Data Processing Agreement

BACKGROUND

This Data Processing Agreement (**DPA**) is entered into by the Client and the Supplier. The DPA shall form part of and is incorporated into the agreement entered into between the parties pursuant to which the Supplier shall provide services to the Client (**Service Agreement**). The term of this DPA will follow the term of the Service Agreement. Terms not otherwise defined in this DPA will have the meaning as set forth in the Service Agreement.

In the event of any conflict between this DPA and the Service Agreement, this DPA shall prevail in all matters relating to the protection of Personal Data.

AGREED TERMS

1. Definitions and interpretation

1.1. The following definitions apply in this DPA.

Applicable Law: any laws or regulations, regulatory policies, guidelines or industry standards or codes of practice which apply to this DPA or its subject matter and are in force from time to time and which have the force of law.

Associated Company: means in relation to a party, any 'subsidiary' or 'holding company' from time to time of that party and any subsidiary from time to time of a holding company of that party (as such terms are defined in section 1159 of the UK Companies Act 2006) and any company 'connected' with that party from time to time (as such term is defined in **section 1122 of the UK Corporation Tax Act 2010**). In relation to the Supplier the companies listed in our Privacy Notice shall be considered Associated Companies.

Data Protection Legislation: means the 'General Data Protection Regulation (EU) 2016/679' and where data subjects are a resident of: -

- the UK this includes the UK Data Protection Act 2018
- Canada: the 'Personal Information Protection and Electronic Documents Act (PIPEDA)' and any applicable provincial laws including the Act respecting the protection of personal information in the private sector (Quebec) ("Quebec Privacy Law")'
- Australia: the 'Privacy Act 1988' and the 'Australian Privacy Principles (APPs)'
- US: the 'California Consumer Privacy Act (CCPA)'.

Data Protection Particulars: means any particularities related to the protection of Personal Data under this DPA, and which are, in particular described in the Data Protocol.

Data Protocol: a protocol setting out the types of personal data which may be processed by the Supplier in the performance of the Services, the subject matter and purposes of the processing, and the duration of the processing, as set out in Schedule 1 and any further data protocol which is agreed in writing and signed by the parties.

Data Subject: means a person who can be identified, directly or indirectly, by any of the Personal Data.

EU-UK-Swiss-GDPR: the European Economic Area (EEA), United Kingdom, Swiss or other jurisdiction where the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing

of personal data and on the free movement of such data and repealing Directive 95/46/EC or equivalent applicable Data Protection Legislation.

Personal Data: means "personal data," "personal information," "protected health information," "non-public personal information," or other similar terms as defined by Data Protection Legislation, which is processed by the Supplier under or in connection with the Service Agreement, the types of such data as are set out in Schedule 1 or in a Data Protocol.

Personal Data Breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized use, or disclosure of, or access to, Personal Data processed by the Supplier.

Person in Charge of Privacy: has the meaning set for the person in charge of the protection of personal information in Quebec Privacy Law.

Regulator: regulator having regulatory or supervisory authority over any part of the Services, or the Client and/or any of its Associated Companies' or the Supplier's business.

Services: the services provided by the Supplier under the Service Agreement.

Standard Contractual Clauses and UK Addendum: the: (i) European Commission's standard contractual clauses for exporting personal data to a processor or controller located outside the EEA (4 June 2021); and (ii) UK International Data Transfer Addendum to the European Commission standard contractual clauses or the UK International Data Transfer Agreement for the exporting of personal data to a processor or controller located outside the UK, each as may be updated or amended from time to time.

Supplier: Shall mean the supplier which has agreed to provide the Services in accordance with the Service Agreement.

1.2. The terms "**controller**", "**processor**", "**process**", "**data protection impact assessment**", "**third country**" and "**international organisation**" shall each have the applicable meaning set out in the Data Protection Legislation, or the usual legal meaning given to these terms in Data Protection Legislation, if these terms are not defined in the Applicable Law governing this DPA.

1.3. References to clauses are to the clauses of this DPA.

1.4. A reference to a statute or statutory provision is a reference to it as amended, extended, or re-enacted from time to time and shall include all subordinate legislation made from time to time under that statute or statutory provision.

1.5. Any words following the terms "**including**", "**include**", "**in particular**", "**for example**" or any similar phrase shall be construed as illustrative and shall not limit the generality of the related words.

