**CHRONUS LLC**

**GLOBAL DATA PROCESSING ADDENDUM**

**Last updated**: March 15, 2023

This Global Data Processing Addendum ("**DPA**") applies where Chronus LLC and you (**"Customer**") have entered into one or more Agreements for the Services, pursuant to which Chronus LLC and/or its Affiliates (collectively, "**Chronus**") process(es) Personal Data for the purpose of providing the Services to Customer. This DPA is incorporated into and made subject to the Agreement. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. **Signatures of assent of Chronus and Customer to the Agreement will be deemed signature to, and acceptance and agreement of, this DPA and the SCCs incorporated hereto.**

1. **DEFINITIONS**. In this DPA, the following initially capitalized words have the meanings set out below.
    1. "**Affiliate(s)**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with a Party to this DPA. "Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" will be construed accordingly.
    2. "**Agreement**" means the written or electronic agreement(s) (including order forms) between Customer and Chronus for the provision of the Services to Customer which reference this DPA.
    3. "**Data Protection Laws**" means any data privacy, security or protection laws or regulations to the extent applicable to the processing of Personal Data under this DPA (including any binding laws or regulations ratifying, implementing, adopting, supplementing, or replacing the foregoing) in each case to the extent in force and as such are updated, amended or replaced from time to time.
    4. "**Data Subject Request**" means a request from a Data Subject to exercise their data subject or consumer rights under Data Protection Laws.
    5. "**Instructions**" means Customer's written instructions to Chronus to process the Personal Data as provided under the Agreement, this DPA, through Customer's use of the features and functionality of the Services or as otherwise mutually agreed by authorized signatories of both parties in writing.
    6. "**Personal Data**" means any data which (i) qualifies as "Personal Data" "Personal Information" "Personally Identifiable Information" or any substantially similar term under Data Protection Laws and (ii) is processed by or on behalf of Chronus its role as a Data Processor or Service Provider in connection with the provision of the Services to Customer.
    7. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Chronus' possession or otherwise under Chronus' control (including when transmitted or stored by Chronus).

8. "**Personnel**" means any employees, agents, officers, consultants, or other personnel of Chronus who are authorized to process Personal Data under the authority of Chronus.
9. "**Services"** means the services provided by Chronus to Customer as defined and described under the Agreement.
10. "**Standard Contractual Clauses**" or "**SCCs**" means the (i) the standard contractual clauses for international transfers published by the European Commission on June 4, 2021 governing the transfer of European Area Personal Data to Third Countries as adopted by the European Commission, and the Swiss Federal Data Protection and Information Commissioner ("Swiss FDPIC") relating to data transfers to Third Countries (collectively "**EU SCCs**"); (ii) the international data transfer addendum ("UK Transfer Addendum") adopted by the UK Information Commissioner's Office ("UK ICO") for data transfers from the UK to Third Countries; or (iii) any similar such clauses (as applicable) adopted by a data protection regulator relating to data transfers to Third Countries; or (iv) any successor clauses to (i) – (iii).
11. "**Subprocessor**" means any person or entity appointed by or on behalf of Chronus in connection with the processing of Personal Data.
12. "**Third Country**" means countries that, where so regulated by Data Protection Laws, have not received an adequacy decision from an applicable authority relating to international data transfers, including regulators such as the European Commission, UK ICO, or Swiss FDPIC.
13. In this DPA, the following terms (and any substantially similar terms as defined under Data Protection Law) shall have the meanings and otherwise be interpreted in accordance with Data Protection Law: **Business, Controller, Data Controller, Data Processor**, **Data Subject, Processor, Sell, Sale, Share, Service Provider, process(ing)** and

