

## Supplier Data Processing Addendum

This Data Processing Addendum (“**DPA**”) is entered by and between “**Client**” (as specified in the Agreement) on behalf of itself and its Affiliates, and Prospect Global Ltd [Sopro] (hereinafter, the “**Supplier**”) on behalf of itself and its Affiliates. Client and the Supplier shall be collectively referred to as the “**Parties**” and individually as the “**Party**”.

In consideration of the mutual obligations set out herein, the Parties hereby agree that the Terms and Conditions set out below shall be added as an Addendum integral to the agreement established between Client and the Supplier (the “**Agreement**”).

### 1. DEFINITIONS

In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth opposite each one of them:

- 1.1. “**Affiliate**” means any entity that directly or indirectly controls, is controlled by or is under common control with the subject entity. “**Control**” for the purposes of this definition means direct or indirect ownership or control of at least 50%.
- 1.2. “**Applicable Law(s)**” means all applicable data protection, privacy and electronic marketing legislation, including (as applicable) the GDPR, UK’s Data Protection Act 2018 and Privacy and Electronic Communications (EC Directive) Regulations 2003, as well as any equivalent laws anywhere in the world, to the extent any such laws apply to Personal Data to be processed hereunder by Supplier.
- 1.3. “**Convention**” means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
- 1.4. The terms “**Commission**”, “**Data Subject**”, “**Member State**”, “**Personal Data Breach**”, “**Process/Processing**”, “**Controller**”, “**Processor**”, and “**Supervisory Authority**” shall have the same meanings given to them in the GDPR.
- 1.5. “**GDPR**” means EU General Data Protection Regulation 2016/679 and any subsequent amendments, replacements or supplements. Any references in this DPA to Directive 95/46/EC shall be read as references to the General Data Protection Regulation (2016/679) (the “**Regulation**”), or, as the data exporter is established in the United Kingdom (the “**UK**”), to the Regulation and/or any UK local law which implements or supplements the Regulation, as applicable from time to time, and in each case references to specific articles or provisions of the Directive shall be read as references to the equivalent article or provision in the Regulation or UK local law, where possible and as appropriate.
- 1.6. “**Personal Data**” means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person, which is processed by Supplier on behalf of Client pursuant to or in connection with the Supplier Services.
- 1.7. “**Standard Contractual Clauses**” means the standard contractual clauses for the transfer of personal data to processors or sub-processors established in third countries, as adopted by the European Commission from time to time under Directive 95/46/EC or the GDPR, as applicable, and all related annexes and appendices.

- 1.8. "**Sub-processor**" means any third party engaged directly by the Supplier to Process any Personal Data pursuant to or in connection with the Supplier Services. The term shall not include employees or contractors of Supplier.
- 1.9. "**Supplier Services**" means any services provided by Supplier to Client, including any storage, software or platform services, pursuant to an agreement, purchase order, license or subscription.

## **2. SCOPE OF PROCESSING**

- 2.1. Supplier shall Process Personal Data as described in **Annex 1** (Details of Processing of Personal Data) attached hereto.
- 2.2. Supplier shall Process Personal Data as a Processor or Sub-processor acting on behalf of Client as the Controller or Processor of such Personal Data, as applicable.
- 2.3. Client hereby instructs Supplier to Process Personal Data only for the limited purposes of providing Supplier Services and solely for the benefit of Client.
- 2.4. Supplier shall only Process the Personal Data in accordance with: (i) the terms of this DPA; (ii) the terms of the Agreement between the Parties; (iii) solely on Client's documented instructions, unless Processing is required by Applicable Laws (in which case, Supplier must inform Client in advance of such requirement, unless prohibited to do so by law); and (iv) in compliance with all Applicable Laws.
- 2.5. Supplier shall notify Client without undue delay if Supplier determines that it can no longer meet Client's instructions or its obligations under this DPA.

