Data Processing Addendum

Policy Owner: Mehdi Djabri

Effective Date: December 20, 2022

This document (hereinafter referred to as "**DPA**" or "**Data Processing Addendum**") reflects the agreement with respect to the Processing of Personal Data by Iteration X on behalf of Customer between Iteration X and Customer. The DPA is concluded in connexion with Iteration X's Terms of Service and Privacy policy, both publicly available. By executing the Addendum, Customer enters into this Addendum on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below), if any.

I. Definitions

(1) "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

(2) "Authorized Sub-Processor" means a third party who has a need to know or otherwise access Customer's Personal Data to enable Iteration X to perform its obligations under this Addendum or the Terms of Service, and who is either (1) listed in Annex II or (2) subsequently authorized under Section 4.2 of this Addendum.

(3) "Customer Account Data" means personal data that relates to Customer's relationship with Iteration X, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Customer Account Data also includes any data Iteration X may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

(4) "Customer Usage Data" means Service usage data collected and processed by Iteration X in connexion with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

(5) "Data Exporter" means Customer.

(6) "Data Importer" means Iteration X.

(7) "Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) the California Consumer Privacy Act ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR" or "GDPR"), (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time. The terms "Data Subject", "Personal Data", "Personal Data Breach", "processing", "processor," "controller," and "supervisory authority" shall have the meanings set forth in the GDPR.

(8) "EU SCCs" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).

(9) "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

(10) "Services" shall have the meaning set forth in the Terms of Service.

(11) "Standard Contractual Clauses" means the EU SCCs.

II. Processing of Data

(1) The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this Addendum or the Terms of Service, Iteration X is a processor.

(2) Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Iteration X to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Iteration X by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Iteration X regarding the processing of such Personal Data. Customer shall not provide or make available to Iteration X any Personal Data in violation of the Terms of Service or otherwise inappropriate for the nature of the Services, and shall indemnify Iteration X from all claims and losses in connection therewith.

(3) Iteration X shall not process Personal Data:

(i) for purposes other than those set forth in the Terms of Service and/or Annex I, (ii) in a manner inconsistent with the terms and conditions set forth in

this Addendum or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Iteration X is subject; in such a case, the Iteration X shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or
(iii) in violation of Data Protection Laws.

Customer hereby instructs Iteration X to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

(4) The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Annex I to this Addendum.

(5) Following completion of the Services, at Customer's choice, Iteration X shall delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If destruction is impracticable or prohibited by law, rule or regulation, Iteration X shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Iteration X have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Iteration X to Customer only upon Customer's request.

(6) CCPA. Except with respect to Customer Account Data and Customer Usage Data, the parties acknowledge and agree that Iteration X is a service provider for the purposes of the CCPA (to the extent it applies) and is receiving personal information from Customer in order to provide the Services pursuant to the Terms of Service, which constitutes a business purpose. Iteration X shall not sell any such personal information. Iteration X shall not retain, use or disclose any personal information provided by Customer pursuant to the Terms of Service except as necessary for the specific purpose of performing the Services for Customer pursuant to the Terms of Service, or otherwise as set forth in the Terms of Service or as permitted by the CCPA. The terms "personal information," "service provider," "sale," and "sell" are as defined in Section 1798.140 of the CCPA. Iteration X certifies that it understands the restrictions of this Section 2.5.

III. Confidentiality

Iteration X shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Iteration X's confidentiality obligations in the Terms of Service. Customer agrees that Iteration X may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this Addendum, the Terms of Service, or the provision of Services to Customer.

IV. Authorized Sub-Processors

(1) Customer acknowledges and agrees that Iteration X may:

(i) engage its affiliates and the Authorized Sub-Processors on the List (defined below) to access and process Personal Data in connection with the Services and
(ii) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. By way of this Addendum, Customer provides general written authorization to Iteration X to engage sub-processors as necessary to perform the Services.

