Data Processing Agreement
(Updated 26 February 2024)

This Data Processing Agreement ("**DPA**") is part of the Master Service Agreement found at https://plumsail.com/master-service-agreement updated from time to time, or other written or electronic agreement between Plumsail Inc. ("**Plumsail**") and Customer for the purchase and/or use of online services from Plumsail (identified either as "**Services**" or otherwise in the applicable agreement, and hereinafter defined as "**Services**") (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of Customer's Authorized Affiliates, if and to the extent Plumsail processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "**Customer**" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Plumsail may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

Definitions
- "**Affiliate**" - (a) any entity on whose behalf Customer obtained the Plumsail Services, and/or (b) 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.
- "**Authorized Affiliate**" - any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Plumsail, but has not signed its own Agreement with Plumsail and is not a "Customer" as defined under the Agreement.
- "**personal data**" - any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- "**processing**" - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection,

recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- "**Controller**" - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- "**Processor**" - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- "**Sub-processor**" - any data processor engaged by the Processor
- "**confidential Information**" – all information disclosed by a Party to the other Party pursuant to this Agreement, including (but not limited to):
- any trade secret, know-how, invention, concept, software program, source code, object code, application, documentation, schematic, procedure, contract, information, knowledge, data, database, process, technique, design, drawing, program, formula or test data, work in progress, engineering, manufacturing, marketing, financial, sales, supplier, technical, scientific, customer, employee, investor, or business information, whether in oral, written, graphic, or electronic form;
    - o any non-public business information, including personnel data, correspondence with any Governmental Authority, historical customer information and data, historical cost information such as budgets, operating expenses, and capital costs, and projected capital additions, operating cost information, and other business, and financial reports and forecasts;
    - o any document, diagram, photograph, drawing, computer program, or other communication that is either conspicuously marked "confidential", or is known or reasonably should have been known by the receiving Party to be confidential;
- "**Security Practices**" means Plumsail's "Security Practices Datasheet", as updated from time to time, and currently accessible at:
    - o Plumsail Documents
      https://plumsail.com/docs/documents/v1.x/general/security-policy.html
    - o Plumsail Actions
      https://plumsail.com/docs/actions/v1.x/general/security-policy.html
    - o Plumsail Forms
      https://plumsail.com/docs/forms-web/general/data-security.html
    - o Plumsail HelpDesk
      https://plumsail.com/docs/help-desk-o365/v1.x/General/Security.html
    - o Plumsail Org Chart
      https://plumsail.com/docs/orgchart/v1.x/general/privacy-policy-o365.html
- "**Standard Contractual Clauses**" or "**SCC**" means the standard contractual clauses for the transfer of personal data from the EEA to third countries set out in Commission

Implementing Decision (EU) 2021/914 and which are hereby incorporated into this DPA. For the purposes of the Standard Contractual Clauses (SCC) attached and incorporated in Exhibit 1 herein, (a) Customer shall be the 'data exporter and Plumsail the 'data importer;' (b) Exhibit 1 incorporates the parties' selection of module 2 (controller – processor data transfer) into the SCC; and (c) the parties agree that Exhibit 1, including its Appendix and attendant annexes as drafted and attached below are the SCCs for purposes of this DPA.

1. Object of this DPA

1.1. In the course of providing the Services to the Controller pursuant to this Agreement, the Processor may process personal data on behalf of the Controller. The Processor agrees to comply with the following provisions with respect to any personal data processed for the Controller in connection with the provision of the Services.

1.2 The Processor shall process personal data it receives from the Controller solely for purposes stemming from usage of Service and for no other purpose except with the express written consent of the Controller.

1.3 The Processor shall process categories of data subjects which are provided to the Service by the Controller. Processor is not entitled to process any category of data without prior demand or consent of the Controller.

1.4 Types of personal data. Contact information, the extent of which is determined and controlled by the Controller in its sole discretion, and other personal data such as navigational data (including website usage information), email data, system usage data, application integration data, internet protocol (IP) and other electronic data submitted, stored, sent, or received by end users via the Service.

1.5 Subject-Matter and nature of the processing. The subject-matter of processing of personal data by the Processor is the provision of the Services to the Controller that involves the processing of personal data. Personal data will be subject to those processing activities as may be specified in the [Documents Privacy Policy](), [Actions Privacy Policy](), [Forms Privacy Policy](), [HelpDesk Privacy Policy](), [Org Chart Privacy Policy]().

1.6 Customer agrees to enter into the Standard Contractual Clauses set out in Exhibit 1 attached hereto and acknowledges that Sub-processors may be appointed by Plumsail in accordance with Clause 9 of Exhibit 1 attached hereto.