## **3. SUB-PROCESSING**

- 3.1. Supplier shall not subcontract any Processing of Personal Data to any third party without prior written consent of Client regarding each such subcontracting activity and third party. Notwithstanding the foregoing, Client authorizes Supplier to engage Sub-processors for the limited purposes of Processing Personal Data as strictly necessary for the fulfilment of Supplier's obligations under the Agreement, provided that Supplier:
  - 3.1.1. Provides to Client at least thirty (30) days prior written notice of its intention to engage or replace a Sub-processor. Such notice shall be sent to the email specified in the Agreement, and must include at least: (i) the name of the Sub-processor; (ii) the type of Personal Data Processed by such Sub-processor and for which purposes; (iii) description of the data subjects whose Personal Data shall be Processed by such Sub-processor, and (iv) location of the Data Processing performed by such Sub-processor;
  - 3.1.2. Conducts the level of due diligence necessary to ensure that such Sub-processor is capable of meeting the requirements of this DPA and any Applicable Laws; and
  - 3.1.3. Ensures that the arrangement between the Supplier and the Sub-processor is governed by a written contract binding on the Sub-processor, which (i) requires the Sub-processor to Process Personal Data in accordance with this DPA or standards that are no less onerous than this DPA; and (ii) includes and relies on the Standard Contractual Clauses, which shall form part of the contract between Supplier and its Sub-processors and shall be binding on both Supplier and its Sub-processor, to the extent that any Personal Data may be Processed by such Sub-processor outside of the EEA.
- 3.2. Client may object to the engagement of any Sub-processor on any privacy, data protection or security grounds. In such case, the Supplier shall not engage a Sub-processor for the provision of Supplier

Services to Client, or Client may terminate or suspend its Agreement with Supplier, with immediate effect and without penalty.

3.3. Supplier shall remain fully liable to Client at all times for the performance of any of its Sub-processors' obligations and its Processing activities relating to Personal Data.

#### **4. VENDOR PERSONNEL**

4.1. To the extent permissible under applicable law, Supplier shall conduct an appropriate background investigation of all employees or contractors of the Supplier and who may have access to Personal Data ("**Supplier Personnel**"), prior to allowing them such access. If the background investigation reveals that the Supplier Personnel are not suited to access Personal Data, then Supplier shall not provide the Supplier Personnel with access to Personal Data.

4.2. Supplier shall ensure that all Supplier Personnel: (i) has such access only as necessary for the purposes of providing Client with the Supplier Services and complying with Applicable Laws; (ii) is contractually bound to confidentiality requirements no less onerous than this DPA; (iii) is provided with appropriate privacy and security training; (iv) is informed of the confidential nature of Personal Data, and required to keep it confidential; and (v) is aware of the Supplier's duties and obligations under this DPA.

#### **5. SECURITY**

5.1. Supplier represents and warrants that it has implemented and will maintain all appropriate technical, physical and organisational measures to protect the Personal Data against accidental or unlawful or accidental loss, alteration, destruction, unauthorized disclosure or access and, in particular, where the processing involves the transmission of data over a network, against all anticipated unlawful forms of processing.

5.2. Having regard to the state of the art and cost of their implementation, Supplier agrees and warrants that such measures shall ensure a level of security appropriate to the risks presented by the Processing (including the risks of a Personal Data Breach), and the nature of Personal Data to be protected, and without limitation. Such measures may include:

- 5.2.1. The pseudonymization and/or encryption of Personal Data, in transit and at rest;
- 5.2.2. The ability to ensure the on-going confidentiality, integrity, availability, and resilience of Processing systems and services;
- 5.2.3. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- 5.2.4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

5.3. The Supplier shall keep records of its Processing activities performed on behalf of Client, which shall include at least:

- 5.3.1. The details of the Supplier as Personal Data Processor, any representatives, Sub-processors, data protection officers and Supplier Personnel having access to Personal Data;
- 5.3.2. The categories of Processing activities performed;
- 5.3.3. Information regarding Cross-Border Data Transfers (as further specified in Section 11 of this DPA), if any; and
- 5.3.4. Description of the technical and organizational security measures implemented in respect of the Processed Personal Data.

5.4. Without derogating from Client's Audit Rights under Section 10, Client reserves the rights to inspect the records maintained by the Supplier under this Section 5 at any time.

## **6. DATA SUBJECT RIGHTS**

6.1. Supplier shall reasonably assist Client in responding to requests to exercise Data Subject rights or Consumer rights (including any complaints regarding the Processing of Personal Data) under Applicable Laws, including, without limitation, EU Data Protection Laws.