(2) A list of Iteration X's current Authorized Sub-Processors will be made available to Customer at https://www.iterationx.com/data-processors. Such List may be updated by Iteration X from time to time. Iteration X will provide a mechanism to subscribe to notifications (which may include but are not limited to email) of new Authorized Sub-Processors and Customer, if it wishes, will subscribe to such notifications where available. If Customer does not subscribe to such notifications, Customer will have waived any right it may have to prior notice of changes to Authorized Sub-Processors. At least ten (10) days before enabling any third party other than existing Authorized Sub-Processors to access or participate in the processing of Personal Data, Iteration X will add such third party to the List and notify subscribers, including Customer, via the aforementioned notifications. Customer may object to such an engagement by informing Iteration X in writing within ten (10) days of receipt of the aforementioned notice by Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Iteration X from offering the Services to Customer.

(3) If Customer reasonably objects to an engagement in accordance with Section 4.2, and Iteration X cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Iteration X. Discontinuation shall not relieve Customer of any fees owed to Iteration X under the Terms of Service.

(4) If Customer does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Iteration X, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

(5) Iteration X will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Iteration X under this Addendum with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Iteration X, Iteration X will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations under such agreement.

(6) If Customer and Iteration X have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Iteration X of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Iteration X to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent,

removed by the Iteration X beforehand, and that such copies will be provided by the Iteration X only upon request by Customer.

V. Security of Personal Data

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Iteration X shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Annex II sets forth additional information about Iteration X's technical and organizational security measures.

VI. Transfers of Personal Data

(1) The parties agree that Iteration X may transfer Personal Data outside the EEA as necessary to provide the Service in accordance with the Terms of Services, and in particular that Personal Data may be transferred in the United States and to other jurisdictions where Iteration X, Iteration X's Affiliates and Iteration X's Sub-Processors have operations. Customer acknowledges that Iteration X's primary processing operations take place in the United States, and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. If Iteration X transfers Personal Data protected under this Addendum to a jurisdiction for which the European Commission has not issued an adequacy decision, Iteration X will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

(2) Ex-EEA Transfers. The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(i) Module One (Controller to Controller) of the EU SCCs apply when Iteration X is processing Personal Data as a controller pursuant to Section 9 of this Addendum.

(i) Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Iteration X is processing Personal Data for Customer as a processor pursuant to Section 2 of this Addendum.

(iii) Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Iteration X is processing Personal Data on behalf of Customer as a sub-processor.

(3) For each module, where applicable the following applies:

(i) The optional docking clause in Clause 7 does not apply.

(ii) In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4.2 of this Addendum;

(iii) In Clause 11, the optional language does not apply;

(iv) All square brackets in Clause 13 are hereby removed;

(v) In Clause 17 (Option 1), the EU SCCs will be governed by French law;

(vi) In Clause 18(b), disputes will be resolved before the courts of France;

(vii) Annex II to this Addendum contains the information required in Annex I of the EU SCCs;

(viii) Annex III to this Addendum contains the information required in Annex II of the EU SCCs; and

(ix) By entering into this Addendum, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

(4) Supplementary Measures. In respect of any ex-EEA Transfer, the following supplementary measures shall apply:

(i) As of the date of this Addendum, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer's Personal Data ("Government Agency Requests");

(ii) If, after the date of this Addendum, the Data Importer receives any Government Agency Requests, Iteration X shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Iteration X may provide Customer's basic contact information to the government agency. If compelled to disclose Customer's Personal Data to a law enforcement or government agency, Iteration X shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Iteration X is legally prohibited from doing so. Iteration X shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this Addendum should be suspended in the light of the such Government Agency Requests; and

(iii) The Data Exporter and Data Importer will meet as needed to consider whether:

(a) the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA;

(b) additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

(c) it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

(iv) If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

(v) If either (i) any of the means of legitimizing transfers of Personal Data outside the EEA set forth in this Addendum cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may, by notice to the Data

Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

VII. Rights of Data Subjects

(1) Iteration X shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Iteration X receives a Data Subject Request in relation to Customer's data, Iteration X will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Iteration X, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

(2) Iteration X shall, at the request of the Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Iteration X's assistance and (ii) Iteration X is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Iteration X.

VIII. Actions and Access Requests

(1) Iteration X shall, taking into account the nature of the processing and the information available to Iteration X, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, *provided that* Customer does not otherwise have access to the relevant information. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Iteration X.

(2) Iteration X shall, taking into account the nature of the processing and the information available to Iteration X, provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Iteration X.

