111 Congress Avenue
Suite 900
Austin, TX 78701

info@csdisco.com
833-653-4726
www.csdisco.com

DATA PROCESSING ADDENDUM ("DPA")

THIS DATA PROCESSING ADDENDUM FORMS PART OF THE AGREEMENT

1. Definitions. Unless otherwise set out in this DPA, any capitalized terms not defined in this DPA shall have the respective meanings given to them in the Agreement.

a. "Customer Personal Data" means personal data or personal information (as defined in Data Protection Laws) contained within Customer Data.

b. "Data Protection Laws" means all laws relating to the use, protection and privacy of Customer Personal Data (including, without limitation, the privacy of electronic communications) which are from time to time applicable to Customer, DISCO, or the Services.

c. "Individual" means an individual who is the subject of Customer Personal Data (or to whom the Customer Personal Data relates).

d. "Individual Request" means a request made by an Individual to exercise a right conferred on them in relation to Customer Personal Data by Data Protection Laws.

e. "Security Incident" means a breach of security leading to the accidental, unlawful or unauthorized loss or disclosure of Customer Personal Data.

f. "Sub-processor" means any sub-contractor engaged by DISCO that agrees to receive from DISCO any Customer Personal Data.

2. Data Processing.

a. DISCO will only process Customer Personal Data in accordance with: (i) the Agreement, to the extent necessary to provide the Services; and (ii) the Customer's written instructions, unless required by applicable laws.

b. The Agreement (subject to any changes to the Services agreed between the parties), including this DPA, shall be the Customer's complete and final instructions to DISCO in relation to the processing of Customer Personal Data.

c. Customer is responsible for ensuring that all individuals who provide written instructions to DISCO are authorized by Customer to issue instructions to DISCO.

d. Customer is solely responsible for its compliance with the Data Protection Laws, including without limitation the lawfulness of any transfer of personal data to DISCO and any subsequent use required to provide the Services.

e. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired or obtained the Customer Personal Data, including providing any required notices, or obtaining any required consents, to Individuals.

f. Customer takes full responsibility to keep the amount of Customer Personal Data provided to DISCO to the minimum necessary for DISCO to administrate the contractual relationship and to provide Customer with the Services.

3. CCPA

a. The parties acknowledge and agree that DISCO is a service provider for the purposes of the California Consumer Privacy Act of 2018 ("**CCPA**") (to the extent it applies) and is receiving Customer Personal Data in order to provide the Services pursuant to the Agreement, which constitutes a business purpose.

b. DISCO shall not sell any Customer Personal Data and DISCO shall not retain, use or disclose any Customer Personal Data except as necessary for the purpose of performing the Services for Customer pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA.

4. Sub-Processors

a. Customer agrees that DISCO may engage Sub-processors to process Customer Personal Data in accordance with this DPA in connection with providing the Services.

b. Customer acknowledges that a list of Sub-processors can be found at this link: DISCO Subprocessor List. DISCO may update such Sub-processors list from time to time as required to provide the Services which Customer is encouraged to review periodically.

c. When engaging Sub-processors, DISCO shall enter into agreements with the Sub-processors to bind them to obligations which are substantially similar to those set out in this DPA.

5. Data Security

a. DISCO will implement the technical and organizational measures set out in Annex 1 to ensure a level of security appropriate to the risk posed by the processing of Customer Personal Data.

b. DISCO may update such measures from time to time to reflect changes in operations, practices and any new or increasing risks provided that the level of security shall not be reduced or diminished in any way.

c. DISCO shall notify Customer without undue delay upon becoming aware of a Security Incident, and shall provide Customer with reasonable assistance to allow Customer to notify Individuals or applicable regulatory authorities of the Security Incident where required by applicable Data Protection Laws.