2. **SCOPE OF DPA.**
    1. **Scope.** This DPA applies where and solely to the extent that Chronus processes Personal Data on behalf of Customer. Chronus shall process such data solely for the "Business Purposes" as further defined and set forth in Exhibit 1. The subject-matter and duration of the processing, nature and purpose of the processing, types of Personal Data and categories of the Data Subjects are as set out in Exhibit 1 attached hereto, which is hereby incorporated by reference.
    2. **Role of the Parties.** As between Chronus and Customer, Customer is the Data Controller and Business of the Personal Data and Chronus is the Data Processor and Service Provider of the Personal Data, except where Customer is the Data Processor of the Personal Data, in which case Chronus is a subprocessor of Customer with respect to the Personal Data.
    3. **Compliance with Data Protection Laws**. Each party will comply with its obligations under Data Protection Laws in connection with the processing of Personal Data. In connection with its access to and use of the Services, Customer shall process Personal Data within such Services and provide Chronus with Instructions in accordance with Data Protection Laws.

3. **CUSTOMER OBLIGATIONS.**
    1. **General.** Customer represents and warrants to Chronus that: (i) it shall comply with its obligations under Data Protection Law(s) in respect of its processing of Personal Data and any processing Instructions it issues to Chronus; and (ii) Customer will remain duly and effectively authorized to give the Instructions.
    2. **Data Quality and Integrity.** Customer acknowledges and agrees that Customer is solely responsible for the accuracy, quality, and legal compliance relating to the processing of Personal Data as detailed under the Instructions and that Chronus has no control over the nature, scope, or origin of, or the means by which Customer acquires Personal Data processed by the Services.
    3. **Notice and Choice.** Customer acknowledges and agrees that Customer is solely responsible for providing its end-users with appropriate notice regarding its processing activities. Where required by Data Protection Laws, Customer is solely responsible for obtaining, and represents and covenants that it has obtained or will obtain prior to processing by Chronus, all necessary consents, licenses, or approvals for the processing, and that Customer otherwise has a valid legal basis under Data Protection Laws for the processing of Personal Data as detailed under this DPA.

4. **CHRONUS OBLIGATIONS.**
    1. **Instructions.** Without limiting the foregoing Section 3, Customer instructs Chronus (and authorizes Chronus to instruct its Personnel and Subprocessors) to process (including internationally transfer) Personal Data in accordance with the Instructions. Except as expressly permitted by the Customer or Data Protection Law, Chronus shall not retain, use, or disclose the Personal Data (i) for any purpose other than the Business Purpose; or (ii) outside of the direct business relationship with the Company unless expressly permitted by Data Protection Laws.
    2. **Infringing Instructions; Contrary Laws**. Chronus shall only process (including transfer) the Personal Data in accordance with the Instructions and shall promptly inform Customer if, in its reasonable opinion, the Instructions violate Data Protection Laws. Chronus will notify Customer in the unlikely event that Data Protection Law requires Chronus to process Personal Data other than pursuant to the Instructions (unless prohibited from doing so by applicable law).
    3. **Restrictions on Selling, Sharing or Combining Personal Data; Unauthorized Processing**. Chronus shall not Sell or Share Personal Data. Further, Chronus shall not combine Personal Data with personal data which Chronus receives from or on behalf of another person or persons, or collects from its own interactions with an individual except where: (i) expressly required to perform the Services, (ii) if combined, such combination does not result in a Sale of Personal Data, or change Service Provider's status as a Service Provider (or Processor) with respect to the Personal Data; and (iii) as expressly permitted by Data Protection Laws. Where and to the extent required by Data Protection Laws: (i) Chronus certifies that it understands the foregoing restrictions and will comply with them; and (ii) Chronus shall allow Customer, upon reasonable notice to Chronus, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data.
    4. **Security Measures.** Chronus shall implement and maintain reasonable and appropriate technical and organizational measures and practices designed to ensure

an appropriate level of security, confidentiality, availability, and integrity of Personal Data from unauthorized access, destruction, use, modification, or disclosure. Such measures shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the likelihood and severity of risk to the rights and freedoms of individuals and the nature of the activities under the Agreement and shall, at a minimum, include the security measures as specified in Chronus' Information Security Management System Policy set forth in Exhibit 2.

