

## DATA PROCESSING AGREEMENT

This DPA is entered into between the Controller and the Processor and is incorporated into and governed by the terms of the Agreement and by any Data Protection Law applicable to each Party in performing its obligations under the Agreement.

### 1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Agreement.

<b>“Affiliate”</b>	means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;
<b>“Agreement”</b>	means the agreement between the Controller and the Processor for the provision of the Services;
<b>“CCPA”</b>	means the California Consumer Privacy Act of 2018, along with its regulations and as amended from time to time;
<b>“Company”</b>	means the SEDNA Affiliate who entered into the Agreement;
<b>“Controller”</b>	means the Customer;
<b>“Customer Data”</b>	means all data imported into the Services for the purpose of using the Services or facilitating the Customer’s use of the Services;
<b>“Data Protection Law”</b>	means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the UK GDPR, the FDPA, the UK Data Protection Act 2018, the CCPA, the Singapore Personal Data Protection Act (PDPA), the Canadian Personal Information Protection Electronic Documents Act (PIPEDA) and any applicable national implementing laws, regulations and secondary legislation relating to the processing of the Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
<b>“Data Retention Policy”</b>	means the data retention policy of the Company published at: <a href="https://sedna.com/data-retention-policy/">https://sedna.com/data-retention-policy/</a> as amended from time to time;
<b>“Data Subject”</b>	shall have the same meaning as in Data Protection Law or means a “Consumer” as that term is defined in the CCPA;
<b>“DPA”</b>	means this data processing agreement together with Exhibits A, B and C;

<b>“EEA”</b>	means the European Economic Area;
<b>“EU GDPR”</b>	means 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);
<b>“FDPA”</b>	means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; FDPA) and as amended from time to time;
<b>“Personal Data”</b>	shall have the same meaning as in Data Protection Law;
<b>“Processor”</b>	means the Company, including as applicable any “Service Provider” as that term is defined by the CCPA;
<b>“Restricted Transfer”</b>	means: (i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission;
<b>“Services”</b>	means all services and software applications and solutions provided to the Controller by the Processor under and as described in the Agreement;
<b>“SCCs”</b>	means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries published at <a href="https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&amp;from=EN">https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&amp;from=EN</a> (“EU SCCs”); and (ii) where the UK GDPR applies standard data protection clauses adopted pursuant to Article 46(2)(d) of the UK GDPR as set out in Exhibit C of this DPA, (“UK SCCs”); and (iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority; (“Swiss SCCs”);
<b>“Sub-processor”</b>	means any third party (including Processor Affiliates) engaged directly or indirectly by the Processor to process Personal Data under this DPA in the provision of the Services to the Controller;

---

<b>“Supervisory Authority”</b>	means a governmental or government chartered regulatory body having binding legal authority over a party;
<b>“UK GDPR”</b>	means the EU 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.

---

## **2. Purpose**

- 2.1 The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Agreement. In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

## **3. Scope**

- 3.1 In providing the Services to the Controller pursuant to the terms of the Agreement, the Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with the terms of the Agreement, this DPA and the Controller's instructions documented in the Agreement and this DPA, as updated from time to time.
- 3.2 The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the Processor who has access to Personal Data does not process them except on the instructions from the Controller unless required to do so by any Data Protection Law.

## **4. Processor Obligations**

- 4.1 The Processor may collect, process or use Personal Data only within the scope of this DPA.
- 4.2 The Processor confirms that it shall process Personal Data on behalf of the Controller in accordance with the documented instructions of the Controller.
- 4.3 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach any Data Protection Law.
- 4.4 The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.
- 4.5 The Processor shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.
- 4.6 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and

evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

- 4.7 The technical and organisational measures detailed in Exhibit B shall at all times be adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA, provided such measures are at least equivalent to the technical and organisational measures set out in Exhibit B and appropriate pursuant to the Processor's obligations in clauses 4.5 and 4.6 above.
- 4.8 The Controller acknowledges and agrees that, in the course of providing the Services to the Controller, it may be necessary for the Processor to access the Personal Data to respond to any technical problems or Controller queries and to ensure the proper working of the Services. All such access by the Processor will be limited to those purposes.
- 4.9 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.
- 4.10 The Processor may not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for commercial purposes other than providing the Services under the terms of the Agreement; or (iii) retain, use, or disclose Personal Data outside of the Agreement.

