

---

## DATA PROCESSING ADDENDUM

---

**Dated:** December 8, 2022

This Data Processing Addendum (“**DPA**”) is incorporated by reference into Ericom’s Master Subscription Agreement available at the [Hosted Services Terms and Agreements page](#) of the Ericom website or other terms of service or agreement governing the use of Ericom’s hosted software services (the “**Agreement**”) between the Customer and Ericom Software Ltd. or its Affiliate (“**Ericom**”). This DPA sets forth the terms of Ericom’s Processing of Personal Data on Customer’s behalf in connection with Ericom’s provision of the services under the Agreement (the “**Services**”), to the extent that such Processing is subject to Data Protection Laws. (Ericom and Customer shall be referred to as the “**Parties**” and each, a “**Party**.”)

This DPA shall be effective for the term of the Agreement or until the deletion or return of Personal Data as instructed by Customer under this DPA, whichever is earlier.

In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

### 1. DEFINITIONS

- (a) “**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control”, for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
- (b) “**Authorized Customer Affiliate**” means any Affiliate of Customer that is explicitly permitted to use the Services pursuant to the Agreement but has not signed its own agreement with Ericom and is not a "Customer" as defined under the Agreement.
- (c) “**CCPA**” means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq. and its implementing regulations
- (d) “**Controller**” means the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. To the extent that the CCPA applies, “**Controller**” shall also mean “**Business**”; and “**Processor**,” shall also mean “**Service Provider**”; and Ericom’s Sub-Processor shall also refer to the concept of Service Provider.
- (e) “**Customer**” means the entity that entered into the Agreement with Ericom.
- (f) The terms “**Member State**,” “**Processor**,” “**Processing**,” and “**Supervisory Authority**,” shall have the same meaning as in the GDPR. The terms “**Business**,” “**Business Purpose**,” “**Consumer**,” and “**Service Provider**” shall have the same meaning as in the CCPA.
- (g) “**Data Protection Laws**” means all privacy and data protection laws and regulations, including such laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Canada, Israel, and the United States of America.
- (h) “**Data Subject**” means the identified or identifiable natural person to whom the Personal Data being Processed relates.
- (i) “**EEA**” means the European Economic Area, consisting of the EU Member States, Iceland, Lichtenstein and Norway.
- (j) “**FADP**” means the Swiss Federal Act on Data Protection of 19 June 1992, and as revised as of 25 September 2020, the “**Revised FADP**.”
- (k) “**GDPR**” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
- (l) “**Personal Data**” or “**Personal Information**” means information which is included in data that Customer (including its Authorized Users) submits to the Services, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person, is subject to Data Protection Laws and is processed by Ericom solely on behalf of Customer under this DPA and the Agreement.
- (m) “**Security Measures**” means the Ericom Security Measures for Data Protection applicable to the Personal Data, available at the [Hosted Services Terms and Agreements page](#) of the Ericom website or as otherwise made available by Ericom, as updated from time to time.
- (n) “**Sell**” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for monetary

or other valuable consideration.

- (o) “**Sensitive Data**” means Personal Data that requires special treatment, such as “special categories of data”, “sensitive data” or similar terms, under applicable Data Protection Laws.
- (p) “**Standard Contractual Clauses**” shall mean the European Commission’s standard contractual clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- (q) “**Sub-Processor**” means any third party that Processes Personal Data under the instruction or supervision of Ericom.
- (r) “**UK GDPR**” means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).
- (s) “**UK Addendum**” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018, as set out in Annex 3-C to this DPA; as amended or replaced from time to time by a competent authority under the relevant UK Data Protection Laws.

Capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

## 2. PROCESSING PERSONAL DATA

- 2.1 **Roles of the Parties.** The Parties acknowledge and agree that regarding the Processing of Personal Data solely on behalf of Customer, (i) Customer is the Controller of Personal Data, (ii) Ericom is the Processor of such Personal Data.
- 2.2 **Customer’s Processing of Personal Data.** Customer shall comply with Data Protection Laws in its use of the Services and its instructions to Ericom. Customer shall establish and maintain all required legal bases to collect, Process, and transfer to Ericom the Personal Data and to authorize Ericom’s Processing activities on Customer’s behalf as set forth in the Agreement and this DPA, including the pursuit of “business purposes” as defined under the CCPA.
- 2.3 **Ericom’s Processing of Personal Data.** Customer appoints Ericom to Process Personal Data for the following purposes: (i) to provide the Services; (ii) to comply with Customer’s reasonable and documented instructions regarding the manner in which the Processing shall be performed, where such instructions are consistent with the terms of the Agreement; (iii) to render Personal Data fully anonymous, non-identifiable, and non-personal in accordance with applicable standards recognized by Data Protection Laws and guidance issued thereunder, for Ericom’s purposes; (iv) to establish, exercise, or defend legal claims; (v) to develop, analyze, and improve Ericom’s products, services, and systems; (vi) Processing as required under the laws applicable to Ericom and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, *provided that* Ericom shall inform Customer of the legal requirement before Processing, unless prohibited on important grounds of public interest; (vii) such other Processing in accordance with the Agreement and this DPA.

If Ericom determines that it cannot Process Personal Data in accordance with Customer’s instructions due to applicable legal requirements, Ericom shall inform Customer without undue delay (to the extent permitted under applicable legal requirements), providing relevant details of the issue. Ericom may, without liability to Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing such Personal Data) and/or suspend Customer’s access to the Services.
- 2.4 **Details of the Processing.** The subject-matter of Ericom’s Processing of Personal Data is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data, and categories of Data Subjects Processed under this DPA are further specified in **Schedule 1** (Details of Processing) to this DPA.
- 2.5 **Sensitive Data.** Any Sensitive Data that may flow through the Services is incidental and transient and dependent on Customer’s use of the Services. The Parties agree that the Services are not intended for the processing of Sensitive Data, and that, if Customer wishes to use the Services to process Sensitive Data, it must first obtain Ericom’s explicit prior written consent and enter into any additional agreements as Ericom requires.
- 2.6 **CCPA Standard of Care; No Sale of Personal Information.** Ericom acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that Ericom provides to Customer under the Agreement. Ericom shall not have, derive, or exercise any rights or benefits regarding Personal Information and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it as stipulated in the Agreement and this DPA. Ericom shall not Sell any Personal Information Processed hereunder without Customer’s prior written consent nor take any action that would cause any transfer of Personal Information to or from Ericom under the Agreement or this DPA to qualify as Selling.

### 3. DATA SUBJECT REQUESTS

If Ericom receives a request from a Data Subject to exercise such Data Subject's rights under applicable Data Protection Laws, including, the right of access, right to rectification, restriction of processing, erasure ("right to be forgotten"), data portability, object to the processing, or the right not to be subject to an automated individual decision making ("**Data Subject Request**"), Ericom shall, to the extent legally permitted, notify Customer or refer the Data Subject to Customer. Taking into account the nature of the Processing, Ericom shall reasonably assist Customer to fulfill its obligation under applicable Data Protection Laws to respond to a Data Subject Request. Ericom may advise Data Subjects on available features for self-exercising their Data Subject Requests through the Services (where appropriate), and/or refer the Data Subjects and Data Subject Requests received directly to the Customer to respond to such requests. To the extent legally permitted, Customer shall be responsible for any reasonable costs that Ericom may incur in providing such assistance.

### 4. CONFIDENTIALITY

Ericom shall take reasonable steps to ensure that personnel authorized to Process Personal Data on its behalf are subject to appropriate confidentiality obligations with respect to such Personal Data.

### 5. SUB-PROCESSORS

5.1 **Authorization of Sub-Processors.** Customer hereby grants Ericom a general authorization to engage Sub-Processors to Process Personal Data, *provided that* Ericom has entered into a written agreement with each such Sub-Processor that binds such Sub-Processor to data protection obligations substantially similar to those under this DPA and complies with the requirements set forth below. Ericom will remain liable for any breach of this DPA that is caused by an act, error, or omission of its Sub-Processors.

5.2 **Sub-Processor List.** Ericom makes available to Client the current list of Sub-Processors used by Ericom to process Personal Data at the [Hosted Services Terms and Agreements page](#) of the Ericom website (the "**Sub-Processor List**"), which also enables Customer to subscribe to notifications of new Sub-processors. The Sub-Processor List as of the date of Customer's first use of the Service is hereby deemed authorized upon first use of the Services.