5. Chronus will not disclose or transfer Personal Data to any third-party without the prior written consent of Customer except as required by Data Protection Laws or as otherwise permitted by this DPA or the Agreement.
6. **Legally Compelled Disclosure.** If a law enforcement agency sends Chronus a demand for Personal Data (for example, through a subpoena or court order), Chronus will attempt to redirect the law enforcement agency to request such Personal Data directly from Customer. As part of this effort, Chronus may provide Customer's basic contact information to the law enforcement agency. Chronus will only disclose Personal Data in response to a demand for Personal Data where legally compelled to do so, in which case Chronus will (as legally permissible) give Customer reasonable notice of the demand to allow Customer to seek a protective order or another appropriate remedy.
7. **Personal Data Breaches.** Chronus shall notify Customer without undue delay (and within any legally required timeframes under Data Protection Laws) upon Chronus' confirmation of a Personal Data Breach. In the event of a Personal Data Breach Chronus will, taking into account the nature of the processing and the information reasonably available to Chronus: (i) provide Customer with sufficient information, as it becomes known to Chronus as required under Data Protection Laws; (ii) take such steps as Chronus, in its sole discretion, deems necessary and reasonable to remediate such Personal Data Breach (to the extent that remediation is within Chronus' reasonable control); and (iii) provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Data Protection Laws with respect to notifying relevant regulators and/or data subjects affected by such Personal Data Breach. Chronus' obligation to report or respond to a Personal Data Breach under this Section is not and will not be construed as an acknowledgement by Chronus of any fault or liability with respect to the Personal Data Breach. Unless prohibited by an applicable statute or court order, Customer will notify Chronus of any third-party legal process relating to any Personal Data Breach, including, but not limited to, any legal process initiated by any governmental entity.
8. **Return of Personal Data.** Chronus will return Personal Data to Customer by permitting Customer to export Personal Data from the Services at any time during the Term using then-existing features and functionality of the Services. Customer is solely responsible for its data retention obligations with respect to Personal Data. On Customer's request, if and to the extent Customer cannot delete and/or overwrite Personal Data stored on Chronus' systems using the then-existing features and functionality of the Services, Chronus shall delete or return to Customer, in accordance with Data Protection Laws, any Personal Data in its possession or control. Thereafter, Chronus will promptly delete Customer's Tenant(s) (and any data

remaining on such Tenants) and any other Personal Data retained by Chronus, if any, provided that Chronus is not obligated to delete copies of Personal Data retained in automated backup copies or archival copies generated by Chronus, which Chronus will retain for up to, and delete within, ninety (90) days from their creation. "**Tenant**" means a logical isolation unit, or dedicated share of a particular instance of the Services. Such backup and archival copies will remain subject to this DPA and the Agreement until they are destroyed. Customer will bear and pay for all costs incurred by Chronus in connection with return or deletion of Personal Data that Customer requires Chronus to perform that it outside the scope of Chronus' customary data retention policies.

9. At Customer's expense and solely as required by Data Protection Laws Chronus will provide Customer with reasonable cooperation and assistance to: (i) support Customer's compliance with Customer's obligations under Data Protection Laws; (ii) (upon Customer's reasonable written request) carry out a data protection impact assessment (or similar risk assessment as required under Data Protection Laws) related to Customer's use of the Services to the extent the information is available to Chronus and Customer is unable to access such information necessary to perform the assessment without Chronus' cooperation; and (iii) to comply with a Data Subject Request. If and to the extent that Customer is unable to respond to a Data Subject Request by using the features and functionality of the Services, Chronus shall, upon Customer's written request, provide Customer with commercially reasonable cooperation and assistance in fulfilling Customer's obligations to respond to Data Subject Requests.
10. **Complaints**. Chronus will promptly notify Customer in writing and without undue delay if Chronus receives any complaint or inquiry relating to the processing of Personal Data hereunder, including allegations that the processing infringes on any individual's or third party's rights. Chronus will not respond to any such request or complaint unless Chronus is required to respond under Data Protection Laws.

