

DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**Agreement**”) have been entered into between the Customer (“**Customer**” or “**Controller**”) and Proxima Research LLC (“**Proxima**” or “**Processor**”).

Processor and Controller are individually referred to as “Party” and collectively as “Parties”.

The Service Agreement between the Parties requires that that the Processor accesses and processes personal data. This Agreement specifies the obligations of the Parties when Proxima acts as Processor.

The capitalized terms used in this Agreement but not defined herein shall have the same meaning as defined in the Service Agreement. In the event of a conflict between this Agreement and Service Agreement, this Agreement shall prevail.

If you are using any service as an employee, agent or contractor of a corporation, partnership or similar entity, then you represent and warrant that you have authority to sign for and bind such entity in order to accept the terms of this Agreement. The rights granted under this Agreement are expressly conditioned upon acceptance by such authorized personnel.

1. Scope of Contract and Distribution of Responsibilities

- 1.1. The Parties agree that, for Processing Personal Data, the Parties shall be Controller and Processor.
- 1.2. Processor shall Process Personal Data only on behalf of Controller and at all times only in accordance with this Agreement.
- 1.3. Within the scope of the Service Agreement, each Party shall be responsible for complying with its respective obligations as Controller and Processor under Data Protection Laws.

2. Processing Instructions

- 2.1. Processor will Process Personal Data in accordance with Controller's instructions. This Agreement contains Controller's initial instructions to Processor. The Parties agree that Controller may communicate any change in its initial instructions to the Processor by way of written notification to the Processor and that Processor shall abide by such instructions. The Processor shall maintain a secure, complete, accurate and up to date record of all such individual instructions.
- 2.2. Regardless of the foregoing prohibitions, the parties agree that Processor may, and Controller instructs Processor to, process Personal Data for the following activities that are necessary to support the Services Agreement: detect data security incidents; protect against fraudulent or illegal activity; effectuate repairs; and provide, maintain, or improve the quality of the services.
- 2.3. For the avoidance of doubt, any instructions that would lead to processing outside the scope of this Agreement (e.g. because a new Processing purpose is introduced) will require a prior agreement between the Parties and, where applicable, shall be subject to the contract change procedure under the Service Agreement.
- 2.4. Where instructed by Controller, Processor shall correct, delete or block Personal Data.
- 2.5. Processor shall promptly inform the Controller in writing if, in Processor's opinion, an instruction infringes Data Protection Laws and provide an explanation of the reasons for its opinion in writing.
- 2.6. Processor shall not be liable for any DP Losses arising from or in connection with any processing made in accordance with Controller’s instructions following Controller’s receipt of any information provided by Processor in this Section 2.

3. Processor Personnel

- 3.1. Processor will restrict its personnel from Processing Personal Data without authorization. Processor will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

4. Disclosure to Third Parties; Data Subjects Rights

- 4.1. Processor will not disclose Personal Data to any third party (including any government agency, court, or law enforcement) except as set forth in this Agreement or with written consent from Controller or as necessary to comply with applicable mandatory laws. If Processor is obliged to disclose Personal Data to a law enforcement agency or third party, Processor agrees to give Controller reasonable notice of the access request prior to granting such access, to allow Controller to seek a protective order or other appropriate remedy. If such notice is legally prohibited, Processor will take reasonable measures to protect the Personal Data from undue disclosure as if it were Processor's own confidential information being requested and shall inform Controller promptly as soon as possible if and when such legal prohibition ceases to apply.
- 4.2. In case Controller receives any request or communication from Data Subjects which relates to the Processing of Personal Data ("**Request**"), Processor shall provide the Controller with full cooperation, information and assistance ("**Assistance**") in relation to any such Request where instructed by Controller.
- 4.3. Where Processor receives a Request, Processor shall (i) not directly respond to such Request, (ii) forward the request to Controller within 3 (three) business days of identifying the Request as being related to the Controller and (iii) provide Assistance according to further instructions from Controller.