## **5. Controller Obligations**

- 5.1 The Controller represents and warrants that: (i) it shall comply with this DPA and its obligations under Data Protection Law; (ii) it has obtained any, and all, necessary permissions and authorisations necessary to permit the Processor, its Affiliates and Sub-processors, to execute their rights or perform their obligations under this DPA; and (iii) all Affiliates of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA.
- 5.2 The Controller shall implement appropriate technical and organisational measures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

- 5.3 The Controller acknowledges and agrees that some instructions from the Controller including the Processor assisting with audits, inspections, DPIAs or providing any assistance under this DPA, may result in additional fees. In such case the Processor shall notify the Controller of its fees for providing such assistance in advance and shall be entitled to charge the Controller for its reasonable costs and expenses in providing such assistance, unless agreed otherwise in writing.
- 6. Sub-processors**
- 6.1 The Controller acknowledges and agrees that: (i) Affiliates of the Processor may be used as Sub-processors; and (ii) the Processor and its Affiliates respectively may engage Sub-processors in connection with the provision of the Services.
- 6.2 All Sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor set out in this DPA.
- 6.3 The Controller authorises the Processor to use the Sub-processors included in the list of Sub-processors published at <https://sedna.com/list-of-sub-processors> to process the Personal Data. During the term of this DPA, the Processor shall provide the Controller with 30 days prior notification, via email, of any changes to the list of Sub-processors before authorising any new or replacement Sub-processor to process Personal Data in connection with provision of the Services.
- 6.4 The Controller may object to the use of a new or replacement Sub-processor, by notifying the Processor promptly in writing within fifteen (15) days after receipt of the Processor's notice. In the event that the Controller objects to a new or replacement Sub-processor (the "Objected Sub-Processor"), Processor will make reasonable efforts to add additional safeguards (covering the specified deficiencies as set out by the Controller) or change the Objected Sub-processor to an alternative Sub-Processor acceptable to the Controller; should Processor be unable to do so, Processor will use reasonable efforts to make available to the Controller a change in the Services or recommend a commercially reasonable change to Controller's configuration or use of the Services to avoid processing of Personal Data by the Objected Sub-processor without unreasonably burdening the Controller. If Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, the Controller may terminate only those Services that cannot be provided by Processor without the use of the Objected Sub-Processor by providing written notice to Processor. The Processor will refund the Controller any prepaid fees covering the remainder of the term of the Agreement following the effective date of termination with respect to such terminated Services.
- 6.5 All Sub-processors who process Personal Data shall comply with the obligations of the Processor set out in this DPA. The Processor shall, prior to the relevant Sub-processor carrying out any processing activities in respect of the Personal Data, enter into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those contained in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.
- 6.6 The Controller agrees that the Processor and its Sub-processors may make Restricted Transfers of Personal Data for the purpose of providing the Services to the Controller in accordance with the Agreement. The Processor confirms that such Sub-processors: (i) are located in a third country or territory recognised by the EU Commission or a Supervisory Authority, as applicable, to have an adequate level of protection; or (ii) have

entered into the applicable SCCs with the Processor; or (iii) have other legally recognised appropriate safeguards in place.

## **7. Restricted Transfers**

7.1 The parties agree that, when a transfer of Personal Data occurs between the Controller and the Processor or from the Processor to a Sub-processor which is a Restricted Transfer, that is not within the scope of clause 6.6 (i) or (iii) above, it shall be subject to the applicable SCCs.

7.2 The parties agree that the EU SCCs shall apply to Restricted Transfers from the EEA. The EU SCCs shall be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

i. Module Two (Controller to Processor) shall apply where the Customer is a Controller of Personal Data and the Company is processing Personal Data;

ii. Module Three (Processor to Processor) shall apply where the Company is a Processor of Personal Data and the Company uses a Sub-processor to process the Personal Data;

iii. Module Four (Processor to Controller) shall apply where the Company is processing Personal Data and the Customer is not subject to the EU GDPR or UK GDPR;

iv. In Clause 7 of the EU SCCs, the optional docking clause will not apply;

v. In Clause 9 of the EU SCCs Option 2 applies, and the time period for giving notice of Sub-processor changes shall be as set out in clause 6.3 of this DPA;

vi. In Clause 11 of the EU SCCs, the optional language shall not apply;

vii. In Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs shall be governed by Irish law;

viii. In Clause 18(b) of the EU SCCs, disputes shall be resolved by the courts of Ireland;

ix. Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A of this DPA;

x. Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit B of this DPA;

