

## Perceptyx Data Processing Addendum

This Data Processing Addendum (“**DPA**”) is by and between Perceptyx (as defined below) and Customer (as defined below) (each a “**Party**,” and collectively the “**Parties**”) on behalf of itself and as agent for its Authorized Affiliates (defined below), and forms part of the Agreement (defined below) between Perceptyx and Customer.

**NOW, THEREFORE**, in consideration of the mutual obligations hereto, the Parties enter into this DPA and agree that the terms of this DPA will form a part of the Agreement, which shall remain in full force and effect except to the extent modified below.

### 1. DEFINITIONS

The capitalized terms set forth in this Section will apply to this DPA. Capitalized terms used but not otherwise defined in this DPA will have the meanings as otherwise set forth in the Agreement.

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.

“**Agreement**” means the Master Services Agreement or other written or electronic agreement between the Parties for the purchase of the SaaS Services, and any Order Form(s), exhibits, schedules and amendments to any of the foregoing documents.

“**Authorized Affiliate**” means an Affiliate of Customer that is authorized to use the SaaS Services pursuant to the Agreement (if any).

“**Controller**” means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“**Customer**” means the purchasing entity identified in the applicable Order Form(s).

“**Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Perceptyx.

“**Data Protection Laws**” means all data protection laws and regulations governing the Processing of the Personal Data, including, to the extent applicable, the General Data Protection Regulation (EU) 2016/679 and the implementing legislation of each EU member state, as amended (“**GDPR**”), the UK General Data Protection Regulation, as amended by the Data Protection Act 2018 (“**UK GDPR**”), the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100, et seq., and its implementing regulations, as amended by the California Privacy Rights Act of 2020 (“**CCPA**”), the Swiss Federal Act on Data Protection of 1992, as amended (“**FADP**”), Lei Geral de Proteção de Dados (Brazil’s General Data Protection Law), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act.

“**Data Subject**” means an identified or identifiable natural person about whom certain Personal Data relates.



**“Data Subject Access Request”** means a request from or on behalf of a Data Subject regarding the Personal Data processed pursuant to the SaaS Services, including a request to exercise rights under the Data Protection Laws.

**“Order Form(s)”** means the document that sets forth the SaaS Services Customer is purchasing.

**“Perceptyx”** means: (i) Perceptyx, Inc., a California corporation, if Customer’s contracting entity is located within North or South America, or (ii) Perceptyx BV, a Netherlands private limited company, if Customer’s contracting entity is located outside of North or South America.

**“Personal Data”** means the following information, to the extent Processed by Perceptyx on behalf of Customer and any Authorized Affiliate, in order to perform the SaaS Services pursuant to the Agreement: (i) any information relating to an identified or identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, and (ii) other information defined as “personal data,” “personal information,” or other similar terms under applicable Data Protection Laws. “Personal Data” does not include anonymous data derived from the use of the SaaS Services, which does not directly or indirectly identify, and is not otherwise linked or linkable, to a particular Data Subject.

**“Process(es)(ed)(ing)”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**“Processor”** means the entity that Processes Personal Data on behalf and under the instructions of the Controller.

**“Restricted Transfer”** means a transfer of Personal Data to or by Perceptyx or a Subprocessor, to a jurisdiction that is not recognized as providing an adequate level of protection for Personal Data by applicable Data Protection Laws, where such transfer would be prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses and UK Addendum, respectively, as applicable.

**“SaaS Services”** means any solution hosted, supported, and licensed under the Agreement by Perceptyx as set forth in the applicable Order Form.

**“Standard Contractual Clauses”** or **“SCCs”** means the standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection of data subjects, which have been approved by the European Commission as adducing adequate safeguards for Restricted Transfers, or any successor clauses thereto or alternative data transfer mechanisms recognized by the European Commission pursuant to Article 46 of the GDPR, or by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another



competent authority under other relevant Data Protection Laws and Regulations.

“**Subprocessor**” means Perceptyx Affiliates and a third person or entity (excluding an employee of Perceptyx) appointed by Perceptyx or Perceptyx Affiliates that Process the Personal Data in accordance with this DPA.

“**Supervisory Authority**” means (a) an independent public authority established by a Member State pursuant to Article 51 of the GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws.

