 "**Platform Analyses**" means aggregated data related to Customer and its Authorized Users use of the Platform.

2. **LICENSE GRANT, RESTRICTIONS, AND PROHIBITIONS**

2.1 **License Grant.** Subject to the terms of this Agreement, Ironscales hereby grants to Customer a worldwide, royalty-free, non-exclusive, time-limited, non-transferrable (except as provided in Section 12.2), non-sub licensable license for its Authorized Users to access and use the Platform during the Term (as defined herein), solely for Customer's internal business purposes and in accordance with the Documentation.

2.2 **License Restrictions.** Except as explicitly approved in this Agreement or an applicable Order, Customer shall not, and shall not permit any third party to: (1) resell, sublicense, lease, time-share or otherwise make the

Platform available to a third-party; (2) attempt to gain unauthorized access to the Platform or disrupt the performance of the Platform; (3) modify, copy or make derivative works based on the Platform (including any data provided and/or included therein which is not Customer Data); (4) decompile, disassemble, reverse engineer or otherwise attempt to derive the source code or underlying algorithms of the Platform; (5) remove or alter any trademarks or other proprietary notices related to the Data Platform; (6) use the Platform in a manner that violates or infringes any rights of any third party, including but not limited to, privacy rights, publicity rights or intellectual property rights; or (7) access the Platform to build a competitive product, platform or service or copying its features or user interface, as well as product benchmarking or other comparative analysis for any external use.

2.3 **Fraudulent Use of the Platform**. Without prejudice to any other right Ironscales has under this Agreement or under applicable law, Ironscales may employ technological measures to detect and prevent fraudulent or unauthorized use of the Platform or parts thereof. Ironscales may suspend Customer's use of the Platform, if Ironscales, at its sole but reasonable discretion, has deemed Customer's use of the Platform (or any Authorized User on its behalf) to be fraudulent or outside the scope of the license granted herein.

2.4 **Purchase of License from Partner**. If Customer has purchased the right to use the Platform granted hereunder from a Partner, then, to the extent there is any conflict between this Agreement and the agreement entered between Customer and the respective Partner, including any purchase order ("**Partner Sales Order**"), then, as between Customer and Ironscales, this Agreement shall prevail. Any rights granted to Customer in such Partner Order Form which are not provided in this Agreement, shall not obligate Ironscales and Customer must seek redress or realization or enforcement of such rights solely with such Partner and not from Ironscales.

3. USE OF PERSONAL DATA

3.1 **DPA**. Ironscales' processing of personal data included in the Customer Data shall be subject to the data processing addendum attached hereto as **Exhibit A** ("**DPA**"). Ironscales may update the DPA from time to time so long as there is no material degradation to the overall protections set forth therein.

3.2 **Privacy Policy**. Any other use of personal data by Ironscales in connection with the Platform which not specified in the DPA (including the use of the Platform Analyses and Analytic Tools), shall be subject to Ironscales' privacy policy, available at: https://ironscales.com/privacy-policy/, as may be updated from time to time.

4. SUPPORT SERVICES

4.1 **Support Services**. Ironscales will provide support services for the Platform in accordance with the support terms set forth in **Exhibit A** ("**Support Terms**"), which may be updated from time to time, provided that such updates do not materially degrade the Support Terms (when taken as a whole).

5. FEES & PAYMENT TERMS

5.1 **Fees**. All fees shall be as specified in the applicable Order (or Partner Order).

5.2 **Payment**. Unless otherwise specified in the applicable Order (or Partner Order), all payments shall be made in the currency specified in the Order (or Partner Order) within thirty (30) days of the date of invoice. Except as expressly provided herein, all payments made hereunder are non-refundable and non-cancellable and are without any right of set-off or cancellation.

5.3 **Delay in Payment**. Payments of fees after their due date will incur interest at a rate equal to one percent (1%) per month (i.e., 12% per annum) or the highest rate permitted by applicable law, whichever is less. If any amount owing by Customer under this Agreement is thirty (30) or more days overdue, Ironscales may, without limiting its other rights and remedies, suspend its performance under this Agreement.