5. **CHRONUS PERSONNEL AND SUBPROCESSORS.**
    1. **Instructions.** Chronus shall require its Subprocessors and Personnel to process Personal Data solely in accordance with the Instructions, unless otherwise required by Data Protection Laws (in which case Chronus shall notify the Customer).
    2. Chronus may disclose or transfer Personal Data to Chronus Personnel and Subprocessors solely for the Business Purpose. Chronus shall ensure that Chronus' Subprocessors and Personnel are subject to confidentiality obligations with respect to the Personal Data.
    3. **Training**. Chronus shall ensure that Personnel have received data privacy and security training appropriate to the nature of their processing of Personal Data and the requirements of Data Protection Laws.
    4. **General Authorization to Subprocess**. Customer hereby authorizes Chronus' use of, and transfer of Personal Data to, the Subprocessors currently listed at https://chronus.com/subprocessors (the "**Subprocessor List**") for the processing of Personal Data for the Business Purpose. Chronus will provide reasonable prior notice to Customer via email if Chronus intends to make any changes concerning the addition or replacement of any Subprocessors, including details regarding the

location and processing of Personal Data, and Chronus will update the Subprocessor List and make such updated version available to Customer prior to such authorization of the Subprocessor. If within thirty (30) business days of receipt of such notice, Customer objects, in writing, on reasonable grounds relating to data protection, to Chronus' appointment of a new Subprocessor, the parties will discuss such concerns in good faith with a goal of achieving resolution. If Customer does not timely object to the engagement of a new Subprocessor in accordance with this Section, that new Subprocessor will be deemed authorized for the purposes of this DPA.

5. **Chronus' Obligations**. Chronus shall ensure that all Subprocessors are bound by written agreements which are no less protective of the Personal Data than this DPA (including with respect to subprocessing by Subprocessors). Chronus will remain liable for any breach of its obligations under this DPA that is caused by an act or omission of a Subprocessor.
6. If Customer and Chronus have entered into the SCCs, the above authorizations will constitute Customer's prior written consent to the subcontracting by Chronus of the processing of Personal Data if such consent is required under the SCCs.

6. **INTERNATIONAL TRANSFER OF PERSONAL DATA.**
   1. **General Authorization to International Transfer.** Customer acknowledges and agrees that Chronus and its Subprocessors may: (i) provide the Services from any state, province, country or other jurisdiction; and/or (ii) transfer and process Personal Data from any location where Chronus or its Subprocessors maintain data processing operations. Chronus will at all times provide an adequate level of protection for the Personal Data processed, in accordance with the requirements of Data Protection Laws and, to the extent applicable, the requirements below.
   2. **Onward Transfers.** In connection with the provision of the Services to Customer, Chronus may (and may authorize its Subprocessors to) receive from, transfer to, or process Personal Data within, any Third Country provided that Chronus and its Subprocessors take measures to adequately protect such data consistent with Data Protection Laws. Such measures may include, to the extent available and applicable under such Data Protection Laws:

- SCCs. The parties' agreement to enter in to and comply with the SCCs which are hereby incorporated into this DPA and as further set forth in Schedule 1. For the sake of clarity, signatures of assent of Chronus and Customer to the Agreement will be deemed signatures to the SCCs;
- BCRs. Processing in compliance with Binding Corporate Rules in accordance with Data Protection Laws; or
- Other Approved Transfer Mechanisms. Implementing any other data transfer mechanisms or certifications approved under Data Protection Laws, including, as applicable, any approved successor or replacement to the EU-US Privacy Shield framework or the Swiss-US Privacy Shield framework.

To the extent that any substitute or additional appropriate safeguards or transfer mechanisms under Data Protection Law are required to transfer data to a Third Country,

the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA.