6. Audits

a. DISCO will provide reasonable information to help Customer to assess DISCO's compliance with its obligations in this DPA and, save as expressly and specifically mandated by Data Protection Laws, no audits are allowed within a data center for security and compliance reasons.

b. As specifically required by applicable Data Protection Laws and subject to the below, only a legally mandated entity (such as a governmental regulatory agency having oversight of Customer's operations) may conduct an on-site visit of the facilities used to provide the Services.

c. After conducting an audit under this Section 6 or after receiving a DISCO report under this Section 6, Customer must notify DISCO of the specific manner, if any, in which DISCO does not comply with any of the data protection obligations in this DPA, if applicable.

d. Any information provided by DISCO under this Section 6 will be deemed Confidential Information of DISCO.

e. Customer may not audit DISCO's Sub-processors without DISCO's and DISCO's Sub-processor's prior agreement and, in relation to its Sub-processors, DISCO will only exercise its audit rights (pursuant to meeting any applicable requirements under Data Protection Laws) to the extent to what it has agreed with its Sub-processors.

f. Without prejudice to the foregoing, Customer agrees its requests to audit Sub-processors may be satisfied by DISCO or DISCO's Sub-processors presenting up-to-date attestations, reports or extracts from independent bodies, including without limitation external or internal auditors, DISCO's data protection officer or IT security personnel, data protection or quality auditors, or other mutually agreed-to third parties, or certification by way of an IT security or data protection audit.

g. On-site audits at Sub-processors' premises may be performed by DISCO acting on behalf of Customer (though DISCO is not under an obligation to do so).

h. Save as otherwise required by Data Protection Laws, Customer may request a summary audit report(s) or audit DISCO no more than once annually provided that Customer provides at least six (6) weeks' prior written notice to DISCO of a request for summary audit report(s) or request to audit.

i. The Customer agrees that the scope of any audit will be limited to DISCO's policies, procedures and controls relevant to the protection of Customer Personal Data.

j. Save as otherwise required by Data Protection Laws, all audits will be conducted during normal business hours, at DISCO's principal place of business or other DISCO location(s) where Customer Personal Data is accessed, processed or administered, and will not unreasonably interfere with DISCO's day-to-day operations.

k. The Customer agrees that any audit will be conducted at Customer's sole cost and by a mutually agreed upon third party who is engaged and paid by Customer, and is under a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement, obligating it to maintain the confidentiality of all DISCO Confidential Information and all audit findings.

l. Before the commencement of any such on-site audit, DISCO and Customer shall mutually agree upon the timing, scope, and duration of the audit and DISCO will reasonably cooperate with the audit, including providing auditor the right to review but not to copy DISCO security information or materials during normal business hours.

m. Customer shall, at no charge, provide to DISCO a full copy of all findings of such audit.

7. Disco Personnel

a. DISCO shall ensure it has in place written agreements with its personnel to maintain the confidentiality of Customer Personal Data.

b. DISCO shall use commercially reasonable efforts to limit access to Customer Personal Data to those personnel who require such access to perform the Agreement.

8. Individual Rights

a. Customer shall respond to inquiries from Individuals and from applicable regulatory authorities concerning the processing of the Customer Personal Data, and will alert DISCO of any inquiries from Individuals or from applicable regulatory authorities that relate to DISCO's processing of the Customer Personal Data.

b. DISCO shall, save as required (or where prohibited) under applicable law, promptly notify Customer if it receives an Individual Request and, to the extent applicable and insofar as possible, DISCO shall provide Customer with commercially reasonable cooperation and assistance as is necessary for Customer to comply with its obligations under the Data Protection Laws in relation to any such Individual Request.

c. Customer shall use its best efforts to respond to and resolve promptly all Individual Requests which DISCO provides to Customer.

d. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from DISCO's provision of assistance under this Section 8.

9. Data Deletion. Unless otherwise required by applicable laws to which DISCO or its Sub-processors are subject, Customer Personal Data will be deleted at the same time and manner in which Customer Data is deleted pursuant to the Agreement.