(3) Iteration X shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum, and retain such records for a period of three (3) years after the termination of the Terms of Service. Customer shall, with reasonable notice to Iteration X, have the right to review, audit and copy such records at Iteration X's offices during regular business hours.

(4) Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Iteration X shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Iteration X's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Iteration X's data security infrastructure and procedures that is sufficient to demonstrate Iteration X's compliance with its obligations under Data Protection Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Iteration X's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Iteration X for any time expended for on-site audits. If Customer and Iteration X have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 8.4.

(5) Iteration X shall immediately notify Customer if an instruction, in Iteration X's opinion, infringes the Data Protection Laws or Supervisory Authority.

(6) In the event of a Personal Data Breach, Iteration X shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Iteration X in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Iteration X's reasonable control).

(7) In the event of a Personal Data Breach, Iteration X shall, taking into account the nature of the processing and the information available to Iteration X, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

(8) The obligations described in Sections 8.5 and 8.6 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Iteration X's obligation to report or respond to a Personal Data Breach under Sections 8.5 and 8.6 will not be construed as an acknowledgement by Iteration X of any fault or liability with respect to the Personal Data Breach.

IX. Iteration X's Role as a Controller

The parties acknowledge and agree that with respect to Customer Account Data and Customer Usage data, Iteration X is an independent controller, not a joint controller with Customer. Iteration X will process Customer Account Data and Customer Usage Data as a controller:

(i) to manage the relationship with Customer;

(ii) to carry out Iteration X's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes;

(iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer;

(iv) for identity verification purposes;
(v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Iteration X is subject; and
(vi) as otherwise permitted under Data Protection Laws and in accordance with this Addendum and the Terms of Service.

Iteration X may also process Customer Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by Iteration X as a controller shall be in accordance with Iteration X's privacy policy set forth at https://www.iterationx.com/privacy.

X. Conflict

In the event of any conflict or inconsistency among the following documents, the order of precedence will be:
(1) the applicable terms in the Standard Contractual Clauses;
(2) the terms of this Addendum;
(3) the Terms of Service; and
(4) Iteration X's privacy policy.

Any claims brought in connection with this Addendum will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Terms of Service.

XI. Applicable Law

The applicable law is the French law, as it is stated in Clause 17 of the SCCs.

XII. Execution of the Addendum

Iteration X has pre-signed this Addendum, in the signature block below and in each of the main body, and Annex II (as the "data importer"). To complete this Addendum, Customer must: (i) complete the information requested in the signature block below and sign there, (ii) complete the information requested of the "data exporter" on Annex II, and (iii) send the completed and signed Addendum to Iteration X by email to legal@iterationx.com. Upon receipt of the validly completed Addendum by Iteration X at this email address, this Addendum will become legally binding.

Customer	**Iteration X**
Signature: Customer Legal Name:	Signature:
Print Name:	Print Name: Mehdi Djabri
Title:	Title: CEO
Date:	Date: 12 / 20 / 2022

Appendix

STANDARD CONTRACTUAL CLAUSES

For the meaning of all capitalized terms that are not explicitly defined hereinafter, please refer to the Privacy policy (www.iterationx.com/privacy), the Data Protection Addendum (www.iterationx.com/dpa-scc) and the Terms of Service (www.iterationx.com/tos).

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

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

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

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

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 (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. 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 1 (one) day 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.[1] 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

[1]

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) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] 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[2];

(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.

[2]

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

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.

(f) The Parties agree that those shall be the courts of FRANCE.

(g) 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.

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

Annex I - Details of Processing

Nature and Purpose of Processing: Iteration X will process Customer's Personal Data as necessary to provide the Services under the Terms of Service, for the purposes specified in the Terms of Service and this Addendum, and in accordance with Customer's instructions as set forth in this Addendum. This includes, without limitation:

- storage and hosting of the Customer Usage Data contained in the content generated by the data controller using of the Services;
- collaboration with the data controller to respond to Personal Data subjects exercised one of his or her individual rights.

Duration of Processing: Iteration X will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Terms of Service; (ii) for Iteration X's legitimate business needs; or (iii) by applicable law or regulation. Customer Account Data and Customer Usage Data will be processed and stored as set forth in Iteration X's privacy policy.

Categories of Data Subjects: Categories of Data Subjects may include, but are not limited to Personal Data relating to the following categories of Data Subjects: Customer's contacts and other end users including Customer's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors.