5.3 **Notification of New Sub-Processors.** Ericom may engage with a new Sub-Processor ("**New Sub-Processor**") to Process Personal Data on Ericom's behalf. If Customer [subscribes to notifications of New Sub-Processors](#), Ericom shall provide notification of any New Sub-Processor(s) before authorizing such New Sub-Processor(s) to Process Personal Data in connection with the provision of the Services to Customer.

5.4 **Objection to New Sub-Processors.** Customer may reasonably object to Ericom's use of a New Sub-Processor for reasons relating to the protection of Personal Data intended to be Processed by such New Sub-Processor by providing a detailed written objection to [privacy@ericom.com](mailto:privacy@ericom.com) within five (5) business days following Ericom's notification. Failure to object to a New Sub-Processor in writing to [privacy@ericom.com](mailto:privacy@ericom.com) within five (5) business days following Ericom's notice shall be deemed as acceptance of such New Sub-Processor. In such event, Ericom will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid Processing of Personal Data by the objected-to New Sub-Processor without unreasonably burdening the Customer. If the parties cannot reach a resolution within sixty (60) days of such objection, then Customer may, as a sole remedy, provide written notice to Ericom of termination of the Agreement and this DPA with respect to those Services affected by the use of the New Sub-Processor. Customer shall pay all amounts owing or due under the Agreement before such termination date with respect to such Services. Until a decision is made regarding objected-to New Sub-Processor, Ericom may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Services.

### 6. SECURITY; AUDITS

6.1 **Security Measures for the Protection of Personal Data.** Ericom shall maintain the technical and organizational security measures for the protection of Personal Data, including protection against unauthorized or unlawful Processing, accidental or unlawful destruction, loss or alteration or damage and unauthorized disclosure of, or access to, Personal Data, as set forth in the Security Measures. Upon Customer's reasonable request, Ericom will reasonably assist Customer, at Customer's cost and subject to the provisions of Section 11.1 below, in complying with Customer's obligations pursuant to Articles 32 to 36 of the GDPR, considering the nature of the processing and the information available to Ericom.

6.2 **Audits and Inspections.** To the extent applicable Data Protection Laws include a right for Customer to audit Ericom's Processing of Personal Data, Customer will exercise such audit right, and Ericom will fulfill its corresponding obligations, as set forth in this Section. Upon Customer's fourteen (14) days' prior written request, no more than once every twelve (12) months and subject to strict confidentiality undertakings, Ericom shall make available to Customer that is not a competitor of Ericom (or Customer's independent, reputable, third-party auditor,

subject to confidentiality undertakings) information necessary to demonstrate compliance with this DPA. If such information is not sufficient to demonstrate compliance with this DPA, then Ericom shall allow for and contribute to audits, including inspections, conducted by Customer. Customer shall reimburse Ericom for any time expended by Ericom or its Sub-Processors in connection with any audits under this Section at Ericom's then-current professional services rates. Prior to the start of an audit, the parties will agree to reasonable scope, time, duration, place and conditions for the audit, and the reimbursement payable by Customer to Ericom for Ericom's audit expenses. All information, audits, inspections, and the results therefrom shall constitute Ericom's Confidential Information under the Agreement. Customer will only use such information, etc. to assess compliance with this DPA and not for any other purpose. Customer will promptly notify Ericom of any non-compliance discovered during an audit and provide Ericom any reports generated in connection with any audit, unless prohibited by Data Protection Laws or otherwise instructed by a supervisory authority. In the event of an audit or inspections as set forth above, Customer shall ensure that it (and each of its mandated auditors) will not cause any damage, injury, or disruption to Ericom's premises, equipment, personnel, and business while conducting such audit or inspection.

#### 7. **DATA INCIDENT MANAGEMENT AND NOTIFICATION**

Ericom maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, Ericom shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data (a "**Data Incident**"). Ericom shall make reasonable efforts to: (a) identify the cause of such Data Incident; and (b) to the extent a Data Incident is caused by Ericom's breach of this DPA, remediate and/or mitigate the cause of such Data Incident. Customer will not make, disclose, release, or publish any finding, admission of liability, communication, notice, press release, or report concerning any Data Incident that directly or indirectly identifies Ericom (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Ericom's prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable Data Protection Laws. In the latter case, unless prohibited by such laws, Customer shall provide Ericom with reasonable prior written notice to enable Ericom to object to such disclosure and, in any case, Customer will limit the disclosure to the minimum scope required.

