Definitions

Capitalised terms used but not defined in this DPA will have the meanings provided in the Agreement. The following defined terms are used in this DPA:

“Agreement” means as applicable the Client Engager Business and Services Agreement as amended from time to time.

“Data Protection Requirements” means the GDPR, UK Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

“DPA Terms” or “DPA” means the terms in this DPA.

“GDPR” means Regulation (EU) 2016/679 of the European Parliament as transposed into UK Law by virtue of being a “Retained Regulation” under the European Union Withdrawal) Act 2018.

“GDPR Terms” means the terms in Attachment 1, under which Client Engager makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

“Personal Data” means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Processed” or “Product Data” means Personal Data uploaded to the Product by the Customer.

“Product” means the online Client Engager service.

“Subprocessor” means other processors used by Client Engager to process Personal Data, including any subcontractor that processes Personal Data.

Lower case terms used but not defined in this DPA, such as “personal data breach”, “processing”, “controller”, “processor”, “profiling”, “personal data”, and “data subject” will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies. The terms “data importer” and “data exporter” have the meanings given in the Standard Contractual Clauses.

General Terms

Compliance with Laws
Client Engager will comply with all laws and regulations applicable to its provision of the Product including security breach notification law and Data Protection Requirements. However, Client Engager is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to accounting service providers of a similar nature to Client Engager.

Customer must comply with all laws and regulations applicable to its use of the Product, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Product is appropriate for storage and processing of information subject to any specific law or regulation and for using the Product in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of the Product.

Data Protection Terms

Scope
The DPA Terms apply to all Products except as described within this section.

Nature of Data Processing; Ownership
Client Engager will use and otherwise process Product Data to provide Customer with access to and use of the Product. As between the parties, Customer retains all right, title and interest in and to Product Data. Client Engager acquires no rights in Product Data, other than the rights Customer grants to Client Engager in this section. This paragraph does not affect Client Engager's rights in Products Client Engager licenses to Customer.

Processing to Provide Customer the Product
For purposes of this DPA, "to provide" Product consists of:

- Delivering the Product access and use by Customer, including providing technical support. For the removal of doubt, providing technical support will include making improvements to the underlying Client Engager products and services subscribed to or utilized by Customer based on issues identified during delivery of the Product.
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified during delivery of the Product); and
- Ongoing improvement of Product subscribed to or utilized by Customer (maintaining the Product, making improvements to the reliability, efficacy, quality, and security of the Product and fixing software defects).

Disclosure of Processed Data
Client Engager will not disclose or provide access to any Processed Data except: (1) as Customer permits; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Product Data; (b) Personal Data included in Product Data; and (c) any other data processed by Client Engager in connection with the Product that is Customer's confidential information under the Agreement. All processing of Processed Data is subject to Client Engager's obligation of confidentiality under the Agreement.

Client Engager will not disclose or provide access to any Processed Data to law enforcement bodies unless required by law. If a law enforcement body contacts Client Engager with a demand for Processed Data, Client Engager will attempt to redirect the law enforcement body to request that data directly to Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Client Engager will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Client Engager will promptly notify Customer unless prohibited by law. Client Engager will reject the request unless required by law to comply. If the request is valid, Client Engager will attempt to redirect the third party to request the data directly from Customer.

Client Engager will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Client Engager is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Client Engager may provide Customer's basic contact information to the third party.

Processing of Personal Data; GDPR
All Personal Data included in Product Data and provided to Client Engager by, or on behalf of, Customer through an engagement with Client Engager to obtain Product is also Product Data. Pseudonymized identifiers may also be generated through IT systems and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent Client Engager is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in Attachment 1 govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and Client Engager agree that Customer is the controller of Personal Data and Client Engager is (except as set out below) the processor of such data, except when Customer acts as a processor of Personal Data, in which case Client Engager is a subprocessor. When Client Engager acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its Agreement (including this DPA Terms and any applicable updates), along with the Product documentation and Customer's use of the Product,) are Customer's complete instructions to Client Engager for the processing of Personal Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's Agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Client Engager that Customer's instructions, including appointment of Client Engager as a processor or subprocessor, have been authorized by the relevant controller. Client Engager shall use Personal Data as controller for the purposes of (a) granting, tracking, auditing and managing access; (b) billing; (c) entering, managing and enforcing the Agreement; (d) protecting its rights; (e) communications with Users and Customers; (f) marketing the Customer using legitimate interest; (f) managing requests or complaints; (g) updating and implementing its systems; (h) such other uses as are required by law or under legitimate interest.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA.
- **Duration of the Processing.** The duration of the processing shall be in accordance with the terms of the DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Product pursuant to Customer's Agreement;
- **Categories of Data.** The types of Personal Data processed by Client Engager when providing Product include: (i) Personal Data that Customer elects to include in Product Data; and (ii) those expressly identified in Article 4 of the GDPR. The types of Personal Data that Customer elects to include in Product Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in "Data Subjects and Categories of Personal Data" in Appendix B
- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers and their relations and employees and others and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in "Data Subjects and Categories of Personal Data" in Appendix B