5. Assistance

- 5.1. The Processor assists the Controller in ensuring compliance with the obligations taking into account the nature of Processing and the information available to the Processor.
- 5.2. Where a Data Protection Impact Assessment ("**DPIA**") is required under applicable Data Protection Laws for the Processing of Personal Data, Processor shall provide upon request Controller with reasonable cooperation and assistance needed to fulfill Customer's obligation to carry out a DPIA related to Customer's use of the Services, to the extent that Customer does not otherwise have access to the relevant information and such information is available to Proxima.
- 5.3. The Controller shall pay the Processor reasonable charges mutually agreed between the parties for providing the assistance in Section 5, to the extent that such assistance is not reasonably able to be accommodated within the normal provision of the Services.

6. Information Rights and Audit

- 6.1. Processor shall, in accordance with Data Protection Laws, make available to Controller on request in a timely manner such information as is necessary to demonstrate compliance by Processor with its obligations under Data Protection Laws.
- 6.2. Processor shall, upon reasonable notice, allow for and contribute to inspections of the Processor's Processing of Personal Data (including data processing systems, policies, procedures and records), during regular business hours and with minimal interruption to Processor's business operations. Such inspections are conducted by the Controller, its affiliates or an independent third party on Controller's behalf (which will not be a competitor of the Processor) that is subject to reasonable confidentiality obligations.
- 6.3. Controller shall pay Processor reasonable costs of allowing or contributing to audits or inspections in accordance with Section 6.2 where Controller wishes to conduct more than one audit or inspection every 12 months. Processor will immediately refer to Controller any

requests received from national data protection authorities that relate to the Processor's Processing of Personal Data.

- 6.4. Processor undertakes to cooperate with Controller in its dealings with national data protection authorities and with any audit requests received from national data protection authorities. Controller shall be entitled to disclose this Agreement or any other documents (including contracts with subcontractors) that relate to the performance of its obligations under this Agreement (commercial information may be removed).

7. Data Incident Management and Notification

In respect of Customer data incident Processor shall:

- 7.1. notify Controller of a Personal Data Breach involving Processor or a subcontractor without undue delay (but in no event later than 72 hours after becoming aware of the incident);
- 7.2. make reasonable efforts to identify the cause of such incident and take those steps as Processor deems necessary and reasonable in order to remediate the cause of the incident to the extent that it is within Proxima's reasonable control.
- 7.3. provide reasonable information, cooperation and assistance to Controller in relation to any action to be taken in response to a Personal Data Breach under Data Protection Laws, including regarding any communication of the Personal Data Breach to Data Subjects and national data protection authorities.
- 7.4. The obligations contained in Section 7 should not apply to data incidents that are caused by Customer or Customer's users.

8. International Data Transfer

- 8.1. Data that Proxima processes for the Customer as a Processor may be stored in the EU or outside of the EU depending on the Proxima's product.
- 8.2. Proxima may also process certain data about Customer or its users as a data controller, including in countries outside of the EU, in accordance with Proxima privacy notice available at <https://proximaresearch.com/us/en/proxima-crm-system/>
- 8.3. Where there is international transfer of Personal Data to the Processor in countries which do not ensure an adequate level of data protection the following applies:
 - a) the Parties enter into Standard Contractual Clauses (Exhibit 1) for the transfer of Personal Data in countries which do not ensure an adequate level of data protection in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. The Standard Contractual Clauses will apply to Personal Data originating from Controller (who, for the purposes of the Standard Contractual Clauses shall be deemed the "Data Exporter") that is processed by Processor (who, for the purposes of the Standard Contractual Clauses shall be deemed the "Data Importer"). If there is any conflict between the Standard Contractual Clauses and this Agreement, the Standard Contractual Clauses shall prevail.
 - b) At Controller's request, the Standard Contractual Clauses shall be replaced and the Parties shall execute new standard contractual clauses for transfers to data processors in third countries adopted pursuant to Art. 46 (2) c) or d) GDPR.
 - c) If and as long as the country where Personal Data is transferred to a country which is subject to an adequacy decision according Article 45 (3) GDPR, no Standard Contractual Clauses are required. Once the adequacy decision is repealed or suspended, a) and b) shall automatically apply.