#### 8. **RETURN AND DELETION OF PERSONAL DATA**

Following termination of the Agreement, unless otherwise prohibited by applicable law, Ericom shall delete (or, at the election of the Customer, return in such format as Customer may reasonably elect, subject to payment of Ericom's fees for transferring Personal Data in such format) all Personal Data stored in the Services. Notwithstanding the foregoing, Ericom may retain Personal Data (i) as required by law or expressly agreed with Customer, (ii) stored in accordance with regular computer back-up operations, in compliance with Ericom's disaster recovery and business continuity protocols, and (iii) to the extent authorized or required by applicable law, solely for evidence purposes and/or for the establishment, exercise, or defense of legal claims.

#### 9. **CROSS-BORDER DATA TRANSFERS**

9.1 **Transfers from the EEA, the United Kingdom and Switzerland to countries that offer adequate level of data protection.** Personal Data may be transferred from EEA member countries, the United Kingdom ("**UK**"), and Switzerland to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the UK, and/or Switzerland ("**Adequacy Decisions**"), as applicable, without any further safeguard being necessary.

9.2 **Transfers from the EEA, the United Kingdom and Switzerland to other countries.** If the Processing of Personal Data by Ericom includes a transfer (either directly or via onward transfer) from the EEA ("**EEA Transfer**"), the UK ("**UK Transfer**"), and/or Switzerland ("**Swiss Transfer**") to other countries that have not been subject to a relevant Adequacy Decision and such transfers are not performed through an alternative recognized compliance mechanism for the lawful transfer of personal data (as defined in the GDPR, the UK GDPR, the FADP, as relevant) outside the EEA, the UK, or Switzerland, as applicable, then (i) the terms set forth in Part 1 of **Schedule 2** (EEA Cross Border Transfers) shall apply to any such EEA Transfer; (ii) the terms set forth in part 2 of **Schedule 2** (UK Cross Border Transfers) shall apply to any such UK Transfer; (iii) the terms set forth in Part 3 of **Schedule 2** (Swiss Cross Border Transfers) shall apply to any such Swiss Transfer; and (iv) the terms set forth in Part 4 of **Schedule 2** (Additional Safeguards) shall apply to any such transfers.

#### 10. **AUTHORIZED CUSTOMER AFFILIATES**

10.1 **Contractual Relationship.** The Parties acknowledge and agree that, by executing the Agreement or this DPA, the Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Customer Affiliates, in which case each Authorized Customer Affiliate agrees to be bound by Customer's obligations under this DPA, if and to the extent that Ericom Processes Personal Data on behalf of such Authorized Customer Affiliates, thus qualifying them as the "**Controller.**" All access to and use of the Service by Authorized Customer

Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Customer Affiliate shall be deemed a violation by Customer.

10.2 **Communication.** Customer shall remain responsible for coordinating all communication with Ericom under the Agreement and this DPA and Ericom shall be entitled to rely on Customer to make and receive any communication in relation to this DPA on behalf of its Authorized Customer Affiliates.

#### 11. OTHER PROVISIONS

11.1 **Limitations of Liability.** The liability of each party and its Affiliates under this DPA (including the Standard Contractual Clauses) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

11.2 **Data Protection Impact Assessment and Prior Consultation.** Upon Customer's reasonable request, Ericom shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under applicable Data Protection Law to carry out a data protection impact assessment related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information and to the extent such information is reasonably available to Ericom. Ericom shall provide, at Customer's expense, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 11.1 to the extent required under applicable Data Protection Law.