“**Swiss Restricted Transfer**” means a transfer of Personal Data by Customer or any Customer Affiliate to Perceptyx or any Perceptyx Affiliate (or any onward transfer), in each case, where such transfer would be prohibited by the FADP in the absence of the protection for the transferred Personal Data provided by the SCCs, provided that such SCCs are subject to the Swiss Addendum set out in Annex 5 to this DPA.

“**Third Party Request**” means any request, inquiry, or complaint received by Perceptyx from a Supervisory Authority or other third party regarding Personal Data, including any request to exercise rights under the Data Protection Laws, but not a Data Subject Access Request.

“**UK Addendum**” means the International Data Transfer Addendum (Version B1.0 in force 21 March 2022) to the Standard Contractual Clauses, issued by the UK Information Commissioner’s Office (“**ICO**”) to provide appropriate safeguards for a UK Restricted Transfers, as set out in Annex 4 to this DPA.

“**UK Restricted Transfer**” means a transfer of Personal Data by Customer or any Customer Affiliate to Perceptyx or any Perceptyx Affiliate (or any onward transfer), in each case, where such transfer would be prohibited by the UK GDPR in the absence of the protection for the transferred Personal Data provided by the SCCs, provided that such SCCs are subject to the UK Addendum set out in Annex 4 to this DPA.

## 2. PROCESSING OF PERSONAL DATA

2.1. **Scope and role of the Parties.** This DPA applies to the processing of Personal Data by Perceptyx in the course of providing the SaaS Services under the Agreement. The Parties acknowledge and agree that with regard to the Processing of Personal Data, Customer and/or the Authorized Affiliate(s) are the Controller(s), and Perceptyx is the Processor (or subprocessor where Customer and/or the Authorized Affiliate(s) are Processors(s)). Annex 1 to this DPA sets out the subject matter and duration of the Processing, the nature and purpose of the Processing, and the categories of Personal Data and Data Subjects, as required by Article 28(3) of the GDPR.

2.2. **Perceptyx.** Perceptyx will only Process Personal Data in accordance with the documented instructions of Customer and as set forth herein, or as otherwise required by applicable Data Protection Laws, in which case Perceptyx will, to the extent permitted by applicable law, inform Customer of the legal requirement before such Processing of Personal Data. Perceptyx will not Process the Personal Data for any purposes other than as specified in the Agreement and this DPA and will not sell, rent, release, disclose, disseminate, make available, transfer or otherwise communicate Personal Data to any third party for monetary or other



valuable consideration. Perceptyx certifies that that it understands the foregoing restrictions and will comply with them.

2.3. **Customer.** Customer, on its own behalf and as agent for any Authorized Affiliate, hereby instructs Perceptyx and authorizes Perceptyx to instruct each approved Subprocessor to: (i) Process the Personal Data (a) in order to provide the SaaS Services and perform Perceptyx's obligations under the Agreement, including to respond to, complete, carry out or apply account settings and actions requested or initiated by Customer or Authorized Affiliates via the SaaS Services, to respond to customer service and support requests, to perform any necessary technical support, and as otherwise set forth in the Agreement, this DPA or other documented instructions of Customer; and (ii) to Process and transfer the Personal Data outside the jurisdiction in which it was collected, including in the United States, the European Economic Area, the United Kingdom and other jurisdictions where Perceptyx, its Affiliates and Subprocessors are located.

2.4. **Compliance.** The Parties will comply with their respective obligations under applicable Data Protection Laws. Without limiting the foregoing, Customer agrees that (a) Customer is solely responsible for, and represents and warrants that any required notices have been provided to and any required consents have been obtained from Data Subjects related to the Processing of Personal Data as contemplated in this DPA and the Agreement; and (b) Customer will have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Customer acquired Personal Data. With respect to the instructions set forth in this Section 2, Customer represents and warrants that it is, and at all relevant times will remain, duly and effectively authorized to give such instruction and that such the instruction to Process the Personal Data will not violate applicable laws including the Data Protection Laws, or the instructions of any third party. Notwithstanding any other provision in the Agreement or herein to the contrary, Customer will indemnify, defend and hold harmless Perceptyx, its Affiliates and Subprocessors, from and against any and all liability or third party claims arising out of or relating to Customer or its Affiliate's breach of this Section 2.