5.4 **Payment Disputes**. In the event Customer disputes an invoiced amount in good faith, Customer shall notify Ironscales of such dispute, providing any relevant information regarding the circumstances of the dispute within 30 days of date of receipt of invoice and the parties shall work together promptly and in good faith to resolve such dispute and Customer shall pay the amount not disputed in accordance with the applicable payment terms.

5.5 **Taxes.** All amounts payable by Customer hereunder are exclusive of all duties and taxes, including but not limited to sales, use, goods and services, excise or value added taxes and withholding taxes (collectively, "**Taxes**"). Where applicable, Customer shall pay and bear all Taxes associated with this Agreement, excluding taxes based solely on Ironscales' net income. Any withholding amount or deduction imposed on the payment to be made to Ironscales shall be the sole responsibility of Customer and any payments or fees due to Ironscales shall not be decreased in any manner by such withholding amount.

6. PROPRIETARY RIGHTS; THIRD PARTY COMPONENTS

6.1 **Ownership by Customer.** Customer is the sole owner of all intellectual property rights in the Customer Data (excluding any Platform Analysis) and in any report provided to Customer through the Platform based on Customer Data ("**Reports**"). Customer hereby grants Ironscales a non-exclusive right to use the Customer Data and Reports during the Term in order to provide the Platform.

6.2 **Ownership by Ironscales**. As between Customer and Ironscales, Ironscales is the sole owner of all intellectual property rights in and to: (i) all materials provided by Ironscales hereunder, including the Platform and Documentation (but excluding the Reports), (ii) Ironscales' Confidential Information, (iii) Ironscales' names, trademarks, trade names and logos, (iv) Platform Analyses, and (vi) any improvements, derivative works, enhancements, and/or modifications of/to any of the foregoing, as well as any other intellectual property rights conceived, authored, or otherwise developed pursuant to this Agreement, in each case regardless of inventorship or authorship, and Customer acknowledges that it has no rights thereto except as expressly set forth herein.

6.3 **Platform Analyses and Analytic Tools**. Ironscales may compile Platform Analyses in an aggregated form to create statistical analyses for research and development purposes, and make available such Platform Analyses in a form. Furthermore, the Platform may incorporate analytics tools in order to optimize Customer's use and experience of the Platform. To the extent that Customer desires to opt out of the compilation of Ironscales' Platform Analysis, it shall contact Ironscales' customer success team at support@ironscales.com.

6.4 **Feedback**. Nothing in this Agreement or in the parties' dealings related to this Agreement will restrict Ironscales' right to use, disclose, publish, or otherwise exploit Feedback (as defined below), without compensating or crediting Customer or the individual providing such Feedback. No Feedback shall be deemed Customer Confidential Information to the extent that such Feedback relates to Ironscales' Platform and services. "**Feedback**" means any suggestion or idea for improving or modifying the Platform. There are no implied rights and all rights not expressly granted herein are reserved.

6.5 **Third Party Components and Sources.** The Platform uses and/or includes third party software, files, libraries that are based, among others, on third-party sources, as well as components that are subject to third party open source license terms. A list of such sources and components may be provided to Customer upon written request to Ironscales. Accordingly, and without derogating from anything in this Agreement, Ironscales hereby disclaims any and all express and/or implied warranties with respect to any Report and/or recommendation provided in connection with or based on such features and third-party sources.

7. CONFIDENTIAL INFORMATION.

7.1 **Confidential Information**. Each party agrees that "**Confidential Information**" includes, without limitation, all information provided by a party ("**Disclosing Party**") to the other party ("**Receiving Party**") that is either designated as confidential at the time of disclosure or should reasonably be considered, given the nature of the information or the circumstances surrounding its disclosure, to be confidential. For the avoidance of doubt, Ironscales' Confidential Information includes all non-public product features and information regarding pricing of its products and services. The Receiving Party will only use the Disclosing Party's Confidential Information in connection with this Agreement and will not disclose it to any third party, except to the Receiving Party's and its Affiliates' employees, directors, consultants (collectively, "**Representatives**") who have a need to know, and are subject to non-disclosure obligations with terms no less restrictive than those herein. The Receiving Party shall remain liable for any acts or omissions of its Representatives with respect to the Disclosing Party's Confidential Information.