7.3 The parties agree that the EU SCCs as amended in clause 7.2 above, shall be adjusted as set out below where the FDPA applies to any Restricted Transfer:

i. The Swiss Federal Data Protection and Information Commissioner (“FDPIC”) shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the FDPA;

ii. Restricted Transfers subject to both the FDPA and the EU GDPR, shall be dealt with by the EU Supervisory Authority named in Exhibit A of this DPA;

iii. The term ‘member state’ must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;

- iv. Where Restricted Transfers are exclusively subject to the FDPA, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA;
  - v. Where Restricted Transfers are subject to both the FDPA and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA insofar as the Restricted Transfers are subject to the FDPA;
  - vi. The Swiss SCCs also protect the Personal Data of legal entities until the entry into force of the revised FDPA.
- 7.4 The parties agree that the UK SCCs shall apply to Restricted Transfers from the UK and the UK SCCs shall be deemed entered into (and incorporated into this DPA by reference), as set out in Exhibit C of this DPA.
- 7.5 In the event that any provision of this DPA contradicts directly or indirectly any SCCs, the provisions of the applicable SCCs shall prevail over the terms of the DPA.
- 8. Data Subject Access Requests**
- 8.1 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Controller acknowledges and agrees that the Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.
- 8.2 In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.
- 9. Audit**
- 9.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.
- 9.2 Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may conduct a more extensive audit which shall be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance; (iii) carried out during the Processor's usual business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Processor's day-to-day business.
- 9.3 This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.
- 10. Personal Data Breach**
- 10.1 The Processor shall notify the Controller without undue delay after becoming aware of (and will make all commercially reasonable efforts to notify within 72 hours of discovering)

any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data (“Personal Data Breach”).

- 10.2 In the event of the Personal Data Breach, the Processor shall take all commercially reasonable measures to prevent a further Personal Data Breach, to limit the effects of any Personal Data Breach, and to assist the Controller in meeting the Controller’s obligations under applicable law.

## **11. Compliance, Cooperation and Response**

- 11.1 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller, unless such notification is not permitted under applicable law or a relevant court order.
- 11.2 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.
- 11.3 The Processor shall reasonably assist the Controller in meeting the Controller’s obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of the processing and the information available to the Processor.
- 11.4 The Controller shall notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the Processor is unable to accommodate necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.
- 11.5 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Law.

## **12. Liability**

- 12.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.
- 12.2 The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.
- 12.3 The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Controller itself.
- 12.4 The Controller shall not be entitled to recover more than once in respect of the same loss.

## **13. Term and Termination**

- 13.1 The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall



terminate automatically together with termination or expiry of the Agreement. Notwithstanding the foregoing, if the Processor continues to process Personal Data beyond the termination or expiry of the Agreement for any reason, this DPA shall continue to be in effect after the termination of the Agreement until the Processor ceases to process Personal Data on behalf of the Controller.

**14. Deletion and Return of Personal Data**

14.1 The Processor shall at the choice of the Controller, upon receipt of a written request received within 30 days of the end of the provision of the Services, delete or return Personal Data to the Controller. The Processor shall in any event delete all copies of Personal Data in its systems after the termination of the Agreement in accordance with the Processor's Data Retention Policy unless: (i) applicable law or regulations require storage of the Personal Data after termination; or (ii) partial Personal Data of the Controller is stored in backups, then such Personal Data shall be deleted from backups after the effective date of termination of the Agreement in accordance with the Processor's Data Retention Policy. Until Personal Data is deleted or returned, Processor shall continue to comply with this DPA and its Exhibits.

**15. General**

15.1 This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

15.2 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

15.3 Subject to any provision of the SCCs to the contrary, this DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

15.4 The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

**Exhibit A**

**List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority**

**A. LIST OF PARTIES**

**The Exporter:**

<b>means the Customer</b>	
<b>Address:</b>	As set out for the Customer in the Agreement.
<b>Contact person's name, position and contact details:</b>	As provided by the Customer in its account and used for notification and invoicing purposes.
<b>Activities relevant to the data transferred under the SCCs:</b>	Use of the Services.
<b>Signature and date:</b>	By entering into the Agreement, the Controller is deemed to have signed the SCCs incorporated into this DPA and including their Annexes, as of the Effective Date of the Agreement.
<b>Role:</b>	Controller.
<b>Name of Representative (if applicable):</b>	Any UK or EU representative named in the Controller's privacy policy.

