Our DPA and SCCs

This Data Processing Addendum, including its Schedules and Appendices, ("DPA") forms part of the Written Agreement or other written or electronic agreement between MBN Solutions and Customers of our services .

If the Customer entity signing this DPA is a party to the Written Agreement, this DPA is an addendum to and forms part of the Written Agreement between us.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations.

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

This DPA has been pre-signed on behalf of MBN Solutions. The Standard Contractual Clauses in Schedule3 have been pre-signed by MBN Solutions, where applicable, as the data importer.

To complete this DPA, Customer must complete the information in the signature box and sign where indicated. To register this document send the signed DPA to MBN Solutions by email to GDPR@mbnsolutions.com

Upon receipt of the validly completed DPA by MBN Solutions at this email address, this DPA will become legally binding. For the avoidance of doubt, signature of the DPA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices.

MBN Solutions - Vendor Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered by and between MBN Solution's clients (hereinafter, "**Company**") on behalf of itself and its Affiliates, and MBN Solutions (hereinafter, the "**Vendor**") on behalf of itself and its Affiliates. Company in the text below will be referred to as the "**Parties**", and individually as **"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 Company and the Vendor (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 Vendor.

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.

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 Vendor on behalf of Company pursuant to or in connection with the Vendor 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, which together form an integral part of this DPA and are attached as **Annex 2** hereto, as may be updated from time to time.

1.8. "**Sub-processor**" means any third party engaged directly by the Vendor to Process any Personal Data pursuant to or in connection with the Vendor Services. The term shall not include employees or contractors of Vendor.

1.9. "**Vendor Services**" means any services provided by Vendor to Company, including any storage, software or platform services, pursuant to an agreement, purchase order, license or subscription.

2. SCOPE OF PROCESSING

2.1. Vendor shall Process Personal Data as described in **Annex 1** (Details of Processing of Personal Data) attached hereto.

2.2. Vendor shall Process Personal Data as a Processor or Sub-processor acting on behalf of Company as the Controller or Processor of such Personal Data, as applicable.

2.3. Company hereby instructs Vendor to Process Personal Data only for the limited purposes of providing Vendor Services and solely for the benefit of Company.

2.4. Vendor 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 Company, unless Processing is required by Applicable Laws (in which case, Vendor must inform Company in advance of such requirement, unless prohibited to do so by law), and (iv) in compliance with all Applicable Laws.

2.5. Vendor shall notify Company without undue delay if Vendor determines that it can no longer meet instructions of the Company or its obligations under this DPA.

3. SUB-PROCESSING

3.1. Vendor shall not subcontract any Processing of Personal Data to any additional third party without prior written consent of Company regarding each such subcontracting activity and third party. Notwithstanding the foregoing, Company authorizes Vendor to engage Sub-processors without limitation for the limited purposes of Processing Personal Data as strictly necessary for the fulfillment of Vendor's obligations under the Agreement, provided that Vendor:

3.1.1. Provides to Company at least thirty (30) days prior written notice of its intention to engage or replace a Sub-processor. Such notice shall be sent the nominated Company 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;

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 Vendor 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 Vendor and its Sub-processors and shall be binding on both Vendor and its Sub-processor, to the extent that any Personal Data may be Processed by such Sub-processor outside of the EEA.

3.2. Company may object to the engagement of any Sub-processor on reasonable privacy, data protection or security grounds. In such case, the Vendor shall only engage Sub-processor for the provision of Vendor Services to the Company after completing appropriate risk assessment and ensuring appropriate technical and organisational controls are in place. Should Company object to the engagement

of the Sub-processor, Company may terminate or suspend its Agreement with Vendor, with immediate effect and without penalty.

3.3. Vendor shall remain fully liable to Company 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, Vendor shall conduct an appropriate background investigation of all employees or contractors of the Vendor and who may have access to Personal Data ("**Vendor Personnel**"), prior to allowing them such access. If the background investigation reveals that the Vendor Personnel are not suited to access Personal Data, then Vendor shall not provide the Vendor Personnel with access to Personal Data.

4.2. Vendor shall ensure that all Vendor Personnel: (i) has such access only as necessary for the purposes of providing Company with the Vendor 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 Vendor's duties and obligations under this DPA.