7.2 **Exclusions**. The duties described in Section 7.1 will not apply to any information that: (a) is or becomes publicly available through no fault of the Receiving Party; (b) is rightfully known by the Receiving Party prior to disclosure by the Disclosing Party; (c) is rightfully obtained by the Receiving Party without restriction from a third party not known by the Receiving Party to be subject to restrictions on disclosure; or (d) is disclosed by the Receiving Party with the prior written approval of the Disclosing Party. Notwithstanding the foregoing, the Receiving Party may also disclose Confidential Information if and only to the extent it is required to be disclosed by law or regulatory or court order, so long as, if permitted under applicable law, Receiving Party provides advance notice to the Disclosing Party as promptly as possible and reasonably cooperates with the Disclosing Party's efforts to limit or obtain a protective order or other relief regarding such disclosure at Disclosing Party's expense.

7.3 **Injunctive Relief**. Both parties hereby agree that the Confidential Information to be disclosed hereunder is of a unique and valuable character, that damages to the Disclosing Party that would result from the unauthorized dissemination of the Confidential Information would be impossible to calculate and that such party agrees that the Disclosing Party has no adequate remedy at law. The parties further agree that the Disclosing Party shall be entitled to obtain injunctive relief (without the posting of any bond or other security) preventing the further use and/or disclosure of any Confidential Information in violation of the terms hereof.

7.4 **Return and Destruction**. Upon termination of this Agreement, the Receiving Party will, upon written request, promptly destroy or return the Disclosing Party's Confidential Information and all copies thereof, provided that the Receiving Party shall not be obligated to erase Confidential Information contained in archived computer system backups in accordance with its security and/or disaster recovery procedures, provided further that any such retained Confidential Information shall continue to be protected by the confidentiality obligations of this Agreement.

8. <u>WARRANTIES; DISCLAIMERS</u>

8.1 **Mutual Warranties**. Each party warrants that it: (a) has the legal power to enter into this Agreement and to perform its obligations hereunder; and (b) complies with all applicable laws in its performance hereunder.

8.2 **Customer Warranties**. Customer warrants that it has all legal rights to all Customer Data, including the right to provide Customer Data to Ironscales in accordance with the terms of this Agreement.

8.3 **Warranty Disclaimer**. EXCEPT FOR THE EXPRESS WARRANTIES INCLUDED IN THIS SECTION 8, THE PLATFORM AND REPORTS ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, AND IRONSCALES HEREBY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, ACCURACY, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. WITHOUT LIMITING THE FOREGOING, IRONSCALES SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES THAT ANY OF THE PLATFORM WILL MEET CUSTOMER'S REQUIREMENTS OR FULFILL ANY OF CUSTOMER'S NEEDS. TO THE

EXTENT IRONSCALES MAY NOT, AS A MATTER OF APPLICABLE LAW, DISCLAIM ANY WARRANTY, THE SCOPE AND DURATION OF SUCH WARRANTY SHALL BE THE MINIMUM PERMITTED UNDER SUCH LAW.

8.4 **Additional Disclaimers**. Customer acknowledges that the Platform relies on network, infrastructure, hardware and software, partly managed and operated by others. Ironscales does not warrant that the Platform will operate in an uninterrupted or error-free manner, or that it will always be available, free from errors or omissions, malfunctions, bugs or failures, including hardware failures, software failures and software communication failures. Customer further acknowledges that certain aspects of the are designed for training purposes, and may include developing, customizing, and sending fake cyber security attack campaigns for purposes of employee training, but that Customer, and not Ironscales or its Affiliates, will be responsible for its compliance with all laws and governmental regulations, and any results in connection with Customer's use of the Platform. For the avoidance of doubt, Ironscales will assume no liability whatsoever for damages incurred or sums paid by Customer or anyone on its behalf, in connection with any fault by Customer or any third party's harmful components impacting Customer's computer network (such as computer viruses, worms, computer sabotage, or "denial of service" attacks)