**The Importer:**

<b>means the Company: SEDNA Communications Limited</b>	
<b>Address:</b>	Buckingham Green 65 Buckingham Gate London

	SW1E 6AS United Kingdom
<b>Activities relevant to the data transferred under the SCCs:</b>	The provision of cloud computing solutions to the Controller under which the Processor processes Personal Data upon the instructions of the Controller in accordance with the terms of the Agreement.
<b>Signature and date:</b>	By entering into the Agreement, the Processor is deemed to have signed the SCCs, incorporated into this DPA, including their Annexes, as of the Effective Date of the Agreement.
<b>Role:</b>	Processor
<b>Representative Contact Details (if applicable)</b>	privacy@sedna.com

## B. DESCRIPTION OF PROCESSING AND TRANSFERS

<b>Categories of Data Subjects:</b>	<p>Employees, agents, advisors, consultants, freelancers of the Controller (who are natural persons).</p> <p>Users, Affiliates and other participants authorised by the Controller to access or use the Services in accordance with the terms of the Agreement.</p> <p>Prospects, customers, clients, business partners and vendors of the Controller (who are natural persons) and individuals with whom those end users communicate with by email and/or other messaging media.</p> <p>Employees or contact persons of Controller’s prospects, customers, clients, business partners and vendors.</p> <p>Suppliers and service providers of the Controller.</p> <p>Other individuals to the extent identifiable in the context of emails of their attachments or in archiving content.</p>
-------------------------------------	--

<b>Categories of Personal Data:</b>	<p>The Controller may submit Personal Data to the Services, the extent of which is determined and controlled by the Controller. The Personal Data includes but is not limited to:</p> <ul style="list-style-type: none"> <li>· Personal details, names, email addresses of users of the Services.</li> <li>· Unique identifiers such as username, account number or password.</li> <li>· Personal Data derived from a user's use of the Services such as records and business intelligence information.</li> <li>· Personal Data within email and messaging content which identifies or may reasonably be used to identify, Data Subjects.</li> <li>· Metadata including sent, to, from, date, time, subject, which may include Personal Data.</li> <li>· Geolocation based upon IP address.</li> <li>· Financial data required for invoicing.</li> <li>· Consumption habits</li> <li>· Data concerning education and profession</li> <li>· Images and sound recordings</li> <li>· File attachments that may contain Personal Data</li> <li>· Survey, feedback and assessment messages</li> <li>· Information offered by users as part of support enquiries</li> <li>· Other data added by the Controller from time to time</li> </ul>
<b>Sensitive Data:</b>	<p>No sensitive data will be processed or transferred and shall not be contained in the content of or attachments to, emails.</p>
<b>The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):</b>	<p>Continuous basis for the duration of the Agreement.</p>
<b>Nature of the processing:</b>	<p>Processing operations include but are not limited to: ingestion, indexing, storage, and presentation of email correspondence, including attachments and metadata; transmission of outbound emails and their attachments; storing contact information via an address book; exchanging data with other systems used by the Controller through APIs; analytics based on system usage. These operations are provided to users of the Services as defined in the Agreement.</p>
<b>Purpose(s) of the data transfer and further processing:</b>	<p>Personal Data is transferred to sub-contractors who need to process some of the Personal Data in order to provide their services to the Processor as part of the Services provided by the Processor to the Controller.</p>

<b>The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:</b>	Unless agreed otherwise in writing, for the duration of the Agreement, subject to clause 14 of the DPA.
<b>For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:</b>	The Sub-processor list accessed via <a href="https://sedna.com/list-of-sub-processors">https://sedna.com/list-of-sub-processors</a> sets out the Personal Data processed by each Sub-processor and the services provided by each Sub-processor.

**C. COMPETENT SUPERVISORY AUTHORITY**

<b>Identify the competent supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)</b>	<p>Where the EU GDPR applies, the Irish Data Protection Authority – the Data Protection Commission (DPC)</p> <p>Where the UK GDPR applies, the UK Information Commissioner’s Office, (ICO).</p> <p>Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner, (FDPIC).</p>
---	---

**Exhibit B**  
**Technical and Organisational Security Measures**  
**(Including Technical and Organisational Measures to Ensure the Security of Data)**

Below is a description of the technical and organisational measures implemented by the Processor (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.