3. **European Personal Data Transfers**.
   - **European Personal Data Transfers**. Transfers of Personal Data from the European Union, European Economic Area, Switzerland, or the United Kingdom of Great Britain and Northern Ireland ("**UK**") by Customer to Chronus or Chronus to Customer in Third Countries are subject to the Standard Contractual Clauses, Module Two ("**Controller to Processor**"), and Module Three ("**Processor to Processor**") attached to this DPA and incorporated by reference. The information required for the purposes of the Standard Contractual Clauses is provided in Schedule 1 ("**Description of Processing and Transfer Detail**s") to this DPA. The Parties agree that the Standard Contractual Clauses are incorporated into this DPA without further need for reference, incorporation, or attachment and that by executing this DPA, each party is deemed to have executed the Standard Contractual Clauses.

1. **Swiss Personal Data Transfers**. For international transfers of Personal Data subject to Data Protection Laws in Switzerland, the Standard Contractual Clauses shall be read to be modified as follows as applicable:
   1. References to "Regulation (EU) 2016/679" and any articles therefrom shall be interpreted to include references to the Swiss FDPIC; and
   2. References to "EU", "Union" and "Member State" shall be interpreted to include references to "Switzerland."

1. **UK Personal Data Transfers**. For international transfers of Personal Data subject to Data Protection Laws in the UK and transferred in accordance with the UK Transfer Addendum, the Parties agree as follows:

1. Each Party agrees to be bound by the terms and conditions set out in the UK Transfer Addendum, in exchange for the other Party also agreeing to be bound by the UK Transfer Addendum.
2. The Standard Contractual Clauses will be interpreted in accordance with Part 2 of the UK Transfer Addendum.
3. Sections 9 to 11 of the UK Transfer Addendum override Clause 5 (Hierarchy) of the EU SCCs

1. For the purposes of Section 12 of the UK Transfer Addendum, the EU SCCs will be amended in accordance with Section 15 of the UK Transfer Addendum.
2. Information required by Part 1 of the UK Transfer Addendum is provided as Schedule 1 to this DPA.
3. To the extent that any revised transfer addendums or mechanisms are issued by the UK ICO, the Parties agree to incorporate such revisions in accordance with Section 18-20 of the UK Transfer Addendum.

4. Supplementary Measures to the SCCs. To the extent required by Data Protection Laws, in cases where transfer of Personal Data to Third Countries requires supplemental measures above and beyond those outlined under this DPA, the parties agree to implement such supplementary measures as may be required on a case-by-case basis.

7. **AUDITS AND RECORDS**.
    1. **Customer assurance.** To the extent required by Data Protection Laws Chronus grants Customer the right to take reasonable and appropriate steps, as such steps are further defined by Data Protection Law, to ensure that Chronus uses the Personal Data in a manner consistent with Customer's obligations under Data Protection Laws.
    2. **Provision of Information**. To the extent required by Data Protection Laws and solely upon reasonable Customer request, Chronus shall make available to Customer the information in Chronus' control which is necessary to demonstrate its compliance with Data Protection Laws.
    3. **Audit Right**. To the extent required by Data Protection Laws and solely upon reasonable Customer request, Chronus shall allow and cooperate with audits or assessments of the data-processing facilities in Chronus' control for the processing activities covered by this DPA. Audits shall occur no more than once a year (unless required otherwise by Data Protection Laws) and shall be carried out by Customer or by third party auditors who are bound by a duty of confidentiality at least as restrictive as the terms of confidentiality set forth in the Agreement.

8. **LIMITATION OF LIABILITY.**
    1. Chronus' entire liability arising out of or related to this DPA (including under the SCCs), whether in contract, tort or under any other theory of liability, is subject to the limitations and exclusions of liability contained in the Agreement. For the avoidance of doubt, Chronus' total liability for all claims from Customer and all of its users arising out of or related to the Agreement and this DPA will apply in aggregate for all claims under both the Agreement and this DPA. Nothing in this DPA will limit Chronus' liability with respect to bodily injury or death or any other liability or loss which may not be limited under Data Protection Laws.