9. **INDEMNIFICATION**

9.1 **Ironscales Indemnity**. Subject to Section 9.2, Ironscales will indemnify and defend Customer and hold Customer harmless against all third party losses finally awarded by a court of competent jurisdiction or pursuant to a settlement agreement signed by Ironscales arising from actions, proceedings, suits, claims or demands that may be brought or instituted against Customer by any third party that Customer's use of the Platform in accordance with the terms of this Agreement infringes such third party's intellectual property rights ("**Infringement Claims**"). Notwithstanding the foregoing, Ironscales shall have no liability or obligation hereunder with respect to any Infringement Claim to the extent arising from or related to (a) any use of the Platform not in accordance with this Agreement (including but not limited to Section 8.4) and the Documentation; (b) modifications, adaptations, alterations, or enhancements of the Platform not created by or for Ironscales; (c) the combination of the Platform with items not supplied by Ironscales or approved for use with the Platform by Ironscales in the Documentation to the extent such claim would not have arisen but for the combination; and/or (d) Customer's continuing use of any version of the Platform after an update, modification or replacement of the Platform is made available to the Customer and Customer fails to implement within a reasonable period of time. If the Platform or any part thereof becomes, or in Ironscales' opinion may become, subject to an Infringement Claim or Customer's use thereof may be otherwise enjoined, Ironscales may, at its option, either: (i) procure for Customer the right to continue using the Platform; (ii) replace or modify the, so that it is non-infringing; or (iii) if neither of the foregoing alternatives is reasonably practical, terminate this Agreement and refund any prepaid fees for the unexpired term, if any. This Section 9.1 states Ironscales' entire liability and Customer's exclusive remedy for infringement.

9.2 **Indemnification Procedure**. The Customer shall give Ironscales prompt notice of any Claim, grant Ironscales sole control of the defense and/or settlement of any Claim (provided that Ironscales shall not enter into any settlement that admits liability on behalf of the Customer or imposes any obligations on the Customer without the prior written consent of the Customer, other than payment of amounts indemnified hereunder or, in the case of an Infringement Claim, cessation of use of the allegedly infringing item) and provide reasonable assistance as requested by Ironscales at Ironscales' expense.

10. **LIMITATION OF LIABILITY**.

EXCEPT FOR EITHER PARTY'S WILLFUL MISCONDUCT OR CUSTOMER'S BREACH OF IRONSCALES' INTELLECTUAL PROPERTY RIGHTS: (A) IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY, OR TO ANY THIRD PARTIES FOR INDIRECT, SPECIAL, CONSEQUENTIAL, COLLATERAL OR INCIDENTAL DAMAGES, LOSS OF BUSINESS, REVENUES, PROFITS AND GOODWILL, OR INTERRUPTION OF USE, LOSS OR INACCURACY OF DATA, LOSS OF, OR COST OF PROCURING SUBSTITUTE TECHNOLOGY, GOODS OR SERVICES, IN EACH CASE EVEN IF A

PARTY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; AND (B) IN NO EVENT SHALL EITHER PARTY'S AGGREGATE, CUMULATIVE LIABILITY TO THE OTHER PARTY OR ANY OTHER PARTY UNDER THIS AGREEMENT REGARDLESS OF THE FORM OF ANY CLAIM OR ACTION (WHETHER IN CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE) EXCEED THE PAYMENTS PAID BY CUSTOMER TO IRONSCALES UNDER AN ORDER DURING THE TWELVE (12) MONTHS PRECEDING THE EVENT GIVING RISE TO LIBAILITY.