Full details of the Processor's/Data Importer's technical and organisational security measures used to protect Personal Data is available in Exhibit A of this DPA.

Where applicable this Exhibit B will serve as Annex II to the SCCs.

Measure	Description
Measures of pseudonymisation and encryption of Personal Data	<p>All data at rest, including backups, are encrypted using the AES-256 encryption algorithm. Data in transit to and from SEDNA is protected via NSB-approved communications protocols such as TLS/SSL. Inbound and outbound Email is delivered with TLS/SSL encryption when available. All encryption is performed in accordance with NIST <u>Cryptographic Standards and Guidelines</u> and the NIST <u>Policy on Hash Functions</u>. The following types of encryption may be employed, depending on the purpose:</p> <ul style="list-style-type: none"> <li>· Asymmetric encryption: public key infrastructure underlying SSL/TLS 1.2, and SSH FTP (e.g., RSA 2048-bit)</li> <li>· Symmetric encryption: private key encryption (e.g., AES-128, 192, 256 bit)</li> <li>· Hashing: one-way encryption for confirming authenticity (e.g., digital signature signings)</li> </ul> <p>Virtual private networks (VPNs) may also be used to assist with the protection of information, and with accessing private, authentication-required services. Amazon Web Services (AWS) Key Management Service (KMS) is employed for the management of encryption keys.</p>
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	<p>Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept. In accordance to the “least privilege” and “need-to-know” principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person.</p>

<p>Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident</p>	<p>All of the Processor's applications are built in a High Availability configuration. Databases are subject to synchronous replication across multiple availability zones and backups of the databases are retained for a rolling period of 7 days in accordance with our backup procedures. In the event of failure of both High Availability databases, data can be restored to a third data centre.</p>
<p>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing</p>	<p>The Processor maintains an ISO/IEC 27001:2013-certified Information Security Management System, subject to annual audit as well as other internal assurance exercises. In addition to automated monitoring and alerting, the Processor is subject to penetration testing by an independent third-party at least annually.</p>
<p>Measures for user identification and authorisation</p>	<p>The Processor supports SAML-based authentication as well as enforcing Multi-Factor Authentication. Once a user has been authenticated, authorisation is derived from the roles assigned to the user by the Controller.</p>
<p>Measures for the protection of data during transmission</p>	<p>Data in Transit to and from SEDNA is protected via NSB-approved communications protocols such as TLS/SSL.</p>
<p>Measures for the protection of data during storage</p>	<p>All data at rest, including backups, are encrypted using the AES-256 encryption algorithm.</p>
<p>Measures for ensuring physical security of locations at which Personal Data are processed</p>	<p>Due to their respective security requirements, business premises and facilities are subdivided into different security zones with different access authorisations. AWS data centres are subject to industry-leading controls as outlined at <a href="https://aws.amazon.com/compliance/data-center/controls/">https://aws.amazon.com/compliance/data-center/controls/</a>. Access for employees to office locations is only possible with an encoded ID. All other persons have access only after having registered before (e.g. at the main entrance).</p> <p>The Processor also maintains a Physical and Environmental Security Policy as part of our ISO/IEC 27001:2013-certified ISMS.</p>
<p>Measures for ensuring events logging</p>	<p>The Processor logs all events performed in the system. These events are retained in perpetuity unless destroyed in accordance with the terms of the Master Services &amp; Subscription Agreement. These events are also exposed to the Controller via the User Interface in the form of an Activity Panel, as well as being exposed via API for logging in the Controller's SIEM.</p>