9. Reference to Provisions of the Standard Contractual Clauses

- 9.1. For the technical and organizational measures (TOMs), reference is made to and Annex II of the Standard Contractual Clauses.

9.2. For sub-processing, reference is made to Annex III of the Standard Contractual Clauses. In event of objection by the Controller to the appointment or replacement of any sub processor, Processor will either not appoint or replace the sub processor or, if this is not possible, Controller may suspend or terminate the Service(s) (without prejudice to any fees incurred by Controller prior to such suspension or termination).

10. Term and Termination

10.1. This Agreement becomes effective upon signature. It shall continue to be in full force and effect as long as Processor is processing Personal Data according to Exhibit 1 Annex I and shall cease automatically thereafter.

10.2. The Controller may terminate the Agreement as well as the Service Agreement for cause, at any time upon reasonable notice or without notice, as selected by Controller, if the Processor is in material breach of the terms of this Agreement.

10.3. Where amendments are required to ensure compliance of this Agreements with Data Protection Laws, the Parties shall agree on such amendments upon request of Controller and, for the avoidance of doubt, with no additional costs to Controller. Where the parties are unable to agree upon such amendments, either party may terminate the Service Agreement and this Agreement with 90 days written notice to the other party.

11. Data Export and Retention

11.1. Controller may export all Customer Data prior to the termination of the Customer's Account. In any event, following the termination of the Customer's Account and the Service Agreement, Customer Data will be retained in accordance with the Data Retention Period as defined in the Service Agreement.

12. Miscellaneous

12.1. In case of any conflict, the provisions of this Agreement shall take precedence over the provisions of any other agreement with Processor.

12.2. The limitation of liability stated in the Service Agreement apply to the breach of the Agreement.

12.3. No Party shall receive any remuneration for performing its obligations under this Agreement except as explicitly set out herein or in another agreement.

12.4. Where this Agreement requires a "written notice" such notice can also be communicated per email to the other Party. Notices shall be sent to the contact persons set out in Exhibit 1 Annex I.

12.5. Any supplementary agreements or amendments to this Agreement must be made in writing and signed by both Parties.

12.6. Should individual provisions of this Agreement become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this agreement.

12.7. If Proxima is processing Personal Data within the scope of the CCPA, Proxima makes the following additional commitments to Customer. Proxima will process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the Agreement and as permitted under the CCPA, including under any "sale" exemption. In no event will Proxima sell any such data.

13. Definitions

"**Data Protection Laws**" shall mean the data protection laws of the country in which Controller is established, including the GDPR, CCPA, CPRA and any data protection laws applicable to Controller in connection with the Service Agreement.

“**CCPA**” The California Consumer Privacy Act is a data privacy law that provides California consumers with a number of privacy protections, including right to access, delete, and opt-out of the “sale” of their personal information.

“**CPRA**” The California Privacy Rights Act is a data privacy law that amends and expands upon the CCPA.

“**DP Losses**” means all liabilities, including:

- a) costs (including legal costs);
- b) claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (whether material or non-material, and including for emotional distress);
- c) to the extent permitted by applicable law:
 - i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a data protection authority or any other relevant Regulatory Authority;
 - ii) compensation to a Data Subject ordered by a data protection authority to be paid by Processor;
 - iii) the costs of compliance with investigations by a data protection authority or any other relevant Regulatory Authority.

"**GDPR**" shall mean the 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.

"**Personal Data**" shall mean any information relating to an identified or identifiable natural person as defined by the General Data Protection Regulation of the European Union ("GDPR" EC-2016/679) that is Processed by Processor as part of providing the services to Controller as described in Exhibit 1.