### 3. SUBPROCESSORS

3.1. **Use of Subprocessors.** Perceptyx and Perceptyx Affiliates may appoint Subprocessors to Process Personal Data in accordance with this Section. Customer generally consents and agrees that Perceptyx may engage any Perceptyx Affiliate as a Subprocessor to deliver some or all of the SaaS Services provided to Customer. Perceptyx and/or its Affiliates may (i) continue to use those Subprocessors currently in use as of the effective date of this DPA (as identified in Annex 1 to this DPA); and (ii) may engage other third parties and Subprocessors where Customer has requested SaaS Services that require the engagement of such third party or Subprocessor. Prior to any Processing by Subprocessor of Personal Data, Perceptyx will exercise appropriate care in appointing and overseeing authorized Subprocessors and will enter into contractual terms with authorized Subprocessors that include equivalent terms as applicable to Perceptyx under this DPA. Perceptyx will remain liable to Customer for the performance of the Subprocessors' obligations.

3.2. **Appointment of New Subprocessors.** Prior to Perceptyx and Perceptyx Affiliates appointing any additional Subprocessor, Perceptyx will provide Customer with prior notice and the opportunity to object based on reasonable grounds related to the protection of Personal Data;



if within thirty (30) days of such notice, Customer has not notified Perceptyx in writing of its objection via the Perceptyx Subprocessor webpage, below, Customer will be deemed to have agreed to the appointment of the new Subprocessor. Customer may access Perceptyx and/or Perceptyx Affiliates' up-to-date list of Subprocessors and submit any objections by visiting <https://go.perceptyx.com/legal-perceptyx-sub-processors>. If the Parties cannot reach a resolution within ninety (90) days from the date of Perceptyx's receipt of Customer's written objection, either Party may suspend or terminate (in accordance with the Agreement) the applicable portion of the SaaS Services which cannot be provided by Perceptyx without use of the objected-to Subprocessor, and without prejudice to any fees incurred by Customer prior to such suspension or termination.

3.3. **Emergency Appointment.** Perceptyx and Perceptyx Affiliates may replace or appoint a Subprocessor without advance notice where prompt replacement is required for security or other urgent reasons. In such case, Perceptyx will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 3.2 applies accordingly.

#### 4. COOPERATION BY PERCEPTYX

4.1. **Data Subject Access Requests.** If Perceptyx receives a Data Subject Access Request Perceptyx will, unless prohibited from doing so by applicable laws: (a) promptly notify Customer of such Data Subject Access Request; and (b) not respond to such Data Subject Access Request, except on the documented instructions of Customer or as required by applicable Data Protection Laws. For the avoidance of doubt, Customer is responsible for responding to Data Subject Access Requests. Upon request, Perceptyx will provide reasonable assistance as necessary to enable Customer to respond to a Data Subject Access Request as required by applicable Data Protection Laws.

4.2. **Third Party or Government Requests.** If Perceptyx receives a Third Party Request, Perceptyx will, unless prohibited from doing so by applicable laws: (a) promptly notify Customer of such Third Party Request; and (b) not respond to such Third Party Request, except on the documented instructions of Customer or as required by applicable laws, in which case Perceptyx will to the extent permitted by such applicable laws provide prior notice to Customer of such legal requirement prior to responding to such Third Party Request. Upon request, Perceptyx will provide reasonable assistance to enable Customer to seek to limit, quash or respond to such Third Party Request.

4.3. **Consultations and DPIAs.** Upon request and subject to the information available to Perceptyx, Perceptyx will cooperate and provide commercially reasonable efforts to assist Customer with any data protection impact assessments and any prior consultations with any Supervisory Authority, which are required under applicable Data Protection Laws.

4.4. **Reimbursement.** Customer will reimburse Perceptyx in full for all extraordinary costs (as reasonably determined by Perceptyx) reasonably and properly incurred by Perceptyx in performing its obligations under this Section 4 (including internal costs and third party costs, including legal fees).