2. Data protection

2.1 As the performance of this Agreement implies the processing of personal data, both Parties shall comply with the applicable data protection legislation and regulations including GDPR.

2.2 The Controller will ensure that its instructions for the processing shall comply with applicable data protection legislation and regulations including GDPR. Controller shall have sole

responsibility for the accuracy, quality, and legality of personal data and the means by which Controller acquired personal data.

2.3 The Controller agrees that with regard to the processing the Processor may engage Sub - processors compliant with data protection legislation and regulations including GDPR (general consent). Where the Processor engages another Sub-processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in this Agreement shall be imposed on that Sub-processor by way of a contract or other legal act under applicable data protection legislation and regulations including GDPR.

2.4 The Processor shall ensure that any personal data that it processes are kept confidential. All persons authorized by the Processor to process the personal data are under an appropriate obligation of confidentiality and not disclose the personal data to any person other than to its personnel.

2.5 The Processor shall ensure that it implies appropriate technical and organisational measures in such a manner that processing will meet the requirements of applicable data protection legislation and regulations including the protection of the rights of the data subject.

2.6 In accordance with GDPR regulation as the performance of this Agreement the Processor shall in particular:

- assist the Controller in ensuring compliance with the monitoring of the personal data breach obligations resulting from applicable data protection legislation and regulations including GDPR, taking into account the nature of processing and the information available to the Processor;
- promptly notify the Controller about (i) any legally binding request for disclosure of the personal data by a data subject, a judicial or regulatory authority unless otherwise prohibited, such as the obligation under criminal law to preserve the confidentiality of a judicial enquiry, and to assist the Controller therewith (ii) any accidental or unauthorized access, and more in general, any unlawful processing and to assist the Controller therewith;
- at the choice of the Controller, deletes or returns all the personal data to the Controller after the end of the provision of Service relating to processing, and deletes existing copies unless applicable data protection legislation and regulations requires storage of the personal data;
- make available to the Controller all information necessary to demonstrate compliance with the obligations resulting from this Agreement;
- inform the Controller immediately if it believes that any instruction from the Controller infringes applicable data protection legislation and regulations;
- at the request and costs of the Controller, submit its data processing facilities for audits or control of the processing activities including inspections, conducted by the Controller or another auditor mandated by the Controller.

2.7 Personal data processed in the context of this Agreement are processed by servers located in European Union.

2.8 As the transfer of personal data is necessary for the performance of the Service provided by the Processor the Parties shall ensure that the personal data are adequately protected as set forth in Article 49 of the GDPR. In particular the Processor collects and transfers personal data subject to this Agreement by the Controller to fulfil a compelling legitimate interest of the Processor in a manner that does not outweigh Controller's nor end users rights and freedoms. The personal data safeguard system is described more in detail in the Security Practices.

2.9 In order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer of personal data by the Controller to the Processor agrees and warrants:

- to process the personal data only on behalf of the Controller and in compliance with its instructions; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Controller of its inability to comply, in which case the Controller is entitled to suspend the transfer of data and/or terminate this Agreement;
- that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Controller and its obligations under the Agreement and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Agreement, it will promptly notify the change to the Controller as soon as it is aware, in which case the Controller is entitled to suspend the transfer of data and/or terminate this Agreement;

3. Confidentiality

3.1 Both Parties acknowledge that during this Agreement, a Party may become privy to Confidential information which is disclosed by the other Party.

3.2 The receiving Party shall keep all confidential information confidential, in particular the receiving Party shall not disclose any confidential information to any third party and shall not use these information for purposes not resulting from this Agreement.

3.3 Any violation of this section by either of the Parties shall be deemed a material breach of this Agreement.

4. Liability

4.1 The Parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Section 2 by any Party or Sub-processor is entitled to receive compensation from the Controller for the damage suffered.

4.2 Neither Party shall be liable for any indirect or consequential damages, such as (but not limited to) loss of revenue, loss of profit, loss of opportunity, loss of goodwill and third-party claims.

5. General provisions

5.1 This Agreement shall apply to all personal data disclosed to the Processor or otherwise obtained from the Controller from the date of this Agreement until the expiry of the subscription of the Service.

5.2 Where individual provisions of this Agreement are invalid or unenforceable, the validity and enforceability of the other provisions of this Agreement shall not be affected.

List of Exhibit(s) attached and incorporated:

Exhibit 1: Standard Contractual Clauses with Appendix

Exhibit 1 – Standard Contractual Clauses

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a)   The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b)   The Parties:

(i)   the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii)   the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c)   These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d)   The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

---

[1]   Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

Clause 2

Effect and invariability of the Clauses

(a)   These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b)   These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a)   Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii)   Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii)   Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv)   Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v)   Clause 13;

(vi)   Clause 15.1(c), (d) and (e);

(vii)   Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b)   Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a)   Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b)   These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c)   These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a)   An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b)   Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c)   The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1   Instructions

(a)   The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b)   The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2   Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3   Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4   Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5   Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer

shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6   Security of processing

(a)   The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)   The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c)   In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and

further information shall, as it becomes available, subsequently be provided without undue delay.