Last Updated: **06/09/2023**

ANNEX 1
TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

1. DISCO maintains internal policies and procedures, and procures that its Sub-processors do so, which are designed to:

   a. secure any Customer Personal Data processed by DISCO against accidental or unlawful loss, access or disclosure;

   b. identify reasonably foreseeable and internal risks to security and unauthorized access to the Customer Personal Data processed by DISCO; and

   c. minimize security risks, including through risk assessment and regular testing.

2. DISCO will, and will use reasonable efforts to procure that its Sub-processors periodically will:

   a. conduct periodic reviews of the security of its network and the adequacy of its information security program as measured against industry security standards and its policies and procedures; and

   b. evaluate the security of its network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

I. EU SCCs

Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Processor Established in a Third Country (Controller-to-Processor Transfers)

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
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 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 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

CLAUSE 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

CLAUSE 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

CLAUSE 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

CLAUSE 13
Supervision
(a) The supervisory authority 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.

(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;
(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves

more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

CLAUSE 15

Obligations of the data importer in case of access by public authorities
15.1 Notification
(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation
(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS
CLAUSE 16
Non-compliance with the Clauses and termination
(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
(iv) 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 the Republic of Ireland.

CLAUSE 18
Choice of forum and jurisdiction
(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of the Republic of Ireland.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Customer name as provided in the Order Form Agreement
Address: Customer address as provided in the Order Form Agreement
Contact person's name, position and contact details: as provided in the Order Form Agreement
Activities relevant to the data transferred under these Clauses: processing personal data in connection with the data exporter's use of the Services pursuant to the Agreement between data exporter and data importer. See Annex 1B for further details below.
Signature and date: as provided in the Order Form Agreement
Role (controller/processor): Controller

Data importer(s):
Name: CS Disco, Inc. ("DISCO")
Address: 111 Congress Ave, Suite 900, Austin TX 78701
Contact person's name, position and contact details: Trevor Jefferies, General Counsel, dataprotection@csdisco.com
Activities relevant to the data transferred under these Clauses: processing personal data in connection with the data exporter's use of the Services pursuant to the Agreement between data exporter and data importer. See Annex 1B for further details below.
Signature and date: as provided in the Order Form Agreement
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER
Categories of data subjects whose personal data is transferred:

- Employees, partners, workers, contractors and other personnel of the data exporter ("Data Exporter Personnel");
- End-clients of the data exporter and employees, directors, customers, and other personnel of end-clients of the data exporter ("End-Client Representatives");
- Consultants, professional advisors or expert witnesses retained by data exporter or data exporter's end-clients ("Professional Representatives"); or
- Individuals referred to in, the subject of, or otherwise in relation to, data received from data exporter, or end-clients of the data exporter.

Categories of personal data transferred: this may include:

Data Exporter Personnel, End-Client Representatives and Professional Representatives

- Name, job title, identity of employer/organization and other identity details about the individual;
- Email address, telephone number, work and home address and other contact details about the individual;
- Professional information relating to the individual such as work experience and qualifications

In addition to the above, the data importer receives user-provided content and personal data contained in data received from data exporter or data exporter's end-client. Such data will vary depending on the type of case or matter the data exporter is working on with its end-client but may include, without limitation, name, title, position, employer, contact details, professional data, opinions, details relating to legal advice, proceedings and/or matters and data relating to personal affairs.

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.

Data exporter may at its own discretion submit, without the knowledge of the data importer, data that includes personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic information, or health or sex-life information solely for the purpose of using data importer's software and services. Data importer does not otherwise collect or store such special categories of personal data as a matter of course in its operations and does not require or request its customers to supply it in the course of using data importer's software or services. Any such special category personal data is subject to the technical and organization measures set out in Annex II.

The frequency of the transfer:

Personal data will be transferred on a continuous basis for the duration of the Agreement.

Nature of the processing:

See 'purpose(s) of the data transfer and further processing' below.