#### 5. RESTRICTED TRANSFERS OF PERSONAL DATA



5.1. Customer for itself and each Authorized Affiliate as relevant (each a “**Data Exporter**”) and Perceptyx for itself and its Affiliates as relevant, (each a “**Data Importer**”) hereby enter into the:

(i) SCCs as set forth in Annex 3 to this DPA, in respect of any Restricted Transfer, which will take effect upon the commencement of a Restricted Transfer by the Data Importer and Data Exporter. Appendix 1 to the SCCs shall be deemed to be pre-populated with the relevant sections of Annex 1 to this DPA and the processing operations are deemed to be those described in the Agreement. Annex 2 to the SCCs shall be deemed to be pre-populated with the relevant sections of Annex 2 to this DPA; and

(ii) UK Addendum as set forth in Annex 4 to this DPA, in respect of any UK Restricted Transfer, which will take effect upon the commencement of a UK Restricted Transfer by the Data Importer and Data Exporter. By accepting the SCCs, the Parties agree and accept the UK Addendum, as applicable.

(iii) Swiss Addendum as set forth in Annex 5 to this DPA, in respect of any Swiss Restricted Transfer, which will take effect upon the commencement of a Swiss Restricted Transfer by the Data Importer and Data Exporter. By accepting the SCCs, the Parties agree and accept the Swiss Addendum, as applicable.

5.2. To the extent Data Protection Laws other than the GDPR or UK GDPR apply to a Restricted Transfer, the Data Importer(s) will comply mutatis mutandis with terms of the Standard Contractual Clauses, as applicable to the Data Importer, the terms ‘Member State’ and ‘State’ are replaced throughout by the word “jurisdiction,” and “supervisory authority” will mean the relevant data protection regulator or other government body with authority to enforce Data Protection Laws.

## 6. DATA BREACH NOTIFICATION

6.1. **Notification Term.** Perceptyx will notify the Customer without undue delay after becoming aware of a Data Breach of Personal Data.

6.2. **Breach Information.** Perceptyx will, at the time of the notification or as soon as reasonably possible thereafter, provide the Customer with information (as available) to reasonably assist Customer to meet any obligations to report a Data Breach under applicable Data Protection Laws. Perceptyx will co-operate with Customer and take such reasonable steps as are agreed in good faith by the Parties to assist in the investigation, mitigation and remediation of each Data Breach. To the extent that Customer is responsible for a Data Breach, Customer will reimburse Perceptyx for all costs reasonably and properly incurred by Perceptyx performing its obligations under this Section (including internal costs and third party costs including legal fees).

## 7. SECURITY

7.1. Perceptyx will take appropriate steps to ensure the reliability of any employee, agent, contractor or any other person who may have access to the Personal Data, ensuring that such individuals are subject to confidentiality obligations or professional or statutory obligations of confidentiality.



7.2. Perceptyx will implement and maintain appropriate technical and organizational measures, as set forth in Annex 2 to this DPA, which are designated to provide a level of security appropriate to the risks presented by the Processing of the Personal Data, in particular from a Data Breach, and meet the requirements set forth in this DPA and by Data Protection Laws applicable to Perceptyx.

## 8. DELETION OF PERSONAL DATA

8.1. Except to the extent prohibited by applicable laws, Perceptyx will securely delete the Personal Data (a) as set forth in the Agreement, or (b) to the extent not otherwise set out in the Agreement, within 90 days after the termination or expiration of the Agreement. Upon request, Perceptyx will confirm in writing to Customer that the Personal Data has been deleted in accordance with this DPA.

8.2. If Perceptyx is required by applicable laws to retain any Personal Data, Perceptyx will take steps to (a) ensure the continued confidentiality and security of the Personal Data; (b) securely delete or destroy the Personal Data when the legal retention period has expired; and (c) not actively Process the Personal Data other than as needed for to comply with such applicable laws.

## 9. AUDIT

**9.1. Audit Reports.** Customer agrees that Perceptyx's then-current SOCII-type 2 audit reports (or comparable industry standard reports) and/or Perceptyx's ISO 27001 Certification will be used to satisfy any audit or inspection, request by or on behalf of Customer. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Perceptyx will make available a copy of the most recent certifications and reports, as applicable.

**9.2. Regulator Assistance.** In the event that Customer, a regulator, or data protection or Supervisory Authority requires additional assistance or additional information, including information necessary to demonstrate compliance with this DPA, or an audit related to the Service, such information, contribution and/or audit will be made available, provided Parties reach prior written agreement on scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Perceptyx to unreasonably delay performance of the audit in accordance with applicable Data Protection Laws.

