**Data Processing Addendum and Standard Contractual Clauses**

# **RECITAL**

This Data Processing Addendum [hereinafter**:“DPA”**] is entered by and between **Instant EU GDPR Representative LTD**, a limited company, registered in Dublin, Ireland, with registry number K78 X5P8 and **GDPR Local LTD.** a limited company, registered in Brighton, England, under registry number 12969035, collectively referred to as the **“Parties”** and individually to as the **“Party”**

WHEREAS

(a) Instant EU GDPR Representative LTD acts as the Data Controller, as defined in Section 2 of this DPA;

(b) GDPR Local LTD acts as the Data Processor, as defined in Section 2 of this DPA;

(c) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data;

(d) The Parties wish to lay down their rights and obligations.

This DPA, including its Annexes is supplemental to, and forms part of the Written Agreement [hereinafter the **“Agreement”**], when the Agreement is concluded between the Data Controller and a customer of Data Controller for the purpose of providing Data Controller Services, as defined in clause 2, as defined in clause 2 of this DPA.

# **DEFINITIONS**

# Capitalized definitions not otherwise defined herein shall have the meaning given to them in the General Data Protection Regulation (2016/679) of the European Parliament and of the Council.

# For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:

“**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 Data Processor;

 **“Data Controller”** means the entity determining the means and purpose of processing of Personal Data;

 **“Data Controller Services”** means EU Representative Services, GDPR Consultancy and associated services;

 **“Data Processor”** means the entity processing Personal Data on behalf of the Data Controller;

 **“Data Processor Services”** means UK Representative Services;

**“GDPR”** means EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council and any subsequent amendments, replacements, or supplements.

**“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 the Data Processor on behalf of the Data Controller pursuant to or in connection with the Data Controller Services;

“**Processing Services**” means any services provided by the Data Processor to the Data Controller, including any storage, software or platform services, pursuant to an agreement, purchase order, license or subscription.

**“Services”** means Data Controller Services and Data Processor Services collectively;

“**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 the GDPR, as applicable, and all related annexes and appendices, which together form an integral part of this DPA and are attached as **Annex 2 (ANNEX 2: STANDARD CONTRACTUAL CLAUSES)** hereto, as may be updated from time to time;

**“Sub-processor”** means any third party engaged directly by the Data Processor to process any Personal Data pursuant to or in connection with the Data Processor Services. The term shall not include employees or contractors of Data Processor;

# **SCOPE OF PROCESSING**

* 1. The Data Processor shall process Personal Data as described in **Annex 1** (**ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA**) attached hereto;
	2. The Data Processor shall process Personal Data as a Processor or Sub-processor acting on behalf of Data Controller as the Controller or Processor of such Personal Data, as applicable;
	3. The Data Controller hereby instructs Data Processor to process Personal Data only for the limited purposes of providing Data Processor Services and solely for the benefit of Data Controller;
	4. The Data Processor 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 documented instructions from the Data Controller, unless processing is required by Applicable Laws (in which case, the Data Processor must inform the Data Controller in advance of such requirement, unless prohibited to do so by law), and (iv) in compliance with all Applicable Laws;
	5. The Data Processor shall notify the Data Controller without undue delay if the Data Processor determines that it can no longer meet instructions of the Data Controller or its obligations under this DPA.

# **SUB-PROCESSING**

* 1. The Data Processor shall not subcontract any processing of Personal Data to any additional third party without prior written consent of the Data Controller regarding each such subcontracting activity and third party. Notwithstanding the foregoing, the Data Controller authorizes the Data Processor to engage Sub-processors without limitation for the limited purposes of processing Personal Data as strictly necessary for the fulfillment of Data Processor ’s obligations under the Agreement, provided that Data Processor:
* provides to the Data Controller 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 nominated Data Controller contact, 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;
* conducts the level of due diligence necessary to ensure that such Sub-processor can meet the requirements of this DPA and any Applicable Laws; and
* ensures that the arrangement between the Data Processor 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 Data Processor and its Sub-processors and shall be binding on both Data Processor and its Sub-processor, to the extent that any Personal Data may be Processed by such Sub-processor outside of the EEA.
	1. The Data Controller may object to the engagement of any Sub-processor on reasonable privacy, data protection or security grounds. In such case, the Data Processor shall only engage a Sub-processor for the provision of the Data Processor Services to the Data Controller after completing appropriate risk assessment and ensuring appropriate technical and organisational controls are in place. Should the Data Controller object to the engagement of the Sub-processor, the Data Controller may terminate or suspend its Agreement with the Data Processor, with immediate effect and without penalty.
	2. The Data Processor shall remain fully liable to the Data Controller at all times for the performance of any of its Sub-processors’ obligations and its processing activities relating to Personal Data.