Data Subject Rights; Assistance with Requests

Client Engager will make available to Customer, in a manner consistent with the functionality of the Product and Client Engager's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Client Engager receives a request from a Customer's data subject to exercise one or more of its rights under the GDPR in connection with the Product for which Client Engager is a data processor or subprocessor, Client Engager will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality provided to Customer for that purpose. Client Engager shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires Client Engager to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Client Engager and keep it accurate and up-to-date. Client Engager may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Client Engager will implement and maintain appropriate technical and organizational measures to protect Product Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Client Engager Security Policy.

Data Encryption

Product Data (including any Personal Data therein) in transit over public networks between Customer and Client Engager, or between Client Engager data centers, is encrypted by default.

Data Access
Client Engager employs least privilege access mechanisms to control access to Product Data (including any Personal Data therein). Client Engager maintains Access Control mechanisms described in the table entitled "Security Measures" in Appendix A – Notices. Role-based access controls are employed to ensure that access to Product Data required for service operations is for an appropriate purpose and approved with management oversight.

Customer Responsibilities
Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for Product meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Client Engager provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls.

Auditing Compliance
Client Engager will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Product Data from time to time.

The Client Engager Audit Report will be Client Engager's Confidential Information and not be disclosed.

Nothing in this section of the DPA varies or modifies the Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Requirements. Client Engager Corporation is an intended third-party beneficiary of this section.

Security Incident Notification
If Client Engager becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Product Data while processed by Client Engager (each a "Security Incident"), Client Engager will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's business contacts for the Product by any means Client Engager selects, including via email. It is Customer's sole responsibility to ensure Customer's business contacts maintain accurate contact information.

Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Client Engager shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Client Engager's notification of or response to a Security Incident under this section is not an acknowledgement by Client Engager of any fault or liability with respect to the Security Incident.

Customer must notify Client Engager promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Professional Services.

Data Transfers
Personal Data that Client Engager processes on Customer's behalf may be transferred to, and stored and processed outside the UK/EU in any other country in which Client Engager or its Subprocessors operate. Customer appoints Client Engager to perform any such transfer of Product Data to any such country and to store and process Personal Data in order to provide the Product.

All transfers of Personal Data, out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Product shall be governed by the Standard Contractual Clauses implemented by Client Engager. In addition, transfers from the United Kingdom may be governed by any IDTA implemented by Client Engager. For purposes of this DPA, the "IDTA" means the International data transfer addendum to the European Commission's standard contractual clauses for international data transfers issued by the UK Information Commissioner's Office under S119A(1) of the UK Data Protection Act 2018.

Client Engager will abide by the requirements of European Economic Area, United Kingdom, and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

Product Data Deletion
At all times during the term of Customer's Product engagement, Customer will have the ability to access, extract and delete Product Data.

Client Engager will delete all copies of Product Data within 90 days of the end of the Customer Agreement.

Processor Confidentiality Commitment
Client Engager will ensure that its personnel engaged in the processing of Product Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Client Engager shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Product Data in accordance with laws applicable to Client Engager, Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors
Client Engager may hire Subprocessors to provide services on its behalf. Customer consents to this engagement and to Client Engager Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Client Engager of the processing of Product Data if such consent is required under the Standard Contractual Clauses, IDTA or the GDPR Terms.