(d)   The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7   Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8   Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i)   the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)   the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii)   the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)   the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

---

[2]   The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9   **Documentation and compliance**

(a)   The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b)   The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c)   The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d)   The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e)   The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a)   SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least fourteen (14) days' prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. Customer must subscribe to receive notice of updates to the list of Sub-processors, using the link in ANNEX III. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b)   Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data

---

[3]   This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

(a)   The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to

handle complaints. It shall deal promptly with any complaints it receives from a data subject.

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

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

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

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

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

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

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

Clause 12

Liability

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

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

(c)   Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d)   The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e)   Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f)   The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g)   The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a)   [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

        [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

        [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b)   The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a)   The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b)   The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   (i)   the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   (ii)   the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

   (iii)   any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied

---

[4]   As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

during transmission and to the processing of the personal data in the country of destination.

(c)   The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d)   The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e)   The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f)   Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1   Notification

(a)   The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i)   receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include

information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii)   becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b)   If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)   Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d)   The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)   Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a)   The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)   The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of

destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c)   The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)   The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)   The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   (ii)   the data importer is in substantial or persistent breach of these Clauses; or

   (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)   [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to

ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)   Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a)   Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b)   The Parties agree that those shall be the courts of Ireland.

(c)   A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d)   The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

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

<u>**ANNEX I**</u>

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name: The entity identified as Controller in the Agreement or such other agreement between Plumsail Inc. and Controller.

Address: : The Address for the Controller associated with the Plumsail account.

Contact person's name, position and contact details: The contact details associated with the Plumsail Account.

Activities relevant to the data transferred under these Clauses: The activities specified in the Agreement.

Signature and date: By using Plumsail's Service to transfer data to Third Countries, the exporter will be deemed to have signed Annex 1.

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

Name: Plumsail Inc.

Address: 2125 Biscayne Boulevard, Suite 212, Miami, FL 33137, USA

Contact person's name, position and contact details: Dmitry Kozlov, CEO, contact@plumsail.com.

Activities relevant to the data transferred under these Clauses: Plumsail is a cloudbased software-as-a-service provider of collaboration and communication software which processes personal data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and Plumsail.

Signature and date: By processing the data exporter's data on data exporter's instructions, the

data importer will be deemed to have signed this Annex I

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter and/or Data Subjects (as directed by data exporter), may submit Personal Data to the Services concerning the following categories of Data Subjects:

- Prospects, customers business partners and vendors (who are natural persons) of data exporter;
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors;
- Employees, agents, advisors, independent contractors, members and/or freelancers of data exporter; and/or
- Other categories of Data Subjects as expressly determined by the data exporter.

Categories of personal data transferred

Data exporter and/or Data Subjects (as directed by data exporter) may submit Personal Data to the Service, the type, extent and detail of which is determined and controlled by the data exporter and/or the Data Subject in its sole discretion.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data exporter and/or Data Subjects (as directed by data exporter) may submit Sensitive data to the Service, the type, extent and detail of which is determined and controlled by the data exporter and/or the Data Subject in its sole discretion. Plumsail takes the security and privacy of data very seriously. The restrictions and safeguards that apply to all data, including any sensitive data, can be found in Security Practices.

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

Data exporter and/or Data Subjects (as directed by data exporter) may submit Personal Data to the Service either once, or on a continuous basis (for example by making changes to Personal Data) as determined and controlled by the data exporter and/or the Data Subject in its sole discretion.

Nature of the processing

Plumsail processes Personal Data only as necessary to perform the Service and only performs the type(s) of processing as instructed by the data exporter and/or Data Subject and only pursuant to the Agreement, the DPA and these Clauses.

Purpose(s) of the data transfer and further processing

The purposes of the processing are determined solely by the data exporter and/or Data Subject in its sole discretion.

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

Subject to any other terms allowing or requiring longer retention, and subject to Plumsail's normal data retention policies, Plumsail only processes personal data for the duration of the Agreement, unless the data is deleted prior thereto by the data exporter and/or Data Subject.

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

Plumsail transfers Personal Data to sub-processors as set forth in the Data protection section of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be determined in accordance with the GDPR.

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

The privacy of your data is important to Plumsail. The various measures we take 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, can be found in Security Practices.

ANNEX III – LIST OF SUB-PROCESSORS

The Controller has authorized the following list of sub-processors found at https://plumsail.com/sub-processors/.