# **DATA PROCESSOR PERSONNEL**

* 1. To the extent permissible under applicable law, the Data Processor shall conduct an appropriate background investigation of all employees or contractors of the Data Processor and who may have access to Personal Data [hereinafter: **“Data Processor Personnel”**]**,** prior to allowing them such access. If the background investigation reveals that the Data Processor Personnel are not suited to access Personal Data, then the Data Processor shall not provide the Data Processor Personnel with access to Personal Data.
	2. The Data Processor shall ensure that all Data Processor Personnel: (i) has such access only as necessary for the purposes of providing the Data Controller with the Data Processor 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 the Personal Data, and required to keep it confidential; and (v) is aware of the Data Processor 's duties and obligations under this DPA.

# **SECURITY**

* 1. The Data Processor represents and warrants that it has implemented and will maintain appropriate technical, physical and organizational 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.
	2. Having regard to the state of the art and cost of their implementation, the Data Processor 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 shall ensure that such measures include:
* the pseudonymization and/or encryption of Personal Data, in transit and at rest;
* the ability to ensure the on-going confidentiality, integrity, availability, and resilience of processing systems and services;
* 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
* a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
	1. The Data Processor shall keep records of its processing activities performed on behalf of Data Controller, which shall include at least:
* the details of the Data Processor as Personal Data Processor , any representatives, Sub-processors, data protection officers and Data Processor Personnel having access to Personal Data;
* the categories of processing activities performed;
* information regarding cross-border data transfers (as further specified in Section 11 of this DPA), if any; and description of the technical and organizational security measures implemented in respect of the processed Personal Data.
	1. Without derogating form Data Controller’s Audit Rights under Section 10 (**PROVISION OF INFORMATION AND ASSISTANCE**), Data Controller reserves the rights to inspect the records maintained by the Data Processor under this Section 5 (**DATA PROCESSOR PERSONNEL**) at any time.

# **DATA SUBJECT RIGHTS**

* 1. The Data Processor shall reasonably assist the Data Controller 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 (**Data Subject Request(s)**”).
	2. The Data Processor shall:
* promptly notify Data Controller if it receives a Data Subject Request in respect of Personal Data;
* provide full cooperation and assistance in relation to any Data Subject Request;
* ensure that it does not respond to Data Subject Requests except on the documented instructions of Data Controller or as strictly required by applicable laws to which the Data Processor is subject; and
* Maintain electronic records of Data Subject Requests (under Applicable Laws).

# **LEGAL DISCLOSURE AND PERSONAL DATA BREACH**

* 1. The Data Processor shall notify the Data Controller within 24 hours after becoming aware of:
* 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 Data Processor to preserve the confidentiality of a law enforcement investigation;
	+ 1. any Personal Data breach reasonably suspected or known to be affecting Personal Data. The Data Processor shall provide the Data Controller with sufficient information to allow the Data Controller to meet any obligations to report or inform the Data Subjects or data protection authorities of the Personal Data breach under the Applicable Laws. Other than as required by law, Data Processor shall not make any public statements or other disclosures about a Personal Data breach affecting Personal Data without Data Controller’s prior written consent, which may be provided, at Data Controller’s discretion, on a case-by-case basis.
	1. The Data Processor shall provide the Data Controller with the following details, as possible:
* The nature of the Personal Data Breach, including the categories of Data Subjects concerned and the categories of Personal Data and data records concerned;
* The measures proposed or taken by Data Processor in cooperation with Data Controller to address the Personal Data Breach; and
* The measures Data Controller could take to mitigate the possible adverse effects of the Personal Data Breach.
	1. The Data Processor shall take any actions necessary to investigate any suspected or actual Personal Data breach and mitigate any related damages.
	2. The Data Processor shall fully cooperate with the Data Controller and take such steps as are directed by Data Controller to assist in the investigation, mitigation, and remediation of each such Personal Data breach.