Client Engager is responsible for its Subprocessors' compliance with Client Engager's obligations in this DPA. Client Engager makes available information about Subprocessors on a Client Engager website. When engaging any Subprocessor, Client Engager will ensure via a written contract that the Subprocessor may access and use Product Data only to deliver the services Client Engager has retained them to provide and is prohibited from using Product Data for any other purpose. Client Engager will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Client Engager by the DPA, including the limitations on disclosure of Processed Data. Client Engager agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

How to Contact Client Engager
If Customer believes that Client Engager is not adhering to its privacy or security commitments, Customer may use Client Engager's mailing address at: **contact@engager.app**

Appendix A – Security Measures

Client Engager has implemented and will maintain for Product Data the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms) are Client Engager's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership.** Client Engager has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities.** Client Engager personnel with access to Product Data are subject to confidentiality obligations. **Risk Management Program.** Client Engager performed a risk assessment before processing Product Data. Client Engager retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory.** Client Engager maintains an inventory of all media on which Product Data is stored. Access to the inventories of such media is restricted to Client Engager personnel authorized in writing to have such access. **Asset Handling.** - Client Engager classifies Product Data to help identify it and to allow for access to it to be appropriately restricted. - Client Engager imposes restrictions on printing Product Data and has procedures for disposing of printed materials that contain Product Data. - Client Engager personnel must obtain Client Engager authorization prior to storing Product Data on portable devices, remotely accessing Product Data, or processing Product Data outside Client Engager's facilities.
Human Resources Security	**Security Training**. Client Engager informs its personnel about relevant security procedures and their respective roles. Client Engager also informs its personnel of possible consequences of breaching the security rules and procedures. Client Engager will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities.** Client Engager limits access to facilities where information systems that process Product Data are located to identified authorized individuals. **Physical Access to Components.** Client Engager maintains records of the incoming and outgoing media containing Product Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Product Data they contain. **Protection from Disruptions.** Client Engager uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal.** Client Engager uses industry standard processes to delete Product Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Client Engager maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Product Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no Product Data has been updated during that period), Client Engager maintains multiple copies of Product Data from which Product Data can be recovered. - Client Engager stores copies of Product Data and data recovery procedures in a different place from where the primary computer equipment processing the Product Data is located. - Client Engager has specific procedures in place governing access to copies of Product Data. - Client Engager reviews data recovery procedures at least annually. - Client Engager logs data restoration efforts, including the person responsible, the description of the restored data and, where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Client Engager has anti-malware controls to help avoid malicious software gaining unauthorized access to Product Data, including malicious software originating from public networks. **Data Beyond Boundaries** - Client Engager encrypts, or enables Customer to encrypt, Product Data that is transmitted over public networks. - Client Engager restricts access to Product Data in media leaving its facilities.

Domain	Practices
	Event Logging - Client Engager logs, or enables Customer to log, access and use of information systems containing Product Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Client Engager maintains a record of security privileges of individuals having access to Product Data. **Access Authorization** - Client Engager maintains and updates a record of personnel authorized to access Client Engager systems that contain Product Data. - Client Engager deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Client Engager identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Client Engager ensures that where more than one individual has access to systems containing Product Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Product Data when needed. - Client Engager restricts access to Product Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Client Engager instructs Client Engager personnel to disable administrative sessions when leaving premises Client Engager controls or when computers are otherwise left unattended. - Client Engager stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Client Engager uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Client Engager requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Client Engager requires the password to be at least eight characters long. - Client Engager ensures that de-activated or expired identifiers are not granted to other individuals. - Client Engager monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Client Engager maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Client Engager uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Client Engager has controls to avoid individuals assuming access rights they have not been assigned to gain access to Product Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - Client Engager maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - Client Engager tracks, or enables Customer to track, disclosures of Product Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Client Engager security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Client Engager maintains emergency and contingency plans for the facilities in which Client Engager information systems that process Product Data are located. - Client Engager's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Product Data in its original or last-replicated state from before the time it was lost or destroyed.

Appendix B – Data Subjects and Categories of Personal Data

Data subjects: Data subjects include the Customer's representatives and end-users including employees, contractors, collaborators, and customers of the Customer. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by Client Engager. Client Engager acknowledges that, depending on Customer's use of the Product, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors and temporary workers (current, former, prospective) of Customer;
- Dependents of the above;
- Customer's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users e.g., individuals, sole traders, partners, directors and other data subjects that are users of Customer's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the Customer and/or use communication tools such as apps and websites provided by the Customer;
- Stakeholders or individuals who passively interact with Customer (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the Customer);
- Professionals with professional privilege (e.g., lawyers, accountants, etc.).

Categories of data: The personal data that is included in e-mail, documents and other data in an electronic form in the context of the Product. Client Engager acknowledges that, depending on Customer's use, Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, client number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Location data (for example, Mobile phone ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video and audio;
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified in Article 4 of the GDPR.

Appendix C – Additional Safeguards Addendum

By this Additional Safeguards Addendum to the DPA (this "Addendum"), Client Engager provides additional safeguards to Customer for the processing of personal data, within the scope of the GDPR, by Client Engager on behalf of Customer and additional redress to the data subjects to whom that personal data relates.