Categories of Personal Data: Iteration X processes Personal Data contained in Customer Account Data, Customer Usage Data, and any Personal Data provided by Customer or collected by Iteration X in order to provide the Services or as otherwise set forth in the Terms of Service or this Addendum. Categories of Personal may include but are not limited to the following categories of Personal Data: name, email, job title, username, Iteration X device identifiers (e.g. serial number), and Personal Data included in comments and modified websites.

Sensitive Data or Special Categories of Data: Customers are prohibited from providing sensitive personal data or special categories of data to Iteration X, including any data which discloses the criminal history of any persons.

Annex II - Information on the processing

The following includes the information required by Annex I and Annex III of the EU SCCs.

1. **The Parties**

   Data exporter(s):

   Name: Customer, as defined in the Iteration X's Terms of Service (on behalf of itself and Permitted Affiliates)

   Address: Customer's address, as set out in the Order Form or in Customer's Iteration X Account.

   Contact person's name, position and contact details: The Customer's contact details, as set out in the Order Form and/or as set in Customer's Iteration X Account.

   Activities relevant to the data transferred under these Clauses: As described in Section 2 of the Addendum.

   Signature and date (mm/dd/yyyy) :

   Role (controller/processor): Controller

   Data importer(s):

   Name: Iteration X

   Address: 6 rue du Bois Sauvage, 91000 Evry-Courcouronnes, FRANCE.

   Email: legal@iterationx.io

   Activities relevant to the data transferred under these Clauses: As described in Section 2 of the Addendum.

   Signature and date (mm/dd/yyyy) :

   Role (controller/processor): Processor

2. **Description of the Transfer**

Data Subjects	The data exporter may submit personal data to the data importer through its software, services, systems, products, and/or technologies, the extent of which is determined and controlled by the data exporter in compliance with applicable data protection laws and regulations, and which may include but is not limited to personal data relating to the following categories of data subjects: data exporter's contacts and other end user including data exporter's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors.
Categories of Personal Data	The personal data transferred concern the following categories of data: Any personal data comprised in all data and information submitted by data exporter to data importer's software, services, systems, products, and/or technologies, which may include name,

	contact information, and information about security practices and compliance.
Special Category Personal Data (if applicable)	Data exporters are prohibited from providing sensitive data or special categories to data importers.
Nature of the Processing	Data is processed in order for Customer to manage its information security and data privacy programs and evidence said programs for third-party audit.
Purposes of Processing	To fulfill each party's obligations under the Terms of Service.
Duration of Processing and Retention (or the criteria to determine such period)	During the term of the Terms of Service.
Frequency of the transfer	During the term of the Terms of Service on a periodic basis throughout the day and/or at the discretion of the customer.
Recipients of Personal Data Transferred to the Data Importer	Iteration X will maintain a list of Suprocessors at: https://www.iterationx.com/sub-processors

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with GDPR. For this addendum, the competent supervisory authority is the French national supervisory authority : the CNIL, 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07.

Annex III - Description of the Technical and Organizational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs.

Iteration X currently observes the Security Measures described in this Annex III. All capitalized terms not otherwise defined herein will have the meanings as set forth in the Terms of Service. For more information on these security measures, please refer to Iteration X's Security webpage, available at https://www.iterationx.com/security.

Measures of pseudonymisation and encryption of personal data	Iteration X encrypts at rest its datastores housing sensitive customer data, and uses data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks Iteration X enforces encrypted remote access for its production systems, with restricted access to encryption keys. Iteration X also encrypts portable and removable media devices when used.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Iteration X's customer agreements contain strict confidentiality obligations. Additionally, Iteration W requires every downstream Subprocessor to sign confidentiality provisions that are similar to those contained in Iteration X's customer agreements. Iteration X has undergone a SOC 2 Type 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Daily backups of production datastores are taken. Backups are periodically tested in accordance with information security and data management policies.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Iteration X has undergone a SOC 2 Type 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
Measures for user identification and authorization	Iteration X uses secure access protocols and processes and follows industry best-practices for authentication, including Multifactor Authentication and SSH keys. All production access requires the use of two-factor authentication, and network infrastructure is securely configured to vendor and industry best practices to block all unnecessary ports, services and unauthorized network traffic.
Measures for the protection of data during transmission	Iteration X has deployed secured methods and protocols for transmission of confidential or sensitive information over public networks Iteration W uses only recommended secure cypher suites and protocols to encrypt all traffic in transit (i.e. TLS 1.2)
Measures for the protection of data during storage	Encryption-at-rest is automated using AWS transparent disk encryption, which uses industry standard AED-256 encryption to secure all volume data.