Purpose(s) of the data transfer and further processing:

The data importer provides to practising legal professionals a suite of software and solutions including DISCO Ediscovery, DISCO Case Builder, and DISCO Review, which process personal data upon the instructions of the data exporter in accordance with the terms of the Order Form Agreement. The personal data transferred will be subject to the following processing activities carried out:

- access to personal data in the provision of support, data remediation and/or troubleshooting services where requested by the data exporter; or
- hosting of personal data as part of the provision of services by the data importer.

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

See data retention section in Annex II.

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

See Annex III

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 of the EEA SCCs is the Irish Data Protection Commission.

ANNEX II

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The data importer has implemented and will maintain the following security measures intended to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

Security Measure	Practices
Pseudonymisation and Encryption	Encryption: All data is encrypted at rest and motion. DISCO customers send data to DISCO via secure FTP, HTTPS or on an encrypted hard drive. All ingested data is protected using SHA1 key exchange, AES-256 encryption, and TLS, SSH, and SCP for transfers. Thus, customer data is protected both in transit and on disk at DISCO's data centers and credentials are encrypted in transit. Pseudonymisation: Data is not pseudonymised. However, DISCO has taken the following steps to ensure compliance with GDPR and/or other applicable data protection regulatory regimes: - Requiring that all data processed is encrypted at rest and in transit. - Through the DISCO Privacy Policy, informing data subjects interacting with DISCO regarding (among other things) how their data is used and what their data rights are. - Maintaining default data protection processes and triggers by which DISCO can satisfy its obligations to comply or assist with a data subject's request to exercise his/her rights with respect to personal data under applicable data protection laws, and to respond to data protection authority inquiries where required by such laws. - Exercising due diligence with respect to processors and sub-processors retained by DISCO to ensure that personal data, if any, that is processed by these third-parties is carried out in accordance with the GDPR and/or other applicable data protection laws.
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	Backed-up data is always available for a current restore in the event of corruption or accidental deletion. Additional information may be found in DISCO's Confidential Business Continuity Disaster Recovery Plan, subject to entering into an NDA.
Ongoing Confidentiality, Integrity, Availability and Resilience	Standards. Commercially reasonable and appropriate methods and safeguards are utilized to protect the confidentiality, availability, and integrity of customer data (including personal data). Confidentiality. DISCO ensures that personnel authorized to access customer data (including personal data) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Training All DISCO employees are required to take security awareness training and pass an exam. The topics covered include: • CS DISCO Security Policy • Data Security • Data Privacy Regulation • Ethics • Ransomware • Phishing and other attacks

Security Measure	Practices
	Backups. Incremental backups are performed on a daily basis, and full backups are performed on a weekly basis. The encrypted backup data sets are distributed across multiple devices and physical facilities. Environmental protection, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements. Thus, backed-up data is always available for a current restore in the event of corruption or accidental deletion. Disaster Recovery: Please see DISCO's Confidential Business Continuity Disaster Recovery Plan, subject to entering into an NDA
Regularly Testing, Assessing and Evaluating the Effectiveness of the Measures	Vulnerability Testing Application vulnerability assessment is run daily by a third party. In addition, a number of tests are regularly conducted by Amazon Web Services. Please see the DISCO Confidential Security Controls Overview, subject to entering into an NDA. Penetration Testing Penetration testing (White Hat) is conducted annually by a person using information gathered from daily automated scans.
User Identification and Authorization	Access Authorization. DISCO was designed from the ground up to enable customers to perform all tasks and administration by themselves with the ability to engage DISCO Professional Services as needed. Customer admins can easily manage users and specify who has access to what features, ingest their data, configure searches, tags, folders, and hit highlighting, specify review workflows, and run their own productions. Periodic user access reviews are performed to remove unauthorized access. Documented policies and procedures are in place regarding user access authorization, provisioning, and revocation. Standardized user access request tickets are utilized to request access to the production system. Access to the production systems (logical access) is revoked as a component of the termination process. Authentication. 2FA is available as an MFA through SSO via SAML. Strong passwords are enforced. System access is via an HTML5 compliant browser, and no local applications or other products are required to gain access. DISCO supports all major IdPs, including Microsoft Active Directory Federation Services, Okta, Microsoft Azure AD, and others.
Protection of Personal Data During Transmission	All data is encrypted at rest and motion. DISCO customers send data to us via secure FTP, HTTPS or on an encrypted hard drive. All ingested data is protected using SHA1 key exchange, AES-256 encryption, and TLS, SSH, and SCP for transfers.
Protection of Personal Data During Storage	See above. All personal data, and all matter data, is encrypted using best-practices AES-256.
Physical Security	Security Safeguards DISCO restricts physical access to information assets and functions by users, and by support personnel. Customer data is processed and stored at Amazon Web Services (AWS) data centers. For more information about AWS security controls, follow the link listed below. https://aws.amazon.com/compliance/data-center/controls <u>POWER</u> DISCO's AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility. <u>CLIMATE AND TEMPERATURE</u> AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels. <u>FIRE DETECTION AND SUPPRESSION</u> AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