## 10. AUTHORIZED AFFILIATES

10.1. **Authorized Affiliates.** Parties acknowledge and agree that, by entering into an agreement incorporating this DPA, (i) Customer enters into this DPA on behalf of itself and as agent for any Authorized Affiliate and (ii) the Parties are deemed to be signing and executing the applicable Standard Contractual Clauses and applicable appendices and annexes in their entirety as of the same date hereof. Customer represents and warrants that it has the authority and right to enter into this DPA and to instruct Perceptyx to Process the Personal Data as set forth hereunder, on behalf of itself and the Authorized Affiliate(s). All access to and use of the SaaS Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA,



and any violation of the terms and conditions of the Agreement by an Authorized Affiliate will be deemed a violation by Customer.

10.2. **Communication.** Customer is responsible for coordinating all communication with Perceptyx on behalf of its Authorized Affiliates with regard to this DPA. Customer represents that it is authorized to issue instructions as well as make and receive any communications or notifications in relation to this DPA on behalf of its Authorized Affiliates.

## 11. GENERAL PROVISIONS

11.1. **Termination.** The term of this DPA will end simultaneously and automatically with the termination of the Agreement (unless renewed or otherwise extended by the Parties in writing).

11.2. **Conflict.** This DPA supersedes any prior data processing agreements, data processing addenda or other terms addressing the subject matter of this DPA, between the Parties. In the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA will prevail with regard to the Parties' data protection obligations or the subject matter herein. In the event of inconsistencies between the provisions of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

11.3. **Governing Law.** Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses, the Parties hereby agree to submit to the choice of jurisdiction and venue set forth in the Agreement, with respect to any disputes or claims arising under this DPA.

11.4. **Limitation of Liability.** The aggregate liability of Perceptyx arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the limitations on liability in the Agreement.

11.5. **Changes in Data Protection Law.** If any variation is required to this DPA (including the Standard Contractual Clauses) as a result of a change in Data Protection Laws, either Party may provide written notice to the other Party of that change in Data Protection Law. The Parties will discuss and negotiate in good faith any necessary variations to this DPA to address such changes.

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

*(Signatures on following page)*



**This Data Processing Addendum is agreed to by authorized representatives of Perceptyx and Customer effective as of the last date below.**

**Customer**

**Perceptyx**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

Contact: \_\_\_\_\_

Contact: infosec@perceptyx.com

Customer DPO/EU Rep details if applicable:

\_\_\_\_\_



## Annex 1 to the DPA:

### Description of Processing

#### A. Activities/Purposes

Perceptyx will process the Personal Data for the following activities/purposes:

- Launching, administering, analyzing, and reporting on surveys
- Providing SaaS Services pursuant to the Agreement
- Other, please describe

N/A

#### B. Categories of Personal Data

For this purpose, Perceptyx will process the following categories of Personal Data:

Please include an overview of the categories of Personal Data which will be processed by Perceptyx, for example:

- Employee HR datafiles (basic details: e.g., full name, contact data: e.g. corporate telephone, corporate e-mail, work address; employment details: e.g., work center, job title, department, manager; academic and professional data: e.g., education, training / qualifications, professional experience
- Survey and assessment responses
- Analytics and reports prepared on behalf of Customer relating to employees and/or survey and assessment responses
- Special categories of data such as related to health, race or religion
- Other, please describe

N/A

#### C. Categories of Data Subjects

Perceptyx will process the following categories of Data Subjects for this purpose:

- Employees (including where applicable contractors, or other personnel)
- Suppliers
- Consultants and sales agents
- Others: please describe below

N/A



**D. Current Affiliates and other Subprocessors engaged by Perceptyx and/or its Affiliates**

Affiliate Name	Subprocessing Activity	Entity Country
Perceptyx, Inc.* *Applicable if Perceptyx, BV is contracting Party.	General services and support	USA

Subprocessor Name	Subprocessing Activity	Subprocessor Country
Amazon Web Services, Inc.	Cloud compute servers and storage	USA (EU storage subject to Agreement)
Call Experts, LLC	Customer support	USA
DataDog, Inc.	Infrastructure monitoring	USA
Google LLC	Incidental account administration	USA
Freshworks Inc.	Customer support	USA
Microsoft Corporation	Cloud compute servers and storage, and/or language translation of comments	USA
Mixpanel, Inc.	Analytics	USA
OKTA, Inc. (IaaS)	IDP MFA SSO SAML provider	USA
OpenAI, LLC* *Optional, used for Comment Copilot only	AI capabilities, including generative AI	USA