<p>Measures for ensuring system configuration, including default configuration</p>	<p>The Processor's system configuration is managed via feature flags editable only by authorized individuals. Changes to configuration beyond the default configuration are logged and monitored. System configuration is applied and maintained by software tools that ensure the system configurations do not deviate from the specifications. Deviations will be fixed automatically and reported to our ISSC.</p>
<p>Measures for internal IT and IT security governance and management</p>	<p>Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems.</p> <p>The Controller's Personal Data is stored in a way that logically or physically separates it from other customer data as determined in the Agreement.</p>
<p>Measures for certification/assurance of processes and products</p>	<p>The Processor is ISO/IEC 27001:2013 certified and will continue to maintain this certification for the term of the Agreement. The technical and organisational measures defined herein are implemented based on the international standard ISO/IEC 27001:2013. The Processor shall maintain controls materially as protective as those provided in the ISO 27001 and ISO 27018 or other substantially similar or equivalent certification requirements. In addition, the Processor utilises third-party Infrastructure as a Service providers that maintain current ISO 27001 certifications. The Processor will only use third party data centres that maintain the aforementioned certifications and/or attestations, or that have other substantially similar or equivalent certifications and/or attestations.</p> <p>See: <a href="https://aws.amazon.com/compliance/iso-certified/">https://aws.amazon.com/compliance/iso-certified/</a>  Upon the Controller's written request (no more than once in any 12 month period), the Processor shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties</p>
<p>Measures for ensuring data minimisation</p>	<p>If Personal Data is no longer required for the purposes for which it was processed, it is deleted in accordance with the terms of the Agreement between the parties.</p>



Measures for ensuring data quality	All of the data processed is provided by the Controller. The Processor does not assess the quality of the data provided by the Controller. The Processor provides reporting tools within its product to help the Controller understand and validate the data that is stored. The Processor also uses a combination of a firewall and malware detection software which monitors data for potential threats and blocks requests as required.
Measures for ensuring limited data retention	The Processor uses a data classification scheme for all data that it stores. When a record with Personal Data is deleted then it will be permanently removed from the Processor's active databases. The data is retained in backups until they are replaced by more recent backups.
Measures for ensuring accountability	The Processor internally reviews its information security policies at least annually. All employees must acknowledge the information security policies. These employees are re-trained on information security policies once per year. A disciplinary policy is in place for employees that do not adhere to information security policies.
Measures for allowing data portability and ensuring erasure	The Processor maintains procedures and tools that allow data to be exported and provided to the Controller. Further procedures are maintained to allow the Processor to permanently delete data in accordance with the terms of the Agreement between the parties.
Measures to be taken by the (Sub-) processor to be able to provide assistance to the Controller (and, for transfers from a Processor to a Sub-processor, to the Data Exporter).	The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) is only made if a corresponding contract exists, and only for the specific purposes. If Personal Data is transferred outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the EU SCCs.

### Exhibit C

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

**VERSION B1.0, in force 21 March 2022**

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

<b>Start date</b>	<b>The date set out in Annex I of the Approved EU SCCs.</b>	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	Full legal name: the Customer named in the Agreement. Main address (if a company registered address): As set out in Annex I of the Approved EU SCCs. Official registration number (if any) (company number or similar identifier): Where set out in the Agreement.	Full legal name: SEDNA Communications Limited Main address: 10 John Street, London, WC1N 2EB, United Kingdom. Official registration number (if any) (company number or similar identifier): 13367033.
<b>Key Contact</b>	Full Name (optional): As set out in Annex I of the Approved EU SCCs. Job Title: As set out in Annex I in the Approved EU SCCs Contact details including email: As set out in Annex I the Approved EU SCCs.	Full Name (optional): Cheikh Ndoeye Job Title: Senior Pre-Sales Solutions Engineer Contact details: <a href="mailto:privacy@sedna.com">privacy@sedna.com</a>
<b>Signature (if required for the purposes of Section 2)</b>	no signature is required.	no signature is required.

Table 2: Selected SCCs, Modules and Selected Clauses

<b>Addendum EU SCCs</b>	the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:
-------------------------	---

Module	Module in operation	Clause 11 (Option)	Clause 9a General Authorisation	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	no	not used	–	–	–
2	yes	not used	Yes	30 days	–

3	yes	not used	Yes	30 days	–
4	yes	not used	–	–	no

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: for Module 2 and Module 3

Annex 1B: Description of Transfer: for Module 2 and Module 3

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: for Module 2

Annex III: List of Sub-Processors (Module 2) The Sub-processor list accessed via <https://sedna.com/list-of-sub-processors> sets out the Personal Data processed by each Sub-processor and the services provided by each Sub-processor.

Table 4: Ending this Addendum when the Approved Addendum Changes

<b>Ending this Addendum when the Approved Addendum changes</b>	Which Parties may end this Addendum as set out in Section19: Importer Exporter
--	--

## Part 2: Mandatory Clauses

### Entering into this Addendum

- 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.
- 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

- 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) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A 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" means 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 benefiting 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 benefiting 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 one, 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.