Security Measure	Practices
	LEAKAGE DETECTION In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage. Facilities DISCO has three physical facilities where project managers, data specialists and engineers are located. All company facilities are protected by appropriate access controls. The corporate headquarters in Austin, TX has a designated reception area which is attended by either a receptionist or a security guard 24 hours per day; access to the DISCO offices is not permitted without registration and photographic identification being provided in advance. Physical access to the office is controlled through the use of a card access system. Card access is controlled, to ensure only appropriate personnel have access to certain parts of the office; locations with sensitive information are further protected by doors with keypad locks that undergo periodic changes to access codes.
Event Logging	Network Security DISCO's firewalls are located and managed within our private cloud at AWS. Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees. Event Logging For the DISCO Ediscovery solution (application level) DISCO maintains audit logs of every action taken in DISCO. DISCO periodically reviews the audit log information to ensure compliance with DISCO's obligations. User history is maintained at the record level within DISCO and is available to search and view by the client directly. For database logging audit logging settings are in place that includes: - Directory Service Access - Logon events - Object access - Policy changes - Process tracking - System events For infrastructure logging such as operating system audit logging settings are in place that include: - Account logon events - Logon events - Privilege use
System Configuration	Malicious Software. Anti-malware controls are maintained to help prevent malicious software from causing accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to customer data (including personal data).
Governance and Management	Information Security Management. ● DISCO has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. ● DISCO maintains an information security program designed to protect customer data (including personal data) against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. DISCO Personnel. DISCO maintains written policies and procedures that address the roles and responsibilities of personnel, including both technical and non-technical personnel, who have access to customer data (including personal data) in connection with providing the Services. Data Management. DISCO maintains commercially reasonable controls for information governance and data management in connection with the Services.

Security Measure	Practices
Certification of Processes	DISCO annually certifies and complies with ISO 27001 and SOC 2, Type II standards, and is audited annually by an independent audit firm to those standards. At customer's request, and provided that the customer has executed an NDA with DISCO, DISCO will provide customer with copies of applicable ISO and SOC audit reports so that data exporter can review the descriptions of the technical and organizational security measures implemented by DISCO.
Data Minimization / Data Quality	Data Minimization. DISCO shall make reasonable efforts to use the minimum necessary personal data to provide the Services. Data Quality. At all times during the applicable duration of the processing, customer shall have the ability to amend and delete customer data (including personal data) to assist data exporter with its data minimization and data quality obligations.
Data Retention	Data Retention. DISCO will retain customer data (including personal data) stored in the Application Services for 30 days after deactivation of a database or expiration or termination of the Agreement so that data exporter may extract customer data. Following expiry of that period, DISCO will promptly delete all customer data (including personal data), save to the extent that DISCO is required by any applicable law to retain some or all of such data.
Accountability	Accountability. DISCO defines accountability as holding individuals accountable for their internal control responsibilities. Control Activities. Specific control activities that DISCO has implemented in this area are described below. ● A member of personnel may be terminated for non-compliance with a policy and/or procedure; and ● A performance review of employees is conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct and hold them accountable for their internal control responsibilities.
Allowing Portability and Erasure	The DISCO Privacy Policy informs data subjects interacting with DISCO regarding (among other things) how their data is used and what their data rights are (including the right of erasure). In addition, it is as easy to export information in a useable format from any DISCO platform as it is to import data into any DISCO platform.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has generally authorized the engagement of the Sub-processors at this link: DISCO Subprocessor List