# **DELETION OR RETURN OF PERSONAL DATA**

* 1. Upon expiration or termination of the provision of the Data Processor’s services, the Data Processor shall, at the choice of the Data Controller, 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, the Data Processor warrants that it will guarantee the confidentiality of the Personal Data and will not actively process Personal Data anymore and will guarantee the return and/or destruction of the Personal Data as requested by the Data Controller when the legal obligation to not return or destroy the information is no longer in effect.
	2. Upon prior written request by the Data Controller, the Data Processor ’s Chief Privacy Officer or equivalent shall provide written certification to Data Controller that Data Processor has fully complied with this section.

# **PROVISION OF INFORMATION AND ASSISTANCE**

The Data Processor shall cooperate and reasonably assist the Data Controller with any data protection impact assessments, prior consultations regarding relevant competent data protection authorities and with any other assistance related to compliance with the obligations of the Data Controller 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 Data Processor.

# **AUDIT RIGHTS**

* 1. The Data Processor shall promptly make available to the Data Controller, upon written request, all information necessary to demonstrate compliance with this DPA and with any Applicable Laws, including industry-standard third-party audit certifications.
	2. The Data Processor shall allow for and contribute to audits, including inspections, by the Data Controller and/or an auditor mandated by the Data Controller. In any event, a third-party auditor shall be subject to confidentiality obligations. The Data Processor may object to the selection of an auditor if it reasonably believes that the auditor does not guarantee confidentiality, security or otherwise puts at risk the Data Processor ’s business.

# **CROSS-BORDER DATA TRANSFER**

* 1. Personal Data may be transferred from European Union (“EU”) to countries that offer adequate levels of data protection under or pursuant to the adequacy decisions published by the relevant data of EU (“Adequacy Decisions”) as applicable, without any further safeguard being necessary;
	2. If the Processing of Personal Data by the Data Processor includes transfers from EU 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 Data Processor for the lawful transfer of personal data as defined in the GDPR, then the Standard Contractual Clauses shall apply;
	3. Where the transfer of Personal Data is made subject to the Standard Contractual Clauses, these shall be completed and signed simultaneously with the execution of this DPA by the Data Controller and the Data Processor. The Data Processor shall ensure that each Sub-processor engaged in the processing of such Personal Data shall comply with the Data Processors’s obligations of the SCCs and the Data Controller shall comply with the Data Controller’s obligations, in each case under the applicable Standard Contractual Clauses. If requested by the Data Controller, the Data Processor will ensure and procure that its Sub-processor(s) enter into Standard Contractual Clauses with the Data Controller directly;
	4. The Standard Contractual Clauses will not apply to Personal Data that relates to individuals located outside of the UK and 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 UK and EEA, Data Processor shall abide by all Applicable Laws of the territory of origin of the Personal Data;
	5. Data Processor shall provide the Data Controller with all relevant information to enable the Data Controller to comply with its obligations in case of cross-border transfers of Personal Data. The Data Controller may object to the transfer of Personal Data under this Section 11 (**AUDIT RIGHTS**) on privacy and security grounds. In such case, the Data Processor shall not effectuate such transfer of Personal Data or Data Controller may terminate or suspend the provision of Data Processor Services with immediate effect without penalty.

# **INDEMNIFICATION**

* 1. The Data Processor shall indemnify, to the extent provided by Data Processor’s Personal Identifiable Information [hereinafter: **“PII”**], defend, and hold harmless the Data Controller and it’s respective officers, directors, and employees from and against claims and proceedings and all liability, loss, costs, fines, and expenses (including reasonable legal fees) arising in connection with (i) Data Processor ’s unlawful or unauthorized Processing, destruction of, or damage to any Personal Data; and/or (ii) Data Processor ’s (including the Data Processor Personnel and Data Processor ’s Sub-processors) failure to comply with its obligations under this DPA, the existing Agreement or any further instructions as to such Processing given in writing by Data Controller in accordance to this DPA.

