Standard Data Protection Terms

GDPR CLAUSE DEFINITIONS:

Data Protection Legislation: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy;

Data Protection Impact Assessment: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer take the meaning given in the GDPR.

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data**.**

DPA 2018: Data Protection Act 2018

GDPR: the General Data Protection Regulation *(Regulation (EU) 2016/679)*

LED: Law Enforcement Directive *(Directive (EU) 2016/680)*

Protective Measures: appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it.

Sub-processor: any third Party appointed to process Personal Data on behalf of the Supplier related to this Agreement.

Supplier Personnel: all directors, officers, employees, agents and consultants of the Supplier and/or of any Sub-Supplier engaged in the performance of its obligations under this Agreement

1. DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor. The only processing that the Supplier is authorised to do is listed in Schedule A by the Customer and may not be determined by the Supplier.

1.2 The Supplier shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

1.3 The Supplier shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule A, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Customer as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Supplier Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule A);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:

(a) are aware of and comply with the Supplier's duties under this clause;

(b) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

(c) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this Agreement; and

(d) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

(i) the Customer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Customer in meeting its obligations); and

(iv) the Supplier complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(e) at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of the Agreement unless the Supplier is required by Law to retain the Personal Data.

1.5 Subject to clause 1.6, the Supplier shall notify the Customer immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third Party for disclosure of Personal Data where

compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event.

1.6 The Supplier's obligation to notify under clause 1.5 shall include the provision of further information to the Customer in phases, as details become available.

1.7 Taking into account the nature of the processing, the Supplier shall provide the Customer with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Customer) including by promptly providing:

(a) the Customer with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Customer following any Data Loss Event;

(e) assistance as requested by the Customer with respect to any request from the Information Commissioner's Office, or any consultation by the Customer with the Information Commissioner's Office.

1.8 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

(a) the Customer determines that the processing is not occasional;

(b) the Customer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(c) the Customer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Supplier shall allow for audits of its Data Processing activity by the Customer or the Customer's designated auditor.

1.10 The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Supplier must:

(a) notify the Customer in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Customer;

(c) enter into a written agreement with the Sub-processor where the contract is on terms no less onerous than the terms set out within this contract; and

(d) provide the Customer with such information regarding the Sub-processor as the Customer may reasonably require.

1.12 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The Customer may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer may on not less than 30 Working Days' notice to the Supplier amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Standard Data Protection Terms

Schedule A - Schedule of Processing, Personal Data and Data Subjects

1. The Supplier shall comply with any further written instructions with respect to processing by the Customer.

2. Any such further instructions shall be incorporated into this Schedule.

Description	**Details**
Subject matter of the processing	*[This should be a high level, short description of what the processing is about i.e. its subject matter]*
Duration of the processing	*[Clearly set out the duration of the processing including dates]*
Nature and purposes of the processing	*Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*
Type of Personal Data	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	*[Describe how long the data will be retained for, how it be returned or destroyed]*