DEFINITIONS

Agreement: this contract.

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

Data Protection Legislation: (i) the DPA; (ii) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; and (iii) all applicable Law about the processing of Personal Data and privacy.

Data Protection Officer: the meaning given in the GDPR.

Data Subject: the meaning given in the GDPR.

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: (i) the Data Protection Act 1998 and (ii) subject to Royal Assent, the Data Protection Act 2018 to the extent that it relates to processing of Personal Data and privacy.

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

Law: any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Service Provider is bound to comply.

LED: the Law Enforcement Directive (Directive (EU) 2016/680).

Party: a Party to this Agreement.

Personal Data / Personal Data Breach: the meaning given in the GDPR.

Processor: the meaning given in the GDPR.

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 any such measures adopted by it.

Service Provider's Personnel: all employees, staff, other workers, agents and consultants of the Service Provider and of any Sub-Contractors who are engaged in the provision of the Services from time to time.

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

CLAUSES

1. Data Protection

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

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

1.3 The Service Provider shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Authority, 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 Service Provider 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 Service Provider is required to do otherwise by Law. If it is so required the Service Provider shall promptly notify the Authority 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 Authority 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 Service Provider's 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 Service Provider's Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Service Provider's duties under this Clause;

(B) are subject to appropriate confidentiality undertakings with the Service Provider 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 Authority 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 Authority has been obtained and the following conditions are fulfilled:

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

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

(iii) the Service Provider 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 Authority in meeting its obligations); and

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

(e) at the written direction of the Authority, and at the Service Provider's sole cost, delete or return Personal Data (and any copies of it) to the Authority on termination of the Agreement unless the Service Provider is required by Law to retain the Personal Data.

1.5 Subject to Clause 1.6, the Service Provider shall notify the Authority 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 Service Provider's obligation to notify under Clause 1.5 shall include the provision of further information to the Authority in phases, as details become available.

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

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

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

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

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

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

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

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

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

1.9 The Service Provider shall allow for audits of its Data Processing activity by the Authority or the Authority's designated auditor.

1.10 The Service Provider 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 Service Provider must:

(a) notify the Authority in writing of the intended Sub-Processor and processing;

(b) obtain the written consent of the Authority;

(c) enter into a written agreement with the Sub-Processor which give effect to the terms set out in this Clause 1 such that they apply to the Sub-Processor; and

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

1.12 The Service Provider shall remain fully liable for all acts or omissions of any Sub-Processor.

1.13 The Service Provider 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 Authority may on not less than 30 Working Days' notice to the Service Provider amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

SCHEDULE A: PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. The Service Provider shall comply with any further written instructions with respect to processing by the Authority.

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

Description	Details
Subject matter of the processing[1]	
Duration of the processing[2]	
Nature and purposes of the processing[3]	
Type of Personal Data[4]	
Categories of Data Subject[5]	
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[6]	

[1] This should be a high level, short description of what the processing is about i.e. its subject matter.
[2] Clearly set out the duration of the processing including dates.
[3] 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.
[4] Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.
[5] 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.
[6] Describe how long the data will be retained for, how it will be returned or destroyed.