This Addendum supplements and is made part of, but is not in variation or modification of, the DPA.

1. Challenges to Orders. In the event Client Engager receives an order from any third party for compelled disclosure of any personal data processed under this DPA, Client Engager shall:

- **a.** use reasonable effort to redirect the third party to request data directly from Customer;
- **b.** promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and
- **c.** use lawful efforts to challenge the order (at the cost of the Customer) for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with applicable law.

If, after the steps described in a. through c. above, Client Engager remains compelled to disclose personal data, Client Engager will disclose only the minimum amount of that data it deems necessary to satisfy the order for compelled disclosure.

For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2. Indemnification of Data Subjects. Subject to Sections 3 and 4, Client Engager shall be liable to a data subject for any material or non-material damage to the data subject caused by Client Engager's disclosure of personal data of the data subject that has been transferred in response to an order from a non-EU/EEA government body or law enforcement agency in violation of Client Engager's obligations under Chapter V of the GDPR (a "Relevant Disclosure"). Notwithstanding the foregoing, Client Engager shall have no obligation to pay the data subject under this Section 2 to the extent the data subject has already received compensation for the same damage, whether from Client Engager or otherwise.

3. Conditions of Indemnification. Section 2 is conditional upon the data subject establishing, to Client Engager's reasonable satisfaction, that:

- **a.** Client Engager engaged in a Relevant Disclosure;
- **b.** the Relevant Disclosure was the basis of an official proceeding by the non-EU/EEA government body or law enforcement agency against the data subject; and
- **c.** the Relevant Disclosure directly caused the data subject to suffer material or non-material damage.

The data subject bears the burden of proof with respect to conditions a. to c. (inclusive).

Notwithstanding the foregoing, Client Engager shall have no obligation to indemnify the data subject under Section 2 if Client Engager establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

4. Scope of Damages. Section 2 is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Client Engager's infringement of the GDPR.

5. Exercise of Rights. Rights granted to data subjects under this Addendum may be enforced by the data subject against Client Engager irrespective of any restriction in Clauses 3 or 6 of the Standard Contractual Clauses. The data subject may only bring a claim under this Addendum on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Addendum are personal to the data subject and may not be assigned.

6. Notice of Change. Client Engager agrees and warrants that it has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the Customer and its obligations under this Addendum or the Standard Contractual Clauses or IDTA 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 this Addendum or the Standard Contractual Clauses or IDTA, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract.

Attachment 1 –General Data Protection Regulation Terms

Client Engager makes the commitments in these GDPR Terms, to all customers, and may update them at any time. These commitments are binding upon Client Engager with regard to Customer regardless of (1) the version of the DPA that is otherwise applicable to any given engagement or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and Client Engager agree that Customer is the controller of Customer Personal Data and Client Engager is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Client Engager is a subprocessor, or Client Engager acts as Controller. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Client Engager on behalf of Customer.

These GDPR Terms do not limit or reduce any data protection commitments Client Engager makes to Customer in the Client Engager Product Data Protection Addendum or other agreement between Client Engager and Customer.

These GDPR Terms do not apply where Client Engager is a controller of Personal Data.

Relevant GDPR Obligations: Articles 28, 32, and 33

1. Client Engager shall inform Customer of any intended changes concerning the addition or replacement of other processors. (Article 28(2))

2. Processing by Client Engager shall be governed by these GDPR Terms under UK law and are binding on Client Engager with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer's Agreement, including these GDPR Terms. In particular, Client Engager shall:

- **(a)** process the Personal Data as set out in the Client Engager standard terms and this DPA, including with regard to transfers of Personal Data to a third country or an international organisation;
- **(b)** ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- **(c)** take measures required pursuant to Article 32 of the GDPR;
- **(d)** respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;
- **(e)** taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
- **(f)** assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 34 of the GDPR, taking into account the nature of processing and the information available to Client Engager;
- **(g)** at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;
- **(h)** make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Client Engager shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR. (Article 28(3))

3. Where Client Engager engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Client Engager shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))

4. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and Client Engager shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- **(a)** the pseudonymisation and encryption of Personal Data;
- **(b)** the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) 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

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))

5. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Article 32(2))

6. Customer and Client Engager shall take steps to ensure that any natural person acting under the authority of Customer or Client Engager who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by law. (Article 32(4))

7. Client Engager shall notify Customer without undue delay after becoming aware of a Personal Data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Client Engager.