9. **MISCELLANEOUS.**
    1. This DPA is expressly incorporated into and amends each of the Agreements.
    2. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless otherwise provided by this DPA or required by Data Protection Laws. This DPA constitutes and embodies the entire agreement and understanding between the parties with respect to the subject matter hereof and supersedes all prior or contemporaneous written, electronic, or oral communications, representations, agreements or understandings between the parties with respect thereto. This DPA is without prejudice to the rights and obligations of the parties under the Agreement which will continue to have full force and effect.
    3. This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. Other than in respect of statements made fraudulently, no other representations or terms will apply or form part of this DPA.

4. Except as otherwise provided under this DPA or required by Data Protection Laws: (i) a person who is not a party to this DPA will not have any rights under this DPA (including under the Contracts (Rights of Third Parties) Act 1999) to enforce any term of this DPA; and no one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.
5. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict so far as the subject matter concerns the processing of Personal Data. In the event of any conflict or inconsistency between the terms of this DPA and the terms of the SCCs, then, only insofar as the SCCs apply, the SCCs shall prevail.
6. The provisions of this DPA are severable. If any phrase, clause, or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.
7. Chronus may update the terms of this DPA from time to time; provided, however, Chronus will provide at least thirty (30) days' prior written notice to Customer (which may be via email to the primary Customer contact) when an update is required as a result of (a) changes in Data Protection Laws; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Services. The then-current terms of this DPA are available at https://chronus.com/data-processing-agreement.

# Exhibit 1

### Description of Processing Activities and Data Transfers

1. **Data Exporter**

| Company Name | Address | Contact name, position, and contact information | Role |
|---|---|---|---|
| As provided under the Agreement. | | | Controller |

2. **Data Importer**

| Company Name | Address | Contact name, position, and contact information | Role |
|---|---|---|---|

| | | |
|---|---|---|
| Chronus LLC | 450 Alaskan Way South, Suite 200, Seattle, WA 98104 Sabarish Sankar, Data Protection Officer<br>legal@chronus.com | Processor |

3. **Activities relevant to the data transferred under the SCCs.**

The activities relevant to the data transferred at the Services more fully described in the Agreement and applicable Orders.

4. **Details of Personal Data processing and transfer**

| | |
|---|---|
| **Categories of Data Subjects** | Data exporter's, its affiliates', and its and their respective service providers' employees, consultants, agents, and representatives authorized by data exporter to use the Services. |
| **Categories of Personal Data** | Data exporter may submit personal data to data importer which may include, but is not limited to, the following categories of personal data:· **Identifiers and commercial information such as:** (a) first and last name; (b) title; (c) position; (d) employer; € email, phone, physical business address;· **Internet or other electronic network activity information** (including IP address); and· any other personal data that data exporter chooses to provide to the Services in accordance with the Agreement and DPA. |
| **Sensitive Personal Data** | The Services do not require, nor does Chronus recommend the use of Sensitive Personal Data. However, Sensitive Personal Data may be processed as determined by Customer in its sole discretion |
| **Frequency of transfers** | Continuous |
| **Nature and purpose of Personal Data transfer and further processing** | The nature and purposes of Processing carried out by Chronus shall be as set out in the Agreement, and includes the provision, maintenance and securing of the Services by Chronus, including the following Business Purposes: – Performing services on behalf of Customer (including maintaining or servicing accounts, providing customer service, processing, or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, or providing similar services on behalf of the Customer);– Debugging to identify and repair errors that impair existing and intended functionality;– Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity; and– Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards. Chronus may also use the Personal Data for internal use to build or improve the quality of the Services, to retain and employ another Subprocessor (or service provider) or as otherwise explicitly set forth under the Agreement. |

| | |
|---|---|
| **Period for which the Personal Data will be retained or criteria used to determine that period** | The period for which the Personal Data will be retained is more fully described in the Agreement, DPA, and accompanying Order Forms. |
| **Subprocessor transfers – subject matter, nature, and duration of processing** | The subject matter, nature, and duration of the Processing as more fully described in the Agreement, DPA, and accompanying Order Forms as well as Chronus' Subprocessor List currently available at https://chronus.com/subprocessors.. |