11. **TERM; TERMINATION**

11.1 **Term.** The term of this Agreement shall commence on the earlier of: (i) Customer's access to the Platform; or (ii) the date set forth in the Order and continue until no Orders remain in effect hereunder, including any Renewal Periods as defined herein, unless otherwise terminated as stated below (the "**Term**"). The subscription term under an Order (referred to therein as the "**Subscription Period**") shall be as set forth in such Order and if no such term is set forth, the subscription shall continue for one (1) year from the effective date of such Order. The Subscription Period granted under each Order shall automatically renew for additional one (1) year terms following the end of each Subscription Period unless either party provides written notice of nonrenewal of such Subscription Period to the other party, not less than sixty (60) days prior the expiration thereof (the "**Renewal Periods**").

11.2 **Termination**. Either party may terminate this Agreement: (a) at any time, if the other party fails to cure a material breach of any of its obligations hereunder within thirty (30) days after receipt of written notice; (b) immediately upon written notice if the other Party commits a non-remediable, material breach or (c) immediately upon written notice, if the other party makes any assignment for the benefit of creditors, or a receiver, trustee in bankruptcy or similar officer is appointed to take charge of any or all of the other party's property, or the other party seeks protection under any bankruptcy, receivership, trust deed, creditors arrangement, composition or comparable proceeding or such a proceeding is instituted against the other party and is not dismissed within 90 days, or the other party becomes insolvent or, without a successor, dissolves, liquidates or otherwise fails to operate in the ordinary course.

11.3 **Effect of Termination**. Upon expiration the remaining Order or termination of this Agreement, Customer shall discontinue any further use and access to the Platform and shall promptly pay any then-outstanding amounts owed to Ironscales. In the event that this Agreement is terminated for Customer's breach, then all outstanding Orders shall be terminated immediately. For the removal of any doubt, no refunds or any portion thereof will be made except as explicitly set forth herein.

11.4 **Survival**. Notwithstanding any termination of this Agreement, Sections 6 (Proprietary Rights), 7 (Confidential Information), 9 (Indemnification), 10 (Limitation of Liability), 11.3 (Effect of Termination), 12 (General Provisions), shall survive and continue to be in effect in accordance with their terms.

12. **GENERAL PROVISIONS**

12.1 **Entire Agreement**. This Agreement (including all Orders) constitutes the entire agreement, and supersedes all prior negotiations, understandings or agreements (oral or written), between the parties regarding the subject matter of this Agreement (and all past dealing or industry custom). Any inconsistent or additional terms on any related Customer-issued purchase orders, vendor forms, invoices, policies, confirmation or similar form, even if signed by the parties hereafter, will have no effect under this Agreement. In the event of any conflict between the terms of this Agreement and the terms of any Order, the terms of this Agreement will control unless otherwise explicitly set forth in an Order. This Agreement may be executed in one or more counterparts, each of which will be an original, but taken together constituting one and the same instrument. Execution of a facsimile/electronic copy will have the same force and effect as execution of an original, and a facsimile/ electronic signature will be deemed an original and valid signature. No modification, consent or waiver under this Agreement will be effective unless in writing and signed by both parties. The failure of either party to enforce its rights under this Agreement at any time for any period will not be construed as a

waiver of such rights. If any provision of this Agreement is determined to be illegal or unenforceable, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

12.2 **Assignment**. This Agreement may not be assigned by Customer, in whole or in part, without Ironscales' prior express written consent. Ironscales may assign this Agreement, in whole or in part, without restriction or obligation. Any prohibited assignment will be null and void. Subject to the provisions of this Section (Assignment), This Agreement will bind and inure to the benefit of each party and its respective successors and assigns.

12.3 **Notices**. All notices and demands hereunder shall be in writing and shall be delivered to the address of the Receiving Party referenced below (or at such different address as may be designated by such party by written notice to the other party). All notices or demands shall be served by personal service or sent by certified, registered or signed-for mail, return receipt requested, by reputable national or international private express courier, or by electronic transmission, with confirmation received, to the email address specified below, and shall be deemed complete upon receipt: **To Ironscales**: the address listed in the applicable Order or by email to legal@ironscales.com. **To Customer**: the address and contact information listed in the applicable Order.