Responsive Translation Services (Clark Media Corp)	Language translation of survey questions	USA
Slack, Inc.	Incidental account administration	USA
Snowflake, Inc.	Data warehouse	USA
Splunk, Inc.	Security monitoring, logging and analytics	USA
Textline, Inc.	Customer support	USA
Twilio, Inc.	Text messages for launching surveys	USA



## **Annex 2 to the DPA: Security Controls**

This Annex 2 sets forth the minimum security requirements applicable to Agreement, the SaaS Services and the Processing of Personal Data pursuant to the DPA.

1. The technical and organizational security measures applicable to Personal Data will provide at least equivalent protections as Perceptyx applies to its own personal data and confidential information.
2. Perceptyx has implemented and will maintain a comprehensive, written information security program that materially conforms to the National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev 4. and ISO/IEC 27001:2013 information technology — security techniques — information security management systems — requirements. One or more designated qualified individuals will be responsible for maintaining Perceptyx information security program. Perceptyx will regularly review the information security program to identify and assess reasonably foreseeable internal and external risks to the privacy, security, and/or integrity of any electronic, paper, or other records containing Personal Data and to ensure that Perceptyx's information security program continues to comply with applicable Data Protection Laws.
3. Processing of Personal Data will take place on information processing systems for which commercially reasonable technical and organizational measures designed for protecting Personal Data have been implemented. Perceptyx will maintain reasonable and appropriate technical, physical, and administrative measures designed to protect Personal Data under its possession or control against unauthorized or unlawful Processing or accidental loss, destruction or damage in accordance with the applicable Data Protection Laws, taking into account the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage and sensitivity of the Personal Data.
4. Perceptyx will (a) take reasonable steps to ensure the reliability of employees, temporary workers, contractors and other personnel (collectively “**Personnel**”) having access to Personal Data, (b) limit access to Personal Data to those Personnel who have a business need to have access to such Personal Data and have received reasonable and appropriate privacy and security training; and (c) conduct background checks for employees and contractors with responsibilities for or access to Personal Data, to the extent permissible under applicable law.
5. **Minimum Controls.** Without limiting any other obligations herein, the following security controls will be implemented:
  - (a) policies, procedures and processes to manage the security risks related to Processing of Personal Data are documented and understood and reviewed and updated periodically;
  - (b) devices, systems, facilities and other assets (“**Assets**”) that access, store and Process Personal Data, as well as those that are material to the provision of the SaaS Services to the Customer, under this DPA are identified and managed;
  - (c) physical access to Assets is managed and controlled, including measures to prevent and detect unauthorized access to Assets, and access to Assets is limited to authorized users;
  - (d) security risk assessments are performed to identify and assess reasonably foreseeable internal and external security risks;



- (e) remote access by Personnel and others to Assets is restricted and securely managed with multi-factor authentication;
  - (f) Personal Data and related records are identified, and access is managed to protect the confidentiality, integrity and availability of such information;
  - (g) Personal Data is physically and logically separate from the data of other Perceptyx customers;
  - (h) monitoring tools are in place to allow for the review of unauthorized activity;
  - (i) electronic and paper records containing Personal Data are securely destroyed in accordance with secure destruction policies and procedures;
  - (j) appropriate technical security solutions are implemented and managed to protect the confidentiality, integrity and availability of Personal Data;
  - (k) critical operating system and software security patches will be installed in a timely manner on all devices used to Process Personal Data, and security-related fixes identified will be promptly installed;
  - (l) anti-malware software will be installed and configured to check for updates on a regular basis on all devices used to Process Personal Data;
  - (m) maintenance and repair of information system components is performed in a controlled and secure manner;
  - (n) Perceptyx's network and Assets are monitored to detect vulnerabilities, threats, anomalous or unauthorized activity and other potential cyber security events (collectively, "Events") in a timely manner;
  - (o) Personal Data will not be stored on any portable or removable media;
  - (p) Personal Data will not be stored or used in test or other non-production environments; and
  - (q) incident response processes and procedures are maintained and executed, to ensure timely response to detected Events, and the following activities take place according to such established processes and procedures: (i) Events are investigated, understood and categorized; (ii) activities are performed to contain an Event, mitigate its effects and address any remaining threat or vulnerability; (iii) Assets and Personal Data affected are restored, and other appropriate mitigating actions are taken; (iv) response and recovery activities are documented; and (v) policies and procedures are routinely reviewed and updated to incorporate lessons learned and address potential threats and vulnerabilities.
6. **Encryption and Infrastructure Protection.** Personal Data, including Personal Data on portable devices and backup media, will be encrypted in transmission and at rest, using industry-standard cryptographic techniques and secure management of keys.
7. **System Authentication and Authorization.** Access to Personal Data will be subject to secure user authentication protocols, including controls around user IDs, other identifiers, passwords, biometrics, authentication token devices, active account log-in procedures, log records that record access attempts and blocking after multiple unsuccessful log-in attempts.
- (a) Review of user access rights to systems containing Personal Data will be conducted regularly.
  - (b) Perceptyx will maintain electronic logs of persons accessing Personal Data depicting the