# **MISCELLANEOUS**

* 1. This DPA, including the attached SCC, may be executed in counterparts, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same agreement. Delivery of an executed counterpart of a signature page to this DPA by fax or by email of a scanned copy, or execution and delivery through an electronic signature service (such as DocuSign), shall be effective as delivery of an original executed counterpart of this DPA.
	2. 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.
	3. Notice: All notices required under this DPA shall be sent to the Data Controller by email.
	4. Notices to the Data Processor shall be sent to: contact@gdprlocal.com
	5. 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) this DPA; (iii) any terms of agreement, purchase orders, license or subscription, pursuant to which Data Processor Services are provided.
	6. Modifications by the Data Processor : the Data Processor may by at least forty-five (45) calendar days' prior written notice to the Data Controller, 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 Data Processor ’s notice as soon as is reasonably practicable.
	7. Modifications by the Data Controller: the Data Controller may by at least thirty (30) calendar days’ prior written notice to Data Processor , 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, or to otherwise protect the interests of Data Controller, in each case as reasonably determined by Data Controller at its discretion. If Data Processor 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 notice from the Data Controller 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 the Data Controller 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 Data Processor Services which are affected by the proposed variations (or lack thereof).

IN WITNESS WHEREOF, this DPA is entered into and becomes binding between the Parties with effect from the date first set out above.

|  |
| --- |
| **On behalf of the Controller:** |
| Full Name: Adam Brogden |
| Position: Director |
| Address: Office 2 12A Lower Main Street, Lucan Co. Dublin K78 X5P8 Ireland  |
| Other information necessary in order for the contract to be binding (if any): |
| Signature: Adam Brogden |
|  |
| **On behalf of the Processor:** |
| Full Name: Zlatko Delev |
| Position: Compliance Team Lead |
| Address: 1st Floor Front Suite, 27-29 North Street, Brighton, England BN1 1EB  |
| Other information necessary in order for the contract to be binding (if any): |
| Signature: Zlatko Delev |

#

# **ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA**

This **Annex 1** includes certain details of the processing of Personal Data.

**Description of Data Importer Services:** processing personal data from the Data Exporter in order to provide Services, as defined in Clause 2 of this DPA.

**Duration of the processing:** as long as the Data Importer Services are provided.

**The nature and purpose of the processing:** the nature and purpose of the processing is to provide the services for our client in order to be compliant with UK Data Protection Act, GDPR and related data protection regulations.

**Types of personal data processed: Data to be processed includes contact details of the Data Exporter and data subjects plus data related to the processing of requests, complaints, and other interactions resulting from provision of the services. This includes: data subject’s** name, contact details, email, phone number, payment details, billing address, and interactions by emails / phone / post etc.….

# **ANNEX 2: STANDARD CONTRACTUAL CLAUSES**

# **(Controller to Processors)**

Clause 1: **Purpose and scope:**

1. The Data Exporter and the Data Importer, as defined below, or in other agreement or addendum effectively governing the processing of Personal Data by the Data Importer on behalf of the Data Exporter, including all annexes, exhibits and appendices thereto, each a "**Party**"; and collectively the "**Parties**", have agreed on the following Contractual Clauses ("**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Annex.I.
2. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

**Definitions**

Capitalized definitions not otherwise defined herein shall have the meaning given to them in the GDPR and in the DPA. Except as modified or supplemented below, the definitions of the DPA shall remain in full force and effect.

For the purposes of the Clauses:

**“Data Exporter”** means the entity, based in EU/EEA or in a third country transferring the Personal Data;

**“Data Importer”** means the entity in a third country receiving the Personal Data from the Data Exporter;

**“The Subprocessor”** means any processor engaged by the Data Importer or by any other Subprocessor of the Data Importer who agrees to receive from the Data importer or from any other Subprocessor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

**“Technical and Organisational Security Measures”** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: **Effect and invariability of the Clauses**

1. 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 GDPR and, with respect to data transfers from controllers to processors standard contractual clauses pursuant to Article 28(7) of GDPR, provided they are not modified. 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.
2. 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 8.1(b), 16(a), (c), (d) and (e);

(iii) Clause 17(a), (c), (d) and (e);

(iv) Clause 20(a), (d) and (f);

(v) Clause 21;

(vi) Clause 23.1(c), (d) and (e);

(vii) Clause 24(e);

(viii) Clause 26(a) and (b);

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

Clause 4: **Interpretation**

(a) These Clauses shall be read and interpreted in the light of the provisions of GDPR.