2. Data Relationship

2.1. The Supplier and Client agree and acknowledge that for the purpose of the Data Protection Legislation, the Client is the controller, and the Supplier is the processor of the data in Schedule 1 (Data Protocol). The Client acknowledges and agrees that any of the Supplier's Associated Companies may process Personal Data on the Supplier's behalf and that, in such circumstances, the relevant Supplier's Associated Company shall act as a Sub-Processor.

2.2. Each of the parties acknowledges and agrees that Schedule 1 (Data Protocol) of this Agreement is an accurate description of the Data Protection Particulars.

3. Data Processing Obligations

3.1. The Client warrants and undertakes to comply with its obligations under the Data Protection Legislation and that it shall not instruct the Supplier to process Personal Data where such processing would be unlawful.

3.2. The Client warrants and undertakes all necessary consents were obtained before disclosing Personal Data to the Supplier, or where exceptions to obtaining such consents are provided for by Data Protection Legislation, the Client warrants and undertakes that all conditions of such exceptions are complied with, in particular considering the jurisdictions where the Personal Data is processed by the Supplier.

3.3. The Supplier shall only process Personal Data on behalf of the Client as is described in, and for the purposes set out in, Schedule 1 and any other applicable Data Protocol. The Supplier will not process any Personal Data on behalf of the Client for any other purpose or process any other Personal Data on behalf of the Client, without their clear instruction. In the event that the Supplier requires access to or identifies a need to process any other Personal Data in order to provide the Services, it shall notify the Client. Once a Data Protocol has been agreed, it shall form part of and be incorporated into this DPA. In the event of a conflict between this DPA and the Data Protocol, the Data Protocol will prevail.

3.4. The Supplier shall comply with its obligations under the Data Protection Legislation and shall not do any act or omission which causes the Client to breach any of its obligations under the Data Protection Legislation. Without prejudice to the foregoing, the Supplier shall:

a) notify the Client in writing if there are any changes to the types of Personal Data that will be processed by the Supplier or the ways in which the Personal Data will be processed by the Supplier under or in connection with the Service Agreement;

b) process the Personal Data only to the extent, and in such a manner, as is necessary for the provision of the relevant Services under the Service Agreement and the performance of the Supplier's obligations under this Agreement, and shall not process the Personal Data for any other purpose;

c) process the Personal Data in accordance with the terms of this Agreement, the terms of the Service Agreement, lawful Clients' written instructions from time to time, and any applicable Data Protocol, unless otherwise required by Applicable Law or any regulatory body of competent jurisdiction (in which case the Supplier shall inform the Client of that legal requirement before processing, unless prohibited under Applicable Law);

d) notify the Client in writing if the Supplier, acting reasonably, believes (i) it has been provided with any instruction to process Personal Data in breach of Data Protection Legislation; or (ii) it cannot comply, or has reason to suspect it will not be able to comply, with any of the conditions in this Agreement or any additional safeguards put in place pursuant to clause 6.2(a); or (iii) laws applicable to the territory in which Personal Data is processed will undermine the protections provided to Personal Data by virtue of relevant Data Protection Legislation any other Applicable Law to which the Supplier is subject;

e) comply with any request from the Client requiring the Supplier to amend, transfer or delete the Personal Data, except if prohibited by Data Protection Legislation and in such case, the Supplier Shall justify the denial of such request;

f) maintain, and on the Client's request, provide to the Client, full details in writing of its data processing activities in respect of the Personal Data as is required by the Client to demonstrate compliance with the Data Protection Legislation and the terms of this Agreement;

g) unless required to do so by law, not disclose the Personal Data to any Data Subject or to any other person other than at the request of the Client or as provided for within this Agreement;

h) implement appropriate technical and organisational measures including but not limited to those set out in the relevant Data Protocol linked in Schedule 1, to ensure the security of Personal Data against unauthorised or unlawful processing and accidental loss, destruction, or damage, and a level of security appropriate to the data security risks presented by processing such personal data; and taking into account the data protection by design and data protection by default principles under the Data Protection Legislation, shall ensure that the processing of such personal data will meet the requirements of the Data Protection Legislation and protect the rights of the Data Subjects. The Supplier may change these security measures at any time without notice so long as it maintains a comparable or better level of security;

i) regularly review, test, assess, analyse, and update the technical and organisational measures implemented pursuant to clause 3.2(h) in order to ensure that the processing of the Personal Data is performed in accordance with the Data Protection Legislation.