"**Service Agreement**" shall mean the Terms of Service available at <https://proximaresearch.com/us/en/proxima-crm-system/> or a master services agreement executed between the Parties.

"**Standard Contractual Clauses**" mean the standard contractual clauses set forth in Exhibit 1 for the transfer of Personal Data from a Data Controller in the European Economic Area to Processors established in third countries in the form set out in the Annex of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended by incorporating the description of the Personal Data to be transferred and the technical and organizational measures to be implemented as set out in the Appendix.

"**Controller**", "**Data Subject**", "**Personal Data Breach**", "**Processor**" and "**Process**" / "**Processing**" shall have the meaning given to them in the GDPR.

EXHIBIT 1: 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) for the transfer of personal data to a third country.
- (b) The Parties:
- i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and
 - ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)
- have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - iii) Clause 9 – Clause 9(a), (c), (d) and (e);
 - iv) Clause 12 – Clause 12(a), (d) and (f);
 - v) Clause 13;
 - vi) Clause 15.1(c), (d) and (e);
 - vii) Clause 16(e);

viii) Clause 18 – Clause 18(a) and (b);

(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

- a) 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)

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

Clause 7

Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

- a) 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

- a) 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

- a) 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

- a) 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

- a) 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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

- a) 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

- a) The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
 - i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
 - ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
 - iii) the onward transfer is necessary for the establishment, exercise or defense 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.
- b) Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

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

- b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized 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 organizational 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 authorized 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, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data

importer that part of the compensation corresponding to the data importer's responsibility for the damage.

- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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 behavior 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 authorizing 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 authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1. Notification

- a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

- b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2. Review of legality and data minimization

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

- ii) the data importer is in substantial or persistent breach of these Clauses; or
 - iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.
- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

- a) 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 the Slovak Republic.

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 court of Slovak Republic
- (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

ANNEX I

A. LIST OF PARTIES

Data exporter:

Shall be that of the Proxima's Customer described in the Service Agreement.

Role (controller/processor): controller

Data importer:

Name: **Proxima Research LLC**

Address: 12 SE 7th St, unit 703,

Fort Lauderdale, FL 33301, USA

EIN: 37-2049031

office.us@proximaresearch.com

B. DESCRIPTION OF TRANSFER

Personal data as defined in the Service Agreement and imported by the controller into the Services.

Frequency of the transfer.

The frequency of the transfer is on a continuous basis for the duration of the Service Agreement.

Nature of the processing

As defined in the Service Agreement.

Purpose(s) of the data transfer and further processing

Proxima will process Personal Data as necessary to provide the Services pursuant to the Terms of Service or Master Service Agreement, as further specified in the Service Order Form, and as further instructed by the Customer in use of the Services.

Personal Data will be retained during the term of the Agreement and in accordance with the Data Retention Period as defined in the Service Agreement.

For transfers to (sub-)processors ANNEX III LIST OF SUB-PROCESSORS applies.

C. COMPETENT SUPERVISORY AUTHORITY

For the purposes of the Standard Contractual Clauses, the supervisory authority that shall act as competent supervisory authority is either (i) where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR; (ii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Customer's representative is established; or (iii) where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the Data Subjects are predominantly located. In relation to Personal Data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as applicable).

ANNEX II

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

The current technical and organizational Measures (TOMs) shall be provided under the Customer's written demand.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

The current list of subprocesses is available under the Customer's written demand.

- a) If Customer Data are hosted in the EEA datacenter with custom mailbox, only those services are turned on by default, where the specific sub-processor has datacenters in the EEA; however, if Controller chooses to use services like third party integrations and Apps, or Custom Apps, then data is expected to leave the EEA.
- b) Processor intends to use the service of the Proxima group companies as sub processor. The current list of Proxima group companies is available under the Customer's written demand.