5. SECURITY

5.1. Vendor 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.

5.2. Having regard to the state of the art and cost of their implementation, Vendor 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:

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 Vendor shall keep records of its Processing activities performed on behalf of Company, which shall include at least:

5.3.1. The details of the Vendor as Personal Data Processor, any representatives, Sub-processors, data protection officers and Vendor 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 form Company's Audit Rights under Section 10, Company reserves the rights to inspect the records maintained by the Vendor under this Section 5 at any time.

6. DATA SUBJECT RIGHTS

6.1. Vendor shall reasonably assist Company 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)**").

6.2. Vendor shall:

6.2.1. Promptly notify Company 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 Company or as strictly required by Applicable Laws to which the Vendor 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. Vendor shall notify Company within 24 hours of Vendor 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 Vendor 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. Vendor shall provide Company with sufficient information to allow Company 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, Vendor shall not make any public statements or other disclosures about a Personal Data Breach affecting Personal Data without Company's prior written consent, which may be provided, at Company's discretion, on a case by case basis.

7.2. Vendor shall provide Company with the following details, 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 Vendor in cooperation with Company to address the Personal Data Breach; and

7.2.3. The measures Company could take to mitigate the possible adverse effects of the Personal Data Breach.

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

7.4. Vendor shall fully cooperate with Company and take such steps as are directed by Company 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 Vendor Services, Vendor shall, at the choice of the Company , 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, Vendor warrants that it will guarantee the confidentiality of 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 Company when the legal obligation to not return or destroy the information is no longer in effect.

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

9. PROVISION OF INFORMATION AND ASSISTANCE

Vendor shall cooperate and reasonably assist Company 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 Company 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 Vendor.

10. AUDIT RIGHTS

10.1. Vendor shall promptly make available to Company, 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. Vendor shall allow for and contribute to audits, including inspections, by Company and/or an auditor mandated by Company. In any event, a third-party auditor shall be subject to confidentiality obligations. Vendor 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 Vendor's business.

11. CROSS-BORDER DATA TRANSFER

11.1. Personal Data may be transferred from United Kingdom ("**UK**"), to countries that offer adequate levels of data protection under or pursuant to the adequacy decisions published by the relevant data of UK ("**Adequacy Decisions**") as applicable, without any further safeguard being necessary.

11.2. If the Processing of Personal Data by Processor includes transfers from 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 Vendor for the lawful transfer of personal data as defined in the UK GDPR, then the Standard Contractual Clauses shall apply.

11.3. 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 Company and Vendor. The "**data importer**" thereunder shall be Vendor, and the "**data exporter**" shall be Company. Vendor 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 Company shall comply with the data exporter obligations, in each case under the applicable Standard Contractual Clauses. If requested by Company, Vendor will ensure and procure that its Sub-processor(s) enter into Standard Contractual Clauses with Company directly.

11.4. 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, Vendor shall abide by all Applicable Laws of the territory of origin of the Personal Data.

11.5. Vendor shall provide Company with all relevant information to enable Company to comply with its obligations in case of cross-border transfers of Personal Data. Company may object to the transfer of Personal Data under this Section 11 on privacy and security grounds. In such case, the Vendor shall not effectuate such transfer of Personal Data or Company may terminate or suspend the provision of Vendor Services with immediate effect without penalty.

12. INDEMNIFICATION

12.1. Vendor shall indemnify, to the extent provided by Vendor's PII, defend, and hold harmless Company, its Affiliates, and their 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) Vendor's unlawful or unauthorized Processing, destruction of, or damage to any Personal Data; and/or (ii) Vendor's (including the Vendor Personnel and Vendor'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 Company in accordance to this DPA.

13. MISCELLANEOUS

13.1. **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.

13.2. **Notice**: All notices required under this DPA shall be sent to Company by email.

Notices to Vendor shall be sent to: GDPR@mbnsolutions.com .

13.3. **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 Vendor Services are provided.

13.4. **Modifications by Vendor**: Vendor may by at least forty-five (45) calendar days' prior written notice to Company, 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 Vendor's notice as soon as is reasonably practicable.

13.5. **Modifications by Company**: Company may by at least thirty (30) calendar days' prior written notice to Vendor, 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 Company, in each case as reasonably determined by Company at its discretion. If Vendor 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 Company 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 Company 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 Vendor 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 Customer:

Full Name: .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature: .....

On behalf of the Vendor:

Full Name: .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature: .....

ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA

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

Description of Vendor Services: (Explain your services)

Duration of the processing: (duration)

The nature and purpose of the processing: (info)

Types of personal data processed: (info)

List of sub-processors:

Name of Sub-processor	**Services Performed**	**Sub-processor Location**	**Purpose of Processing**	**DPA in place with Sub-processor** **(yes or no)**

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

(Controller to Processors)

The data exporter and the data importer, as defined under the Data Processing Addendum or 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 ("**DPA**"), each a "**party**"; together 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 Appendix 1.

Clause 1 - Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) '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;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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 - Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 - Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 - Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 - Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7 - Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 - Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 - Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 - Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 - Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 - Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Full Name: .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature: .....

On behalf of the data importer:

Full Name: .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature: .....

EXHIBIT A to ANNEX 2: FURTHER PROVISIONS

A. **General Data Protection Regulation**: References throughout these Clauses to Directive 95/46/EC shall be read as references to the General Data Protection Regulation (2016/679) (the "**Regulation**"), or, if 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.

B. **Onward Subprocessing**: For the purposes of Clause 11 of these Clauses, the data exporter hereby consents to the data importer subcontracting any or all of its data processing operations performed under these Clauses in accordance with the DPA.

C. **Data importers established in 'adequate' countries**: To the extent that the data importer is the recipient of personal data pursuant to these Clauses and is:

(i) established in a jurisdiction recognised by the European Commission (or, if the data exporter is established in the UK, then recognized by the relevant authorities in the UK) as providing an adequate level of protection for personal data, the terms of the DPA concerning transfers of personal data to other countries shall apply, such that these Clauses will apply solely on onward transfer of the imported data to the data importer's sub-processors that are located in a jurisdiction not recognised by the European Commission as providing an adequate level of protection for personal data; or

(ii) established in a jurisdiction not recognised by the European Commission as providing an adequate level of protection for personal data, the Clauses shall apply to the data importer directly.

D. **Data exporters established outside the European Economic Area**: To the extent the data exporter pursuant to these Clauses is established in a jurisdiction outside the European Economic Area, these Clauses shall apply solely in respect of transfers of personal data concerning individuals residing within the European Economic Area. In such cases, references to "Member State" shall be read as references to the Member State applicable in respect of the data exporter's processing activities in relation to these Clauses which concern personal data of individuals residing within the European Economic Area.

E. **Instructions**: For the purposes of Clause 5(a) of the Standard Contractual Clauses, the processing described in the DPA and any other mutually agreed upon written instrument by data exporter and data importer constitute as data exporter's instructions to data importer at the time of entering the DPA and/or such written instrument, to process Personal Data on data exporter's behalf. Any additional or alternate instructions shall be subject to the terms of the DPA.

F. **Suspension of Data Transfers and Termination**: If, pursuant to Clause 5(a), the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall provide notice to the data importer and provide data importer with 14 days to cure the non-compliance ("**Cure Period**"). If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instances where it

considers there is a material risk of harm to data subjects or their personal data. Notwithstanding any other terms in this Section F, in the event these Clauses cease to be an appropriate safeguard for the transfer of the personal data in accordance with the applicable data protection law by virtue of a binding decision by a competent supervisory authority, the terms of the DPA concerning modifications necessary pursuant to legislative and regulatory changes shall apply.

G. **Data importer's assistance**: In the event the data exporter seeks to conduct any assessment of the adequacy of these Clauses for the protection of the personal data being transferred, the data importer shall provide reasonable assistance to the data exporter for the purpose of any such assessment.

H. **Audit Rights**: Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) and Clause 12.2 by instructing data importer to comply with the audit measures described in the DPA.

APPENDIX 1
to the Standard Contractual Clauses

Data exporter

The data exporter is the Controller of the personal data being exported, i.e. either the entity identified as "Company" or "Controller" in the DPA, or Company's customer.

Data importer

The data importer is the entity processing Personal Data on behalf of the data exporter under the DPA, and any of its Sub-processors (as such term is used in the DPA).

Data subjects

The personal data transferred concern the categories of data subjects defined in the DPA.

Categories of data

The personal data transferred concern the categories of data defined in the DPA.

Processing operations

The personal data transferred will be subject to the basic processing activities defined in Annex 1 to the DPA.

APPENDIX 2
to the Standard Contractual Clauses

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.

End