4. Data Notification and Breach Reporting Obligations

4.1. Supplier shall promptly notify the Client by email, and in any event within forty-eight hours upon becoming aware of any actual or suspected Personal Data Breach, and shall:

a) implement any reasonable measures deemed necessary to isolate the data breach;

b) where necessary assist the Client to make any notifications to the Regulator and affected Data Subjects;

4.2. Notwithstanding the above, any automatic or random cyberattack including, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing or other similar incidents that result in no unauthorized access to the Client's Personal Data or to any of the Supplier's equipment or facilities storing the Client's Personal Data, shall not constitute a Personal Data Breach or attempt for which the Supplier has to notify the Client.

4.3. Supplier shall notify the Client promptly following its receipt of any Data Subject request which relates directly to Personal Data under this DPA, and shall:

a) unless prohibited by Applicable Law, not disclose any Client data in response to any Data Subject request without the Client's prior written consent;

b) provide the Client with reasonable co-operation and assistance required in relation to any such request;

c) in the event that the Client is the Data Controller and that the Client is able to respond to Data Subject requests for access, modification and correction of

Personal Data, using its own access to the Service, the Supplier will redirect the Data Subject request to the Client.

5. Sub-processor Obligations

5.1. Supplier shall be permitted to appoint sub-processors in accordance with Supplier's obligations under this Agreement, provided always, that:

a) supplier undertakes due diligence on the proposed sub-processors, to ensure that they can implement the appropriate technical and organisational measures that the processing will meet the requirements of the Data Protection Legislation and ensure the protection of the rights of the Data Subjects.

b) Other than for the sub-processor already used by the Supplier at the time this DPA is signed by the Parties, and other than for the Associated Companies, the list of which may be updated from time to time by the Supplier, the Supplier will notify the Client prior to appointing a new sub-processor. The Client may object to a new sub-processor within 14 days of such notification, provided such objection is based on reasonable data protection grounds.

c) Supplier shall make reasonable efforts to find an acceptable alternate solution to any objection pursuant to clause 5.1(b). The Client must collaborate with the Supplier and take reasonable account of the alternative solutions.

5.2. Details of the Supplier's sub-processors for which the Client's authorisation has been obtained at the time of this DPA are set out in Schedule 1.

6. Data Transfer Obligations

6.1. The Client acknowledges that the Supplier may transfer and process Personal Data to a third-country or territory.

6.2. For Personal Data subject to the EU-UK-Swiss-GDPR, in respect of any transfer of Personal Data to a third country, territory or an international organisation which has not been granted: (a) 'data adequacy' status by the relevant supervisory authority or data protection authority, the Supplier shall:

a) put in place appropriate safeguards to ensure an adequate level of protection of Client data;

b) assist the Client in the undertaking, completion and review of any transfer impact assessment in respect of the relevant transfer;

c) undertake a transfer impact assessment in respect of any restricted transfer by the Supplier to an authorised sub-processor and provide a copy of the same to the Client upon request.

The parties agree that the EU Commission Standard Contractual Clauses and the UK International Data Transfer Addendum ("UK Addendum") provide appropriate safeguards pursuant to clause 6.2(a).

7. Supplier Personnel

7.1. The Supplier shall ensure that access to the Personal Data by its employees is limited to those of its employees who need access to the Personal Data to meet the Supplier's obligations under the Service Agreement and/or this Agreement and in the case of any access by any employee, to such parts of the Personal Data as is strictly necessary for performance of that employee's duties.

7.2. The Supplier shall take reasonable steps to ensure the reliability of its employees who have access to the Personal Data, shall ensure such employees comply with the Supplier's obligations under this Agreement and that their access is revoked once no longer required.

8. Audit

8.1. The Supplier shall permit the Client to audit the Suppliers compliance with its obligations under this Agreement on reasonable notice of 30 days prior to the audit, provided that:

a) The Client shall reimburse the Supplier for any time or resources expended for any such audit;

b) Before the commencement of any such audit both parties shall mutually agree upon the scope, timing, duration, and cost of the audit.

8.2. The Supplier shall provide all necessary assistance to conduct such audits.

8.3. The Client shall, within 5 business days of the audit taking place, notify the Supplier of any non-compliance identified during the course of an audit.

8.4. The Client may not request more than one audit during a 24-month period.

8.5. Under no circumstance may such audit allow the Client access to Personal Data or other confidential information that is not information that has been provided by the Client to the Supplier.

9. Liability and Indemnity

9.1. The Supplier's total liability shall in all circumstances be limited in accordance with the Service Agreement or, if no liability cap is detailed in the Service Agreement, the Suppliers' liability will be limited to an amount equal to 100% of the amount actually paid by the Client to the Supplier under the Service Agreement in the 12 months preceding the date on which the claim arose.