(b) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in GDPR.

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**

The details of the transfer, and in particular the categories of Personal Data that are transferred and the purpose 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.

Clause 8: **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.

Clause9: **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.

Clause 10: **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 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 GDPR.

Clause 11: **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.

Clause 12: **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 22, in particular the requirement for the Data Importer under Clause 22 (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 22(a).

Clause 13: **Security of processing**

* 1. 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 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.
	2. 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.
	3. 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.
	4. The Data Importer shall cooperate with and assist the Data Exporter to enable the Data Exporter to comply with its obligations under GDPR 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.

Clause 14: **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.

Clause 15: **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 (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, or if:

* + - 1. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of GDPR that covers the onward transfer;
			2. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of GDPR with respect to the processing in question;
			3. 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
			4. 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.

Clause 16: **Documentation and compliance**

* 1. 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.
	2. 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 GDPR. 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.
	3. In fulfilling its obligations under paragraphs (a) and (b), the Data Importer shall comply with the instructions from the Data Exporter.
	4. The Data Importer shall allow for and contribute to audits by the Data Exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the Data Exporter requests an audit on instructions of the controller. In deciding on an audit, the Data Exporter may take into account relevant certifications held by the Data Importer.
	5. Where the audit is carried out on the instructions of the controller, the Data Exporter shall make the results available to the controller.
	6. 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.
	7. 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 17: **Use of sub-processors**

* 1. 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 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. 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.
	2. 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 15. The Data Importer shall ensure that the sub-processor complies with the obligations to which the Data Importer is subject pursuant to these Clauses.
	3. 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.
	4. 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.
	5. 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 18: **Data subject rights**

* 1. 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.
	2. (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 GDPR. 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.
	3. (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 19: **Redress**

* 1. 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.
	2. 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.
	3. 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:
		+ 1. 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 21;
			2. (ii) refer the dispute to the competent courts within the meaning of Clause 26.
			3. (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 GDPR.
			4. The Data Importer shall abide by a decision that is binding under the applicable EU or Member State law.
			5. (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 20: **Liability**

* 1. Each Party shall be liable to the other Party for any damages it causes the other Party by any breach of these Clauses.
	2. 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.
	3. 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 GDPR or Regulation (EU) 2018/1725, as applicable.
	4. 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.
	5. 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.
	6. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party that part of the compensation corresponding to its responsibility for the damage.
	7. The Data Importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 21: **Supervision**

* 1. The supervisory authority with responsibility for ensuring compliance by the Data Exporter with GDPR as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
	2. 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.

**LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

Clause 22: **Local laws and practices affecting compliance with the Clauses**

* 1. 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 GDPR, are not in contradiction with these Clauses.
	2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
		+ 1. 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;
			2. 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;
			3. any relevant contractual, technical or organisational 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.
	3. 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.
	4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
	5. 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).
	6. 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. 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 23(d) and (e) shall apply.

Clause 23: **Obligations of the data importer in case of access by public authorities**

**23.1 Notification**

* 1. 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:
		+ 1. 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
			2. 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.
	2. 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.
	3. 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.).
	4. 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.
	5. Paragraphs (a) to (c) are without prejudice to the obligation of the Data Importer pursuant to Clause 22(e) and Clause 24 to inform the Data Exporter promptly where it is unable to comply with these Clauses.

**23.2 Review of legality and data minimisation**

* 1. The Data Importer agrees to review the legality of the request for disclosure, in partucular 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 22(e).
	2. 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.
	3. 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.

**FINAL PROVISIONS**

Clause 24: **Non-compliance with the Clauses and termination**

* 1. The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these Clauses, for whatever reason.
	2. 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 21(f).
	3. The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
		+ 1. 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;
			2. the Data Importer is in substantial or persistent breach of these Clauses; or
			3. the Data Importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
	4. 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.
	5. 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.
	6. 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.
	7. 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 GDPR that covers the transfer of personal data to which these Clauses apply; or (ii) GDPR 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 GDPR.

Clause 25: **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 26: **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.