12.4 **Relationship of the Parties**. Customer and Ironscales shall operate as independent contractors and not as partners, joint venturers, agents or employees of the other. Neither party shall have any right or authority or assume or create any obligations or make any representations or warranties on behalf of the other party, whether expressed or implied, or to bind the other party in any respect whatsoever.

12.5 **Export and Import Compliance.** Customer shall comply with all applicable U.S. import, export and re-export regulations, including but not limited to, any regulations of the Office of Export Administration of the U.S. Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, and other U.S. agencies and the export control regulations of the European Union.

12.6 **Use of Customer Name**. Ironscales may use Customer’s name, logo, and trademarks and refer to its relationship with Customer in its business development and marketing efforts.

12.7 **Force Majeure**. Except for payment obligations, neither party shall have any liability under the Agreement to the extent that the performance of its obligations is delayed, hindered or prevented by an event or circumstance outside the reasonable control of the party, including fire, storm, flood, earthquake, adverse weather conditions, pandemic, explosions, Acts of God, terrorism or the threat thereof, nuclear, chemical or biological contamination, compliance with any law, governmental controls, restrictions or prohibitions general strikes, lock-outs, industrial action or employment dispute not caused by or specific or limited to the affected party, protests, public disorder, general interruptions in communications or power supply, and denial of service attacks.

12.8 **Governing Law**; **Jurisdiction**. This Agreement shall be governed by and construed under the laws of the State of Israel, without reference to principles and laws relating to the conflict of laws. The competent courts of the Tel-Aviv shall have the exclusive jurisdiction with respect to any dispute and action arising under or in relation to this Agreement.

IN WITNESS WHEREOF, the parties have caused their authorized signatories to have duly executed this Agreement:

	_____		_____
	IRONSCALES		**Customer**
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Exhibit A

IRONSCALES – DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms an integral part of the End User License Agreement ("**Agreement**") by 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 this term is defined under Data Protection Law. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions
   a. "**Data Controller**", "**Data Processor**", "**Personal Data**" "**Personal Data Breach**", "**data subject**", "**process**", "**processing**" shall have the meanings ascribed to them in the Data Protection Law.
   b. **"EEA"** means those countries that are member of the European Economic Area.
   c. "**Data Protection Law**" 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) ("**GDPR**"), 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.
   d. "**Security Measures**" mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of Ironscales' business, the level of sensitivity of the data collected, handled and stored, and the nature of Ironscales' business activities.
   e. **"Standard Contractual Clauses"** mean the applicable module of 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, a version of which is attached hereto as Appendix 2.
   f. "**Sub-Processors**" mean any affiliate, agent or assign 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.
   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 Data Protection Law.
   c. Ironscales agrees to notify Customer promptly if it becomes unable to comply with the terms of this Addendum 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 **Appendix 1** of this Addendum.
   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, the Agreement 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 law prohibits such information disclosure on grounds of public interest).

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.

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 Articles 32 to 36 of the GDPR, 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 subject 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. 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 Addendum, Ironscales shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. Notwithstanding the foregoing, Ironscales will cooperate with Customer with respect to any action taken pursuant to such order, demand or request, including ensuring 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 is included under **Annex III**.

c. Ironscales may appoint new Sub-Processors provided that Ironscales provides seven (7) days' prior notice 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 Addendum and meet the requirements of article 28(3) of the GDPR.
e. Ironscales will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Ironscales to breach any of its obligations under this Addendum.

7. Personal Data Breach

a. Within 48 hours of becoming aware of a Personal Data Breach, Ironscales will notify Customer without undue delay 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. Ironscales shall, no more than once a year and upon written notice 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 Addendum. Ironscales shall cooperate in good faith with audit requests by providing access to relevant knowledgeable personnel and documentation.
b. At Customer's written request, and subject to obligations of confidentiality, 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 Addendum.