11.3 **Modifications.** Each Party may by at least forty-five (45) calendar days' prior written notice to the other Party, request in writing any modification to this DPA if such modification is required as a result of any change in, or decision of a competent authority under, any Data Protection Laws, to allow Processing of Personal Data to be made (or continue to be made) without breach of those Data Protection Laws. Pursuant to such notice: (i) the Parties shall make commercially reasonable efforts to accommodate such modification requested by Customer or Ericom; and (ii) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Ericom to protect Ericom against additional risks or to indemnify and compensate Ericom for any further steps and costs associated with the variations made herein at Customer's request. The Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's or Ericom's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within thirty (30) days of such notice, then Customer or Ericom may, by written notice to the other Party, with immediate effect, terminate the Agreement with respect to the Services which are affected by the proposed variations (or lack thereof). Customer will have no further claims against Ericom (including, without limitation, requesting refunds for the Services) pursuant to the termination of the Agreement and the DPA as described in this Section.

## SCHEDULE 1 - DETAILS OF THE PROCESSING

### Subject Matter and Nature and Purpose of Processing

1. Providing the Services to Customer and Authorized Customer Affiliates
2. Performing the Agreement, this DPA, and/or other contracts executed by the Parties
3. Acting upon Customer's instructions, where such instructions are consistent with the terms of the Agreement and this DPA
4. Sharing Personal Data with third parties in accordance with Customer's instructions and/or pursuant to Customer's use of the Services (e.g., integrations between the Services and any services provided by third parties, as configured by or on behalf of Customer to facilitate the sharing of Personal Data between the Services and such third-party services)
5. Complying with applicable laws and regulations
6. Tasks related to any of the above

### Duration of Processing

Subject to any section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Ericom will Process Personal Data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

### Types of Personal Data

1. Source IP Address of User.
2. Activity performed by the user in the cloud application (activity limited to data exchange interfaces).
3. Search terms and browser content (processed in a container, which is destroyed upon the closing of the applicable browser tab or window).
4. Customer logs identifying user/location with destinations accessed (URLs) along with statistical information (e.g. bytes sent, browser type, etc.).
5. Cookies and other similar technologies. (By enabling the "Cookies Persistence" option for Ericom Remote Browser Isolation, Customer authorizes Ericom and its permitted third-party hosting service providers the right to store user-level cookies and other similar technologies.)
6. Personal Data included in any Directory Information fetched from Customer's corporate directory.
7. Name, username, email address, authenticated user header or other identifier that identifies a specific user.
8. Personal Data included in Customer files analyzed by CDR software (analyzed in memory and destroyed upon completion of analysis).
9. Personal Data included by Customer in a support ticket.

### Categories of Data Subjects

Customer and Authorized Customer Affiliates' employees, agents, advisors, and freelancers and other natural persons authorized by Customer and Authorized Customer Affiliates to use the Services.



## SCHEDULE 2 – CROSS BORDER TRANSFERS

### **PART 1 – EEA Cross Border Transfers**

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to an EEA Transfer, subject to the provisions set forth below.
2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Personal Data and Ericom is the data processor of the Personal Data.
3. Module Three (Processor to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data processor of the Personal Data and Ericom is a Sub-Processor of the Personal Data.
4. Clause 7 (Docking Clause) shall not apply.
5. Clause 9, Option 2: GENERAL WRITTEN AUTHORISATION shall apply, and the method for appointing and time period for prior notice of Sub-Processor changes shall be as set forth in Section 5 (Sub-Processors) of the DPA.
6. Clause 11, the optional language will not apply.
7. Clause 17, Option 1 shall apply, and the Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland.
8. Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland.
9. Annex I.A shall be completed as follows:
  - Data Exporter: Customer.
  - Contact details: As detailed in the Agreement.
  - Data Exporter Role:
    - Module Two: The Data Exporter is a data controller.
    - Module Three: The Data Exporter is a data processor.
  - Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
  - Data Importer: Ericom.
  - Contact details: As detailed in the Agreement.
  - Data Importer Role:
    - Module Two: The Data Importer is a data processor.
    - Module Three: The Data Importer is a sub-processor.
  - Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
10. Annex I.B shall be completed as follows:
  - The categories of data subjects are described in **Schedule 1** (Details of Processing) of this DPA.
  - The categories of personal data are described in **Schedule 1** (Details of Processing) of this DPA.
  - The Parties do not intend for Sensitive Data to be transferred. (Any Sensitive Data that may be contained in Data Exporter’s traffic flowing through the Products is incidental, dependent on Data Exporter’s use of the Products and deleted upon the closing of the browser, or completion of CDR analysis, as the case may be.)
  - The frequency of the transfer is a continuous basis for the duration of the Agreement.
  - The nature of the processing is described in **Schedule 1** (Details of Processing) of this DPA.
  - The purpose of the processing is described in **Schedule 1** (Details of Processing) of this DPA.
  - The period for which the personal data will be retained is for the duration of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.
  - In relation to transfers to Sub-Processors, the subject matter, nature, and duration of the processing is set forth at the link detailed in Section 5.2 of the DPA.
11. Annex I.C shall be completed as follows:
  - The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 7 above.
12. The Security Measures referred to in the DPA serves as Annex II of the Standard Contractual Clauses.

13. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses will prevail.

### **PART 2 – UK Cross Border Transfers**

The parties agree that the terms of the UK Addendum (which shall supplement the Standard Contractual Clauses as specified above), as amended or replaced from time to time by the ICO or under the UK GDPR, are hereby incorporated by reference and shall apply to a UK Transfer, subject to the provisions set forth below.

- Table 1: the Parties' details and contact information shall be deemed populated with the relevant information in the Agreement
- Table 2: Parties select the approved Standard Contractual Clauses, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved Standard Contractual Clauses brought into effect for the purposes of this Addendum: Module 2 with the following selections:
  - o Optional Clause 7 (Docking Clause) shall apply;
  - o Clause 9a (Prior or General Authorization): General Authorization;
  - o Clause 9a (Time Period): time period for prior notice of Sub-Processor changes shall be as set forth in Section 5 (Sub-Processors) of the DPA.
  - o Clause 11 (Option) shall not apply;
  - o Personal data received from the Importer may be combined with personal data collected by the Exporter.
- Table 3: Parties make the following selections regarding the Appendix Information:
  - o Annex 1A: List of Parties: The Parties are specified in the Agreement;
  - o Annex 1B: Description of Transfer: is set forth under Annex 1 to the DPA;
  - o Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: are set forth in the Security Measures referred to in the DPA;
  - o Annex III: List of Sub processors (Modules 2 and 3 only): N/A as general authorization is selected.
- Table 4: Parties allowed to end the Addendum: Data Exporter, Data Importer.

### **PART 3 – Swiss Cross Border Transfers**

The Parties agree that the Standard Contractual Clauses as detailed in Part 1 of this **Schedule 2**, shall be adjusted as set out below where the FADP applies to Switzerland Transfers:

1. References to the Standard Contractual Clauses mean the Standard Contractual Clauses as amended by this Part 3;
2. The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for Swiss Transfers exclusively subject to the FADP;
3. The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the Standard Contractual Clauses shall be interpreted to include the FADP with respect to Swiss Transfers;
4. References to Regulation (EU) 2018/1725 are removed;
5. Swiss Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named in Part 1 of this **Schedule 2**;
6. References to the "Union," "EU," and "EU Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses;
7. Where Swiss Transfers are exclusively subject to the FADP, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP;
8. Where Swiss Transfers are subject to both the FDPA and the GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FDPA insofar as the Swiss Transfers are subject to the FADP;
9. The Standard Contractual Clauses as amended by this Part 3 also protect the Personal Data of legal entities until the entry into force of the Revised FADP.



#### **PART 4 – Additional Safeguards**

1. In the event of an EEA Transfer, a UK Transfer, or a Swiss Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:
  - a. Ericom shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from the Controller to Ericom and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit and at rest intended to deny attackers the ability to read data.
  - b. Ericom will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under GDPR or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Act (“FISA”).
  - c. If Ericom becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:
    - I. Ericom shall inform the relevant government authority that Ericom is a processor of the Personal Data and that the Controller has not authorized Ericom to disclose the Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to the Personal Data should therefore be notified to or served upon the Controller in writing;
    - II. Ericom will use commercially reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under Ericom’s control. Notwithstanding the above, (a) the Controller acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Personal Data, Ericom has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection (c)(II) shall not apply. In such event, Ericom shall notify the Controller, as soon as possible, following the access by the government authority, and provide the Controller with relevant details of the same, unless and to the extent legally prohibited to do so.
2. Once in every 12-month period, Ericom will inform the Controller, at the Controller’s written request, of the types of binding legal demands for Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.