	All keys are fully managed by AWS.
Measures for ensuring physical security of locations at which personal data are processed	All Iteration X processing occurs in physical data centers that are managed by AWS. https://aws.amazon.com/compliance/data-center/controls/
Measures for ensuring events logging	Iteration X monitors access to applications, tools, and resources that process or store Customer Data, including cloud services. Monitoring of security logs is managed by the security and engineering teams. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	Iteration X adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications and systems. All production changes are automated through CI/CD tools to ensure consistent configurations.
Measures for internal IT and IT security governance and management	Iteration X maintains an ISO 27001-compliant risk-based information security governance program. The framework for Iteration X security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.
Measures for certification/assurance of processed and products	Iteration X undergoes annual SOC 2 Type II and ISO 27001 audits.
Measures for ensuring data minimization	Iteration X's Customers unilaterally determine what Customer PII Data they route through the Services. As such, Iteration X operates on a shared responsibility model. Iteration X gives Customers control over exactly what PII data enters the platform. Additionally, Iteration X has built in self-service functionality to the Services that allows Customers to delete and suppress PII at their discretion.
Measures for ensuring data quality	Iteration X has a multi-tiered approach for ensuring data quality. These measures include: (i) unit testing to ensure quality of logic used to process API calls, (ii) database schema validation rules which execute against data before it is saved to our database, (iii) a schema-first API design and strong typing to enforce a strict contract between official clients and API resolvers. Iteration X applies these measures across the board, both to ensure the quality of any Usage Data that Iteration X collects and to ensure that the Iteration X Platform is operating within expected parameters. Iteration X ensures that data quality is maintained from the time a Customer sends Customer Data into the Services and until that Customer Data is presented or exported.
Measures for ensuring limited data retention	Iteration X's Customers unilaterally determine what Customer Data they route through the Services. As such, Iteration X operates on a shared responsibility model. If a Customer is unable to delete Customer PII Data via the self-services functionality of the Services, then Iteration X deletes Customer Data upon the Customer's written request, within the timeframe specified in the Data Protection Addendum and in accordance with Applicable Data Protection Law. All Customer Data is deleted from the Services following service termination.
Measures for ensuring accountability	Iteration X has adopted measures for ensuring accountability, such as implementing data protection and information security policies across the business, recording and reporting Security Incidents involving Personal Data, and formally assigning roles and responsibilities for information security and data privacy functions. Additionally, Iteration X conducts regular

	third-party audits to ensure compliance with our privacy and security standards.
Measures for allowing data portability and ensuring erasure	All PII in the Services may be deleted by the Customer or at the Customer's request. PII is incidental to Iteration X's Services. Based on Privacy by Design and Data Minimization principles, Iteration X severely limits the instances of PII collection and processing within the Services. Most use cases for porting PII from Iteration X are not applicable. However, Iteration X will respond to all requests for data porting in order to address Customer needs.
Technical and organizational measures of sub-processors	Iteration X enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this Addendum.

Dropbox Sign

Audit trail

Title	DPA - Iteration X
File name	Iteration X - DPA.pdf
Document ID	cdbe74df868417341c37d84aa09d7b02975568ec
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document history

SENT	**12 / 20 / 2022** 20:10:14 UTC	Sent for signature to Mehdi Djabri (mehdi@iterationx.io) from mehdi@iterationx.io IP: 91.168.62.113
VIEWED	**12 / 20 / 2022** 20:10:32 UTC	Viewed by Mehdi Djabri (mehdi@iterationx.io) IP: 91.168.62.113
SIGNED	**12 / 20 / 2022** 20:10:45 UTC	Signed by Mehdi Djabri (mehdi@iterationx.io) IP: 91.168.62.113
COMPLETED	**12 / 20 / 2022** 20:10:45 UTC	The document has been completed.