details of the access and transactional changes made. Such electronic logs must be provided to Customer for inspection upon reasonable request.

8. **Business Continuity.** Perceptyx will have in place appropriate business continuity and disaster recovery procedures for its business (the “**Business Continuity Plan**”) to ensure the continued performance of its obligations under this DPA and operational resilience generally, and will develop, test, and update the Business Continuity Plan regularly, in accordance with good industry practice.



## Annex 3 to the DPA:

### Standard Contractual Clauses

For Restricted Transfers, the SCCs will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

- (a) Module Two (Controller to Processor) of the SCCs will apply where Customer is a Controller of Personal Data and Perceptyx is processing such Personal Data on behalf of Customer;
- (b) Module Three (Processor to Processor) of the SCCs will apply where Customer is a Processor of Personal Data and Perceptyx is processing such Personal Data on behalf of Customer; and
- (c) For each module, where applicable:
  - (i) in Clause 7 of the SCCs, the optional docking clause will apply;
  - (ii) in Clause 9 of the SCCs, Option 2 will apply and the time period for prior written notice of Subprocessor changes will be as set forth in Section 3 (Subprocessors) of this Addendum;
  - (iii) in Clause 11 of the SCCs, the optional language will not apply;
  - (iv) in Clause 17 (Option 1) of the SCCs, the SCCs will be governed by the laws of Ireland; and
  - (v) in Clause 18(b) of the SCCs, disputes will be resolved by the courts of Ireland.

#### **On behalf of the data exporter:**

Name (written out in full): *Name as listed in the signature block of the DPA*

Position: *Title as listed in the signature block of the DPA*

Address: *Customer Address*

Other information necessary in order for the contract to be binding (if any):

Signature and Date: *Executed as of the Effective Date pursuant to Section 10.1 of the DPA*

#### **On behalf of the data importer:**

Name (written out in full): *Name as listed in the signature block of the DPA*

Position: *Title as listed in the signature block of the DPA*

Address: *Perceptyx Address*

Other information necessary in order for the contract to be binding (if any):

Signature and Date: *Executed as of the Effective Date pursuant to Section 10.1 of the DPA*



**APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES –  
DESCRIPTION OF THE PROCESSING**

**EXPLANATORY NOTE:**

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

**ANNEX I**

**A. LIST OF PARTIES**

**Data exporter(s):**

1. Data Exporter: *Customer*  
Address: *Customer Address*  
Contact person's name, position and contact details: *As listed in the signature block of the DPA*  
Activities relevant to the data transferred under these Clauses: *Described in Annex 1 to the DPA*  
Signature and date: *Executed as of the Effective Date pursuant to Section 10.1 of the DPA*  
Role (controller/processor): *Controller*
2. ...

**Data importer(s):**

1. Name: **Perceptyx**  
Address: *Perceptyx Address*  
Contact person's name, position and contact details: *As listed in the applicable agreement or as otherwise specified*  
Activities relevant to the data transferred under these Clauses: **Described in Annex 1 to the DPA.**  
Signature and date: Executed as of the Effective Date pursuant to Section 10.1 of the DPA  
Role (controller/processor): *Processor*
2. ...