9.2. The Client shall indemnify and keep fully indemnified the Supplier at all times against all liabilities, costs (including legal costs on an indemnity basis), expenses, damages, and losses (including any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and other costs and expenses suffered or incurred by the Supplier arising from any breach of this DPA by the Client.

10. Post Termination

10.1. The Supplier shall only be permitted to process the Personal Data for so long as such processing is required under this Agreement, or as required by Data Protection Legislation or other Applicable Law.

10.2. Upon termination of the Service Agreement, the Supplier shall delete all Personal Data processed under the Service Agreement in accordance with the data retention requirement set out in Schedule 1. Notwithstanding anything to the contrary contained in this Agreement, the Supplier shall not be required to purge electronic documents in its electronic archiving system or backups, provided that all such Client's Personal Data shall be deleted at the end of its normal deletion cycle.

10.3. In all cases where the Supplier continues to have access to the Client's Personal Data, the Supplier will remain subject to the obligations set out in this Agreement.

11. Governing Law and Jurisdiction

11.1. The formation, construction, performance, validity, and all aspects whatsoever of this Agreement (including any claim, dispute or matter arising under or in connection with it or its enforceability, whether or not contractual) shall be governed by English law.

11.2. Each Party irrevocably submits to the exclusive jurisdiction of the courts of England and Wales over any claim or matter arising under, or in connection with, this Agreement.

12. Amendments to this Agreement

12.1. This DPA may be amended by the Supplier at any time, *a*ny such amendment may be communicated to the Client via email and shall be published on our website.

Schedule 1

The data protocols applicable to Clients signing up for our services are outlined and linked by the specific Associated Company below. Both parties agree that the relevant data protocol, as referenced and detailed for each service in the Service Agreement, shall govern the processing of data. Each party acknowledges and agrees to comply with the specified data protocol for the services utilised by the Client, as stipulated in the Service Agreement.

Citation Cyber

https://citationcyber.com/data-protocol

Citation ISO Certification

https://www.qmsuk.com/data-protocol

Citation Limited

https://www.citation.co.uk/data-protocol

Food Alert Limited

https://www.foodalert.com/data-protocol

HS Direct

https://www.hsdirect.co.uk/data-protocol

iHasco

https://ihasco.co.uk/data-protocol

Careskills Academy

https://careskillsacademy.co.uk/data-protocol

SMAS

https://smasltd.com/data-protocol

Timetastic

https://timetastic.co.uk/data-protocol

uCheck

https://www.ucheck.co.uk/data-protocol

Disclosure Services

https://disclosureservices.com/data-protocol/

Schedule 2 – Quebec Contract Clauses

The provisions of this Schedule shall only apply if and to the extent the Quebec Privacy Law applies to the provision of services under the Service Agreement.

1. Supplier shall promptly notify the Client by email, and in any event within forty-eight hours upon becoming aware of any actual or suspected Personal Data Breach, and any attempt of a Personal Data Breach, and shall:

a) notify the Person in Charge of Privacy, using its contact details indicated on the Client's website, unless otherwise instructed by the Client;

2. For Personal Data subject to the Quebec Privacy Law, the servers where the Client's Personal Data are stored are located exclusively in the jurisdictions set out on our website here (the "Processing Jurisdictions") and such Personal Data are only processed in these Processing Jurisdictions. It is the Client's responsibility to ensure that Personal Data disclosed to the Supplier can be transferred or accessed within or from the Processing Jurisdictions.

3. For the purpose of clause 8.1 reference to Client shall include the Person in Charge of Privacy.

Schedule 3 - CCPA Contract Clauses

The provisions of this Schedule shall only apply if and to the extent the CCPA applies to the provision of services under the Service Agreement.

1. The Supplier acknowledges that it is acting as a Service Provider under the CCPA and agrees to comply with the applicable provisions of the CCPA.

2. The Supplier shall not:

    a) Sell Personal Data.

    b) Retain, use, or disclose the Personal Data for any purpose other than for the specific purpose of performing the services specified in the Agreement, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the services specified in the agreement.

3. The supplier shall assist the Data Controller in responding to verifiable consumer requests to exercise their rights under the CCPA, including access, deletion, and opt-out requests, to the extent the Data Controller does not have the ability to address a consumer request independently.

4. The Supplier shall promptly inform the Data Controller if it receives a consumer request directly and provide reasonable assistance, as necessary, to enable the Data Controller to comply with such requests.