9. International Data Transfers

a. Ironscales may transfer Personal Data of residents of the EEA or Switzerland outside the EEA ("**Transfer**"), only subject to the following: (i) the Transfer is necessary 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 the Data Protection Law.

b. To the extent necessary under the Data Protection Law, the Parties shall be deemed to enter into the Standard Contractual Clauses, which are incorporated herein under **Appendix 2**, in which event the Customer shall be deemed as the Data Exporter and Ironscales shall be deemed as the Data Importer (as these terms are defined therein);

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 under applicable law to retain the Personal Data (in which case

Ironscales will implement reasonable measures to prevent the Personal Data from any further processing). The terms of this Addendum will continue to apply to such Personal Data.

11. General

a. Any claims brought under this Addendum 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 between the Agreement (and any document referred to therein) and this Addendum, the provisions of this Addendum shall prevail.
c. Any changes to this Addendum 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.

Appendix 1

DETAILS OF THE PROCESSING

Subject matter

Ironscales will process Personal Data as necessary to provide Ironscales' platform pursuant to the Agreement, as further instructed by Customer in its use of Ironscales' platform.

Nature and Purpose of Processing

Providing Ironscales' platform to Customer and performing the Agreement.

Duration of Processing

Ironscales shall process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

- First name
- Last name
- Address
- Phone number
- Email address
- Email content and correspondences
- Headers
- Photos
- Links
- Attachments
- Videos
- Files
- IP addresses
- Payment information
- Business information
- Any other Personal Data or information that the Customer decides to provide to the Data Processor.

Categories of Data Subjects

Customer's users/customers

Appendix 2

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

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) ([1]) for the transfer of 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

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.

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 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. 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 ([2]) (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 non-compliance. 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.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list attached as Annex III to the Addendum to which this Appendix 2 is annexed. 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 3 business 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. ([3]) 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 sub-processor 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 sub-processor 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

(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.

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.

(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

(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

(a) The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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

(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 safeguards ([4]);

  (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).

(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. 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 case of access by public authorities

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.

(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.).

(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.

(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 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

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(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 Ireland.

(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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*
Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller):

Data importer(s):
Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (processor):

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Appendix 1

Categories of personal data transferred

See Appendix 1

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Appendix 1

The frequency of the transfer.

See Appendix 1

Nature of the processing

See Appendix 1

Purpose(s) of the data transfer and further processing

To provide the Platform

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

The duration of the Agreement.

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

See Annex III, for the duration of the Agreement.

C. *COMPETENT SUPERVISORY AUTHORITY*

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

The Irish Supervisory Authority

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE 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. Service Provider 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 Service Provider's own applications and information, including but not limited to the public internet or any system used by Service Provider. 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. Service Provider 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 Service Provider's systems and Customer's information. Service Provider 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 are conditioned on prior approval.*

10. *Transfer of Confidential Information between Customer and the Service Provider will be implemented by using secure file transfer platform.*

11. *Be responsible to architecture reviews, conduct penetration tests and/or code review to the Service Provider'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. *Be in compliance with SOC 2 Type II standard. Customer shall be entitled to receive the SOC 2 Type II report upon its demand (with the current report attached to this Agreement as Exhibit D).*

...

ANNEX III

List of current Sub Processors

Entity Name	Sub-Processing Activities	Entity Country
Amazon Web Services	Primary Application Platform	USA
Amazon Web Service EMEA SARL ("AWS Europe")	Primary Application Platform	Luxembourg (processing activity in Germany)
Check Point Software Technologies Ltd.	Sandbox	Israel
Virus Total (by Google Inc.)	Scan Links	USA
Bitdefender SRL	Scan Links	Romania
Google Web Risk API	Scan Links	USA

Exhibit B

IRONSCALES – SUPPORT TERMS

1. **SERVICE – SaaS solution only**

1.1 Ironscales shall use commercially reasonable efforts to make Ironscales Cloud available 24 hours a day, 7 days a week, except for: (a) planned downtime (for which Ironscales shall provide notice for), and (b) unavailability caused by force majeure circumstances beyond Ironscales' reasonable control. Customer's email traffic will not be impacted in the event of Ironscales service downtime**.**

1.2 False positive rate of identifying phishing emails will be less than 5% (where under the control of Ironscales – Not including Customer's SOC team classifications).