6.2. Supplier shall:

- 6.2.1. Promptly notify Client if it receives a Data Subject Request in respect of Personal Data;
- 6.2.2. Provide full cooperation and assistance in relation to any Data Subject Request;
- 6.2.3. Ensure that it does not respond to Data Subject Requests except on the documented instructions of Client or as strictly required by Applicable Laws to which the Supplier is subject; and
- 6.2.4. Maintain electronic records of Data Subject Requests (under Applicable Laws).

## **7. LEGAL DISCLOSURE AND PERSONAL DATA BREACH**

7.1. Supplier shall notify Client within 24 hours of Supplier becoming aware of:

- 7.1.1. any request for disclosure of Personal Data by a Supervisory Authority and/or any other law enforcement authority or court unless prohibited under criminal law specifically requiring Supplier to preserve the confidentiality of a law enforcement investigation.
- 7.1.2. any Personal Data Breach reasonably suspected or known to be affecting Personal Data. Supplier shall provide Client with sufficient information to allow Client to meet any obligations to report or inform Data Subjects or data protection authorities of the Personal Data Breach under the Applicable Laws. Other than as required by law, Supplier shall not make any public statements or other disclosures about a Personal Data Breach affecting Personal Data without Client's prior written consent, which may be provided, at Client's discretion, on a case-by-case basis.

7.2. Supplier shall provide Client with the following details, as soon as possible:

- 7.2.1. The nature of the Personal Data Breach, including the categories of Data Subjects concerned and the categories of Personal Data and data records concerned;
- 7.2.2. The measures proposed or taken by Supplier in cooperation with Client to address the Personal Data Breach; and
- 7.2.3. The measures Client could take to mitigate the possible adverse effects of the Personal Data Breach.

7.3. Supplier shall take any actions necessary to investigate any suspected or actual Personal Data Breach and mitigate any related damages.

7.4. Supplier shall fully cooperate with Client and take such steps as are directed by Client to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

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

8.1. Upon expiration or termination of the provision of Supplier Services, Supplier shall, at Client's request, promptly delete or return all copies of Personal Data in its and/or any of its Sub-processors'

possession or control, except as required to be retained in accordance with Applicable Laws. In such a case, Supplier warrants that it will guarantee the confidentiality of that Personal Data and will not actively process that Personal Data anymore, and will guarantee the return and/or destruction of the Personal Data as requested by Client when the legal obligation to not return or destroy the information is no longer in effect.

8.2. Upon Client's prior written request, the Supplier's Chief Privacy Officer or equivalent shall provide written certification to Client that Supplier has fully complied with this section.

## 9. PROVISION OF INFORMATION AND ASSISTANCE

Supplier shall cooperate and reasonably assist Client with any data protection impact assessments, prior consultations regarding relevant competent data protection authorities and with any other assistance related to compliance with Client's obligations pursuant to the GDPR and other Applicable Laws. The scope of such assistance shall be limited to the Processing of the Personal Data by the Supplier.

## 10. AUDIT RIGHTS

10.1. Supplier shall promptly make available to Client, upon written request, all information necessary to demonstrate compliance with this DPA and with any Applicable Laws, including industry-standard third-party audit certifications.

10.2. Supplier shall allow for and contribute to audits, including inspections, by Client and/or an auditor mandated by Client. In any event, a third-party auditor shall be subject to confidentiality obligations. Supplier may object to the selection of the auditor if it reasonably believes that the auditor does not guarantee confidentiality, security or otherwise puts at risk the Supplier's business.

## 11. CROSS-BORDER DATA TRANSFER

11.1. Personal Data may be transferred from EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland; collectively, "**EEA**"), Switzerland and the United Kingdom ("**UK**"), to countries that offer adequate levels of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, Member States or the European Commission, or Switzerland or the UK ("**Adequacy Decisions**") as applicable, without any further safeguard being necessary.

11.2. If the Processing of Personal Data by Processor includes transfers (either directly or via onward transfer) from the EEA, Switzerland and/or the UK to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Supplier for the lawful transfer of personal data (as defined in the GDPR or the equivalent Swiss or UK law, as applicable) outside the EEA, Switzerland or the UK, as applicable, then the Standard Contractual Clauses shall apply. The Standard Contractual Clauses, as they apply to the Agreement, can be found here <https://contracts.sopro.io/gdpr-scc>.