Last Updated: **06/09/2023**

II. UK ICO International Data Transfer Addendum

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties: as detailed in the Agreement (including, where applicable, the Addendum EU SCCs).

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs, which this Addendum is appended to, detailed below, including the Appendix Information: Date: the effective date of the Agreement. Reference (if any) at this link: **EU SCCs**

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: as set out in the Addendum EU SCCs.
Annex 1B: Description of Transfer: as set out in the Addendum EU SCCs.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: as set out in the Addendum EU SCCs.
Annex III: List of Sub processors (Modules 2 and 3 only): as set out in the Addendum EU SCCs.

Table 4: Ending this Addendum when the Approved Addendum changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs, those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

"Addendum"	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs;
"Addendum EU SCCS"	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information;
"Appendix Information"	As set out in Table 3;
"Appropriate Safeguards"	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) of the UK GDPR;
"Approved Addendum"	The template Addendum issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18;
"Approved EU SCCs"	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021;
"ICO"	The Information Commissioner;
"Restricted Transfer"	A transfer which is covered by Chapter V of the UK GDPR;
"UK"	The United Kingdom of Great Britain and Northern Ireland;
"UK Data Protection Laws"	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018;
"UK GDPR"	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation ((EU) 2016/679), then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

(a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

(b) Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

(c) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

(a) references to the "Clauses" mean this Addendum, incorporating the Addendum EU SCCs;

(b) In Clause 2, delete the words:

> "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";

(c) Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

(d) Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

(e) Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

(f) References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws".

References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

(g) References to Regulation (EU) 2018/1725 are removed;

(h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

(i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module 1 is replaced with "Clause 11(c)(i)";

(j) Clause 13(a) and Part C of Annex I are not used;

(k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

(l) In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

(m) Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

(n) Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

(o) The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

(a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

(b) reflects changes to UK Data Protection Laws.

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

(a) its direct costs of performing its obligations under the Addendum; and/or

(b) its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Last Updated: **06/09/2023**

I. CANADIAN DATA PROCESSING ADDENDUM (this "CANADIAN DPA")

THIS CANADIAN DATA PROCESSING ADDENDUM FORMS PART OF THE AGREEMENT

1. Application. This Canadian DPA shall apply to the collection, use, disclosure and other processing of Canadian Personal Information. The parties' obligations under this Canadian DPA shall apply in addition to, and not instead of, any other applicable obligations under the Agreement. For the avoidance of doubt, the terms of the Agreement (including the DPA) apply to Canadian Personal Information except as expressly amended in this Canadian DPA. However, to the extent of any conflict with the Agreement (including the DPA), this Canadian DPA shall govern vis-à-vis Canadian Personal Information.

2. Definitions. The following terms shall have the following meanings:

a. "Affiliate" means, with respect to any entity, any other entity controlling, controlled by or under common control with such entity at the time in question.

b. "Canadian Data Protection Laws" means all privacy, data protection and anti-spam legislation in Canada, and all Regulations each thereto, each as amended from time to time, including where applicable: the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (Federal); *An act respecting the protection of personal information in the private sector*, R.S.Q., c.P-39.1 (Quebec); *An Act to modernize legislative provisions as regards the protection of personal information* (Quebec); the *Personal Information Protection Act*, SA 2003, c P-6.5 (Alberta); the *Personal Information Protection Act*, SBC 2003, c 63 (British Columbia); and *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Data Protection and Electronic Documents Act and the Telecommunications Act*. S.C. 2010, c. 23.

c. "Canadian Personal Information" means any Customer Personal Data that (a) constitutes "personal information" for the purposes of any Canadian Data Protection Law, or (b) concerns an Individual that is entitled to exercise rights under any Canadian Data Protection Law.