2. **SUPPORT**

2.1 **Support Request.** For the purposes of this agreement, a "**Support Request**" is generally defined as a request for support to fix a bug in an existing released version of the Platform or a request for support that involves functionality of thereof.

2.2 **Levels of Support**. Two levels of support are provided under this agreement. These levels, which are integrated into Ironscales' support process, are defined as follows:

2.2.1 **Standard Coverage**. This level is inclusive within these Support Terms with no further cost.

2.2.2 **On Premise Coverage.** Requires a remote access to the site, for support purposes as a prerequisite for remote-support. On premise coverage support service does not include travel & accommodation expenses to and from the site upon a support call that requires an on-site visit, which shall be invoiced separately.

2.3 **Standard Support Coverage**. This is support provided by the appropriate Ironscales' help desk when it receives the Support Request from the customer. Customer shall open a support ticket for Ironscales', which is then passed to Ironscales' support specialists.

2.4 **Call Management Process**. Ironscales' problem-ticket system will be used by all support team levels (where approval and technical access has been granted) to record and track all problem reports, inquiries, or other types of calls received by support. Support Requests are taken by Ironscales' Help Desk as follows:

Help Desks	Hours	Phone Contact
Standard Coverage	2:00 a.m. – 5:00 p.m. Monday - Friday 2:00 a.m. – 11:00 a.m. Sunday	US +188-8343-7214 UK +44-80-0041-8133 IL +972-73-796-9729
Support email	support@ironscales.com	

2.5 **Response Time**: The guaranteed response time following any critical/outage incident shall be 24 hours or less. The guaranteed response for any other incidents shall be within one (1) business day or less, normal business hours (2:00 a.m. – 5:00 p.m., Monday – Friday; and 2:00 a.m. – 11:00 a.m., Sunday all US Eastern Time) on a best effort basis. The response time begins when the request is logged with IRONSCALES' problem ticketing system and is stopped when a response has been initiated from Ironscales.

2.6 **Tickets severity** will be classified as Critical, High, Medium and Low. Ironscales will do best efforts to provide a workaround or hot fix to critical (Severity 1) tickets provided within 48 hours from Ironscales response to the ticket.

2.7 **UPDATES & UPGRADES [for On-Premise implementations only]** Updates and upgrades to Ironscales' Platform occurs when an update/upgrade to an existing product is released; Ironscales shall make the updated software version available for the Customer every 3 months or less, and/or in an event on which a critical software upgrade has been released by Ironscales' or any of its 3rd party technology partners.

3. ROLES OF IRONSCALES

3.1 Ironscales has the following general responsibilities under these Support Terms:

3.1.1 Ironscales will use its own appropriate help desk to provide Level-1 to Level-4 Support Services

3.1.2 Once a support request has been submitted, Ironscales will make itself available to work with the Customer support resource assigned to the support request within the stated response time.

3.1.3 Ironscales will attempt to resolve problems over the phone/online on first call.

3.1.4 The customer end-users will not contact Ironscales' support resources directly to report a problem. All problem calls must be logged through the appropriate help desk.

3.1.5 Ironscales will provide all necessary and requested documentation, information, and knowledge capital to the Customer prior to the start of support of Ironscales' Platform.

4. **TERMINATION**

This SLA shall automatically terminate upon the termination or expiration of the Agreement under which the services are provided.

5. **RELATIONSHIP WITH AGREEMENT**

In the event of any conflict between the provisions of this SLA and the provisions of the Agreement, the provisions of this SLA shall prevail over the conflicting provisions of the Agreement.

6. **AMENDMENTS**

This SLA may be amended at any time by a written instrument duly signed by each of the Parties.

	_____		_____
	IRONSCALES		**Customer**
Title:	_____	Title:	_____

_____