11.3. Where the transfer of Personal Data is made subject to the Standard Contractual Clauses, these shall be considered completed and signed simultaneously with the execution of this DPA by Client and Supplier. The "**data importer**" thereunder shall be Client, and the "**data exporter**" shall be Supplier. Supplier shall, and shall ensure that each Sub-processor engaged in the Processing of such Personal Data shall, comply with the data importer's obligations, and Client shall comply with the data exporter obligations, in each case under the applicable Standard Contractual Clauses. If requested by Client, Supplier will ensure and procure that its Sub-processor(s) enter into Standard Contractual Clauses with Client directly.

11.4. The Standard Contractual Clauses will not apply to Personal Data that relates to individuals located outside of the EEA, or that is not transferred, either directly or via onward transfer, outside the EEA. For data transfers originating from other countries outside of the EEA, Supplier shall abide by all Applicable Laws of the territory of origin of the Personal Data.

11.5. Supplier shall provide Client with all relevant information to enable Client to comply with its obligations in case of cross-border transfers of Personal Data. Client may object to the transfer of Personal Data under this Section 11 on privacy and security grounds. In such case, the Supplier shall not effectuate such transfer of Personal Data or Client may terminate or suspend the provision of Supplier Services with immediate effect without penalty, with exception of any Sub-processor(s) listed in this initial agreement in Annex 1.

## 12. MISCELLANEOUS

12.1. **Severance:** Should any provision of this DPA be determined invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be: (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible; (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

12.2. **Notice:** All notices required under this DPA shall be sent to Client via the email specified in the Agreement.

Notices to Supplier shall be sent to [dpo@sopro.io](mailto:dpo@sopro.io).

**Order of Precedence:** In the event of any conflict between the terms of this DPA and other documents binding on Parties, the terms of these documents will be interpreted according to the following order of precedence: (i) the Standard Contractual Clauses, solely to the extent applicable in accordance with Section 11 above; (ii) any terms of agreement, purchase orders, license or subscription, pursuant to which Supplier Services are provided; (iii) this DPA.

12.3. **Modifications by Supplier:** Supplier may, by at least forty-five (45) calendar days' prior written notice to Client, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under any Data Protection Laws, to allow Processing of Personal Data to be made (or continue to be made) without breach of that Data Protection Law. Pursuant to such notice, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the lawful requirements identified in Supplier's notice as soon as is reasonably practicable.

12.4. **Modifications by Client:** Client may, by at least thirty (30) calendar days' prior written notice to Supplier, vary the terms of this DPA and/or any Standard Contractual Clauses applicable pursuant to Section 11 of this DPA, as necessary to allow the Processing of Personal Data to be made (or continue to be made) without breach of applicable Data Protection Laws as reasonably determined by Client at its discretion. If Supplier objects to said variations within the notice period, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Client's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within 30 days of such notice, then Client may, by written notice to the other Party, with immediate effect and without penalty, terminate the Agreement to the extent that it relates to the Supplier Services which are affected by the proposed variations (or lack thereof).



## ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA

This Annex includes certain details of the processing of Personal Data.

**Description of Supplier Services:** Provision of prospect and lead generation services.

**Duration of the processing:** For as long as Supplier Services are provided and as defined the Service Order.

**The nature and purpose of the processing:** Storage and other Processing required to support prospecting services. Disclosure in accordance with the Agreement and/or as compelled by Applicable Laws.

**Types of personal data processed:** Personal data including name, email address, employment details, phone numbers and other professional/business related data. The Parties do not anticipate the transfer of sensitive data.

**Categories of data subjects:** Data subjects are business contacts and Client's team members.

**List of sub-processors in the following format:**

Name of Sub-processor	Services Performed	Sub-processor Location	Purpose of Processing	DPA in place with Sub-processor (yes or no)
Sopro LTD Skopje	Software development, operational support, administrative support, business development and project management.	Republic of North Macedonia	Provision of related services and any operational support.	Yes, with SCCs