**On behalf of the Data Exporter:**

|  |
| --- |
| Full Name: Adam Brogden |
| Position: Director |
| Address: Office 2 12A Lower Main Street, Lucan Co. Dublin K78 X5P8 Ireland  |
| Other information necessary in order for the contract to be binding (if any): |
| Signature: Adam Brogden |
|  |
| **On behalf of the Data Importer:** |
| Full Name: Zlatko Delev |
| Position: Team Lead |
| Address: 1st Floor Front Suite, 27-29 North Street, Brighton, England BN1 1EB  |
| Other information necessary in order for the contract to be binding (if any): |
| Signature: Zlatko Delev |
|  |

**APPENDIX**

**ANNEX I.**

1. **List of Parties**

1.

**Data exporter**

Name: Instant EU GDPR Representative LTD

Address: Office 2 12A Lower Main Street, Lucan Co. Dublin K78 X5P8 Ireland

Contact person’s name, position and contact details: … Adam Brogden, Director, adam@gdprlocal.com

Signature and date: **ADAM BROGDEN**; 13/12/2021

Role: controller and processor

2. …

**Data importer**

Name: GDPR Local LTD

Address: 1st Floor Front Suite, 27-29 North Street, Brighton, England

Contact person’s name, position and contact details: Zlatko Delev, Compliance Team Lead, zlatko.delev@gdprlocal.com

Signature and date: **ZLATKO DELEV**; 13/12/2021

Role: processor

1. **Description of transfer**

**Categories of data subjects whose personal data is transferred**: employees, clients, their suppliers and third parties, regulators, data subjects that make a request, and other companies and agencies that may be involved.

**Categories of personal data transferred:** contact details of the Data Exporter and data subjects plus data related to the processing of requests, complaints, and other interactions resulting from provision of the services. This includes data subject’sname, contact details, email, phone number, payment details, billing address, and interactions by emails / phone / post etc.….

**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. We do not routinely collect or store sensitive personal data. However, where this occures we will assure we take the appropriate measures to protect that sensitive data.

**The frequency of the transfer** (e.g., whether the data is transferred on a one-off or continuous basis). Data is transferred on an ad-hoc basis, as required.

**Nature of the processing**: the nature and purpose of the processing is to provide the services for our client in order to be compliant with UK Data Protection Act, GDPR and related data protection regulations.

**Purpose(s) of the data transfer and further processing:** to provide EU/UK Representative Services, GDPR Consultancy and associated services.

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:** as long as the Data Importer Services are provided.

**For transfers to (sub-) processors**, also specify subject matter, nature and duration of the processing: As required for providing the services.

1. **Competent Supervisory Authority**

The competent supervisory authority is the **Ireland Information Comissioner**:

**Office of the Information Commissioner,**

**6 Earlsfort Terrace,**

**Dublin 2, D02 W773,**

**Ireland.**

**ANNEX II:**

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

Description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

All data is stored in an encrypted Sql Server database hosted in a Microsoft Azure data centre (London).  Access to the data is only provided through our internal platforms which have role and user-based authentication, with access denied by default and granted to campaign teams only.

Encryption – Data stored in our databases is encrypted both in transit and at rest. All computers used for the business have encrypted hard drives.

Access to hub – 2FA – 2FA is available for all users however is not enforced.

Access controls – appropriate access controls have been -   functional/data – Data access is limited by the organisational structure and so is the functional access (regarding SodaStream and Hub). We use “Roles” to appoint different kinds of permissions to different levels of employee access.

Physical security – we have established appropriate physical access controls across all locations as required to protect data assets. – The datacentres used are very secure - full details on the level of physical security can be found here:  <https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security>.

**ANNEX III – LIST OF SUB-PROCESSORS**

The Data Importer and the Data Exporter have authorised the use of the following sub-processors:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name of Sub-processor** | **Services Performed** | **Sub-processor Location** | **Purpose of Processing** | **DPA in place with Sub-processor****(yes or no)** |
| Sopro d.o.o | Software development, operational support, administrative support, business development, project management. | North Macedonia | Development, support, operation, and consultancy for our GDPR and related services. | YesDPA and SCCs |
| Sopro Ltd | Software development, operational support, administrative support, business development, project management. | UK | Business development | YesDPA |
| Sopro Holdings | Software development, operational support, administrative support, business development, project management. | UK | Business development and operations. | YesDPA |