## 5. Signatures

| | |
|---|---|
| **Signatures** | Signatures of assent of Chronus and Customer to the Agreement will be deemed signature to the SCCs incorporated hereto. |

## 6. European Area SCC and UK Transfer Addendum Information

| **SCC Clause** | **GDPR** | **Swiss DPA** | **UK Data Protection Law** |
|---|---|---|---|
| **Module in Operation:** Module Two (Controller to Processor) and Module Three (Processor to Processor) | | | |
| **Clause 7- Docking Clause** | An entity that is not a party to these Standard Contractual Clauses may, with the agreement of the parties, accede to these Standard Contractual Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 1.A of the Standard Contractual Clauses. | | |
| **Clause 9(a)- Use of Sub-processors** | **GENERAL WRITTEN AUTHORISATION**: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 calendar days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object. | | |
| **Clause 11 (Redress)** | Optional language in Clause 11 shall not apply. | | |

| | | | |
|---|---|---|---|
| **Clause 17- Governing Law** | These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland. | These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland. | These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of England and Wales. |
| **Clause 18 – Choice of Forum and Jurisdiction** | The parties agree that those shall be the courts of Ireland. | The parties agree that those shall be the competent courts of Switzerland. | The parties agree that those shall be the competent courts of England and Wales. |
| **Annex 1A- List of Parties** | The name, address, and contact person's name, position, and contact details, and each party's role in processing Personal Data are provided in Section 1, 2, and 3 above | | |
| **Annex 1B – Description of Transfer** | This information can be found in Section 4 above. | | |
| **Clause 13 and Annex 1C – Competent Supervisory Authority** | Identify the competent supervisory authority/ies in accordance with Clause 13:Irish Data Protection Commission | Identify the competent supervisory authority/ies in accordance with Clause 13:FDPIC | Identify the competent supervisory authority/ies in accordance with Clause 13:UK Informational Commissioner |
| **Annex II – Technical and Organizational Measures** | The description of technical and organization measures designed to ensure the security of Personal Data is described more fully in Exhibit 2 of this DPA. | | |
| **Annex III – List of Subprocessors** | See Subprocessors currently listed at https://chronus.com/subprocessors. | | |
| **Ending the UK Transfer Addendum when the Approved Addendum changes** | N/A | | Which Parties may end this Addendum as set out in Section 19:☒Importer☒Exporter□neither Party |

# Exhibit 2

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

Chronus Information Security Management System Policy

## 1. Purpose

This Exhibit 2 is the Information Security Management System Policy (the "**ISMS policy**") for Chronus.

## 2. Security Measures

### 1. **ISO 27001:2013 Domains**

This ISMS policy has the following domains aligned with ISO 27001:2013 as listed below. These domains are subject areas in which management controls are defined, applied, and governed in the Information Security Management System (ISMS). The following table describes these domains.

| **Policy Domain** | **Summary** |
|---|---|
| Information Security Management System (ISMS) | The ISMS provides the framework of principles, policies, standards, and guidelines for the effective management of Information Security initiatives. |
| Human Resources Security | The Company will establish processes and responsibilities relating to information security during the recruitment process, employment, and separation. Security checks will be conducted prior to employment and all employees will receive security awareness training upon induction, and at least annually thereafter. |
| Asset Management | IT assets, including hardware, software and data will be identified and classified and asset inventories will be maintained. The Company will classify and handle all information assets and will dispose of records in accordance with the Company's Disposal and Destruction policy. |
| Access control | Methods and controls to manage logical access to sensitive data to protect confidentiality of information as well as integrity and availability requirements. Access to Company information and systems must be:15.1. Attributable to a uniquely identifiable individual who is responsible for actions performed with their system account.15.2. Based on the requirements of the individual's role15.3. Managed by passwords, according to password policy formally authorised by asset owners, routinely revalidated, and removed if no longer required |