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred.*

**Are set forth in Annex 1 to the DPA.**



*Categories of personal data transferred.*

**Are set forth in Annex 1 to the DPA.**

*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.*

**Are set forth in Annex 1 to the DPA.**

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

**One-off**

**Continuous**

**Other: Personal Data is transferred whenever the Customer submits Personal Data for the purposes of receiving the SaaS Services under the Agreement.**

*Nature of the processing.*

**Is set forth in Annex 1 to the DPA.**

*Purpose(s) of the data transfer and further processing.*

**As set forth in Annex 1 to the DPA.**

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

**Retention periods vary, subject to Section 8.2 of the DPA and are generally determined by the Customer via the processing instructions, unless otherwise required by applicable law.**

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

**Perceptyx uses the Subprocessors set out in Annex 1 to the DPA for subprocessing activities both as listed under Annex 1 to the DPA Section D (as that list may be updated from time to time and posted at <https://go.perceptyx.com/legal-perceptyx-sub-processors> in accordance with the DPA) for as long as the SaaS Services are provided to the Customer.**

## **C. COMPETENT SUPERVISORY AUTHORITY**

For the purposes of the Standard Contractual Clauses, the supervisory authority that shall act as competent supervisory authority is either (i) where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR; (ii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Customer's representative is established; or (iii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the Data Subjects are predominantly located. In relation to Personal Data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as applicable).



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

*The minimum security requirements applicable to the processing of personal data by the data importer(s) hereunder are set forth in Annex 2 to the DPA (Security Controls).*



**Annex 4 to the DPA:  
International Data Transfer Addendum to the SCCs**

For UK Restricted Transfers, the UK Addendum will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

**Part 1: Tables**

**Table 1: Parties**

<b>Start date</b>	The day of the last signature of Annex I of the EU SCCs.	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	Full legal name: See Annex I of the EU SCCs Trading name (if different): Main address (if a company registered address): See Annex I of the EU SCCs Official registration number (if any) (company number or similar identifier):	Full legal name: See Annex I of the EU SCCs Trading name (if different): Main address (if a company registered address): See Annex I of the EU SCCs Official registration number (if any) (company number or similar identifier):
<b>Key Contact</b>	Contact details including email: See Annex I of the EU SCCs	Contact details including email: See Annex I of the EU SCCs
<b>Signature (if required for the purposes of Section 2)</b>	See Annex I of the EU SCCs	See Annex I of the EU SCCs

**Table 2: Selected SCCs, Modules and Selected Clauses**

<b>Addendum EU SCCs</b>	<input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: The day of the last signature of Annex I of the EU SCCs. Reference (if any): Annex 3 (EU SCCs) to the DPA
-------------------------	---



	Other identifier (if any): N/A
--	--------------------------------

**Table 3: Appendix Information**

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

Annex 1A: List of Parties: Annex I of the EU SCCs
Annex 1B: Description of Transfer: Annex I of the EU SCCs
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex 2 of the DPA
Annex III: List of Subprocessors (Modules 2 and 3 only): Annex 1.D of the DPA

**Table 4: Ending this Addendum when the Approved Addendum Changes**

<b>Ending this Addendum when the Approved Addendum changes</b>	Which Parties may end this Addendum as set out in Section 19: <input checked="" type="checkbox"/> Importer <input type="checkbox"/> Exporter <input type="checkbox"/> neither Party
--	--

**Annex 5 to the DPA:  
Swiss Addendum to the SCCs**

Insofar as the data transfer under the DPA is governed by the FADP, and further provided that none of these amendments will have the effect or be construed to amend the Standard Contractual Clauses in relation to the processing of Personal Data under to the GDPR, the following shall apply:

1. Competent supervisory authority in Annex I.C under Clause 13 of the SCCs: The Swiss Federal Data Protection and Information Commissioner (the “**FDPIC**”);
2. Applicable law for contractual claims under Clause 17 of the SCCs: As set forth in the SCCs, subject to #4, below;
3. Place of jurisdiction for actions between the Parties pursuant to Clause 18(b) of the SCCs: As set forth in the SCCs, subject to #4, below;
4. The term “member state” must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs;
5. References to the “GDPR” should be understood as references to the “FADP;” and
6. Where the FADP protects legal entities as data subjects, the SCCs will apply to data relating to identified or identifiable legal entities.