Unless otherwise set out in this Canadian DPA, any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement (including, where applicable, in the DPA).

3. Compliance with Canadian Data Protection Laws. When this Canadian DPA applies, all references to "Data Protection Laws" in the Agreement (including in the DPA) shall be read to include Canadian Data Protection Laws.

4. Data Processing.

a. In addition to such processing as is permitted under Section 2(a) of the DPA, DISCO may also collect, use, disclose and otherwise process Canadian Personal Information and Usage Data for such purposes as are permitted or required by applicable law.

b. Section 2(d) of the DPA shall be deleted and replaced by the following: "Customer is solely responsible for its compliance with Data Protection Laws, including evaluating and ensuring the lawfulness of any transfer or disclosure of Canadian Personal Information to DISCO and any collection, use, disclosure or other processing of Canadian Personal Information and Usage Data by DISCO as required to provide the Services, to comply with Customer's written instructions, and as otherwise described in the Agreement."

5. Affiliates. Customer agrees that DISCO may transfer or share Canadian Personal Information and Usage Data to or with any of DISCO's Affiliates, who may collect, use, transfer, disclose and otherwise process such information and data for the purposes of providing the Services and complying with Customer's written instructions, and for such other purposes as are permitted or required by applicable law.

6. Notices & Consents. Customer shall provide all necessary notices to, and obtain all necessary consents from, Individuals in order for (a) Customer and DISCO to collect, use, transfer and disclose the Customer Personal Data and Usage Data for the purposes of providing the Services, complying with Customer's written instructions and as otherwise described in the Agreement (including in this Canadian DPA), (b) DISCO to allow any applicable third-party technology provider to access Customer Personal Data as described in the Agreement, (c) DISCO to store Customer Personal Data on servers hosted by a third party, and (d) DISCO, its Affiliates and Sub-processors to collect, use, transfer, disclose, store and otherwise process Canadian Personal Information and Usage Data outside of Canada. Each such notice and consent shall be in a form or forms that comply with all applicable laws (including the Canadian Data Protection Laws and the common law), as well as any findings, interpretation bulletins, guidance documents or fact sheets issued by applicable regulatory authorities. Without limiting

the foregoing, Customer shall ensure that Individuals are notified that their personal information will be transferred and stored outside Canada and may be accessed by foreign courts, law enforcement and national security authorities. Customer shall retain appropriate records of the notices and consents described herein, and shall promptly provide evidence of such notices and consents upon DISCO's request.

7. Accuracy. Customer shall take all reasonable steps to ensure that the Customer Personal Data is accurate and up-to-date to the extent required for DISCO to provide the Services and comply with Customer's written instructions.

8. Cooperation. Subject to any legal restrictions, Customer shall reasonably cooperate with DISCO to respond to any demand, claim, action, complaint, investigation or audit by a third party relating to the collection, use, storage, protection, disclosure, destruction or other processing of Canadian Personal Information in connection with the Services (each a "Legal Action"), including but not limited to any Legal Action initiated by any Individual or regulatory authority.

9. Indemnification. In addition to any other indemnity obligations of Customer pursuant to the Agreement, Customer will indemnify and hold harmless DISCO and its officers, directors, employees, agents, successors, assigns and Affiliates from and against any and all losses, damages, liabilities, penalties, costs or expenses (including legal fees and disbursements) incurred by such parties as a result of Customer's failure to comply with any of (i) the Canadian Data Protection Laws, or (ii) Customer's obligations relating to Canadian Personal Information under the Agreement (including this Canadian DPA).

Last Updated: **06/09/2023**