| | |
|---|---|
| Cryptography | Methods and controls for ensuring data will be secured during transmission, or storage through appropriate encryption processes. Includes methods and processes for managing keys, software, and other artefacts. |
| Physical and Environmental Security | Appropriate physical controls will protect information assets against loss, physical abuse, unauthorized access, and environmental hazards. These will include perimeter security controls, physical access controls, fire, and power protection controls. |
| Operations Security | Methods and controls that balance the need for IT Operations professionals to have privileged access to systems and networks with the requirement to maintain secure access and confidentiality of data. Management and operation of computers and networks shall be commensurate with the business risk and value of the information assets. Access into networks will be granted on an individual user and application basis using authorized devices and secured pathways. |
| Communications Security | Methods and controls to manage the secure transmission of information to ensure confidentiality of sensitive data and to minimize the risk of data loss or leakage.Systems and networks will be segregated according to their respective information security risks and use appropriate control mechanisms such as firewalls/gateways, physical isolation, and encryption. |
| System acquisition, development, and maintenance | Information security controls will be specified and included as an integral part of the software development and implementation process. Security requirements will be identified prior to the development or procurement of IT systems, documented in business requirements, validated, and tested prior to implementation, and regularly throughout the systems lifecycle. |
| Supplier Relationships | The Company will implement security controls and processes to manage supplier access to information assets. Suppliers and vendors will be given access privileges only at the level required to deliver contracted services and contracts must comply with information security policies. |
| Information security incident management | The Company will apply a consistent and effective approach to the management of information security incidents. Procedures that define the course of action when a security incident is identified will be documented and made available to all employees. |
| Business Continuity | The application of business continuity management shall minimize disruption to CQU operations, defining the approach to resilience, disaster recovery and general contingency controls. Continuity plans shall align with the Company’s Business Continuity Management Framework. |
| Project Management | Project proposals must include a high-level risk assessment and review of the types and confidentiality levels of information the project will utilize and manage. New systems will be reviewed by the DISO prior to implementation via the change management process. |

| | |
|---|---|
| Data Assurance | The Company will ensure that all reasonable steps are taken to monitor, review and audit information security effectiveness. This will include the assignment of security roles, maintenance of policies and processes and reporting of non-compliance. |
| Data Breach Reporting | The Company has formal processes in place to manage a data breach and the mandatory notifications that are required under the appropriate regulations |

## 2.2. Logical Access

Access to Chronus' systems and information is controlled to protect its confidentiality, integrity, and availability. Accordingly, access is restricted to those with a 'need to know' and is reviewed periodically to ensure appropriate access is maintained. Access credentials must meet specific minimum requirements, depending on the subject system, to reduce the risk of unauthorized access.

## 2.3. Business Continuity

Chronus has global presence and offers several SaaS products to its customers. The implementation of an effective Business Continuity policy ensures preparations are made to identify risks which may affect Chronus' ability to operate during an incident and recover quickly in the aftermath. Business continuity plans and processes are regularly reviewed and tested to ensure effectiveness.

## 2.4. Information Classification, Handling and Retention

Information assets created, stored, and used within Chronus have value, which are identified by the asset owner or creator to allow the appropriate security controls to be applied. Additionally, information processed for customers in Chronus SaaS products are classified according to its value to the customer.

All employees protect information according to the data classification assigned to it. Access to all classified information is based on the Need-to-Know principle. Employees access data when strictly required.

## 2.5. Security Incident Management

All Chronus employees know how to identify and report a security incident and must be fully familiar with their involvement in the incident management process. Chronus' security incident management processes must be in place and tested.

## 2.6. Cryptography

Chronus uses cryptography to protect logical assets. Cryptographic solutions are employed correctly, and cryptographic keys are managed to ensure their availability.

## 2.7. Vendor Management

Vendors having access to Chronus customers data implement appropriate controls to protect services and information. Vendor contracts also include a set of minimum expected security requirements for protecting Chronus assets and information.

## 2.8. Secure Software Development

Application source code and algorithms developed by Chronus are considered intellectual property. Such information is accessible on a need-to-know basis and requires specific security controls.