



Department of Health and Wellbeing

Public Health
5th Floor, Britannia House
Broadway
Bradford BD1 1HX

Tel: (01274) 43[Ext]
Email: [Insert Name] @bradford.gov.uk

Date: [INSERT DATE]

Contract Variation – [INSERT CONTRACT TITLE]

I write with reference to the Contract between our organisations for the provision of the above and further to our previous letter regarding the statutory requirement to vary the Contract to bring it into line with the new Data Protection Legislation.

Organisations which are required to comply with the new Data Protection Legislation may incur costs in doing so, especially where new systems or processes are required. However, these costs are attributable to conducting business in the EU, and not supplying to the UK public sector. We expect all Providers to manage their own costs in relation to compliance.

I enclose again the varied Data Protection terms and conditions and schedule relating to the Contract. The variation reflects the roles and responsibilities between the Controller and the Processor as required by the new Regulations and as you know the variation is effective from the 25th May 2018.

The enclosed terms and conditions and schedule sets out the Council's specific requirements as to how you should process relevant Personal Data on the Council's behalf and which hereby replaces the existing clause or provisions in the Contract which relate to Data Protection matters.

Although the enclosed documentation replaces the existing term relating to Data Protection in accordance with provisions relating to amendments and replacements of legislation set out in the Definitions and Interpretation section of the Contract, I should be obliged if you would also, by way of acceptance, receipt and variation, duly complete, sign, date and return this document by email or post to the address shown above. Please also complete and return the enclosed GDPR / Data Protection due diligence form.

Yours faithfully,

[INSERT NAME & TITLE] [INSERT NAME OF AUTHORISED OFFICER OR STRATEGIC DIRECTOR]

DATA PROTECTION TERMS AND CONDITIONS

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 to the extent that it relates to processing of personal data and privacy; and (iii) 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 have the meanings given in the GDPR;

Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the 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 Subject 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 including security measures.

Schedule: means a schedule of instructions relating to data processing prepared by the Council and entitled: 'Schedule of Processing, Personal Data and Data Subjects'; and

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

1. DATA PROTECTION

- 1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Council is the Controller and the Provider is the Processor. The only processing that the Provider is authorised to do is pursuant to the instructions in the Schedule served by the Council upon the Provider from time to time and may not be determined by the Provider.
- 1.2 The Provider shall notify the Council immediately if it considers that any of the Council's instructions infringe the Data Protection Legislation.
- 1.3 The Provider shall provide all reasonable assistance to the Council in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Council, 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 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 the Schedule, unless the Provider is required to do otherwise by Law. If it is so required, the Provider shall promptly notify the Council before processing the Personal Data, unless prohibited by Law;
 - b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event and which the Council, as Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), 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 Provider Personnel do not process Personal Data except in accordance with this Agreement (and in particular, the Schedule);
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Provider Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Provider's duties under this clause;
 - (B) are subject to appropriate confidentiality undertakings with the 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 Council or as otherwise permitted by this Agreement; and

- (D) have undergone adequate training in the use, care, protection and handling of Personal Data.
 - d) not transfer Personal Data outside of the EU unless the prior written consent of the Council has been obtained and the following conditions are fulfilled:
 - (i) the Council or the 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 Council;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the 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 Council in meeting its obligations); and
 - (iv) the Provider complies with any reasonable instructions notified to it in advance by the Council with respect to the processing of the Personal Data;
 - e) at the written direction of the Council, delete or return by secure means Personal Data (and any copies of it) to the Council on termination of the Agreement unless the Provider is required by Law to retain the Personal Data.
- 1.5 Subject to clause 1.6, the Provider shall notify the Council immediately if it:
- a) receives a Data Subject Request (or purported Data Subject 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 Provider's obligation to notify under clause 1.5 shall include the provision of further information to the Council in phases, as details become available.
- 1.7 Taking into account the nature of the processing, the Provider shall provide the Council 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 Council) including by promptly providing:
- a) the Council with full details and copies of the complaint, communication or request;
 - b) such assistance as is reasonably requested by the Council to enable the Council to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
 - c) the Council, at its request, with any Personal Data it holds in relation to a Data Subject;
 - d) assistance, as requested by the Council, following any Data Loss Event;
 - e) assistance, as requested by the Council, with respect to any request from the Information Commissioner's Office, or any consultation by the Council with the Information Commissioner's Office.

- 1.8 The Provider shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Provider employs fewer than 250 staff, unless:
- a) the Council determines that the processing is not occasional;
 - b) the Council 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; or
 - c) the Council determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 1.9 The Provider shall allow for audits of its Data Processing activity by the Council or the Council's designated auditor.
- 1.10 Each Party 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 Provider must:
- a) notify the Council in writing of the intended Sub-processor and processing;
 - b) obtain the written consent of the Council;
 - c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause, such that they apply to the Sub-processor; and
 - d) provide the Council with such information regarding the Sub-processor as the Council may reasonably require.
- 1.12 The Provider shall remain fully liable for all acts or omissions of any Sub-processor.
- 1.13 The Council may, at any time on not less than 30 Working Days' notice, revise this clause 1 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 Council may, on not less than 30 Working Days' notice to the Provider, amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule of Processing, Personal Data and Data Subjects

1. The Processor shall comply with any further written instructions from the Controller with respect to processing.
2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	<i>[This should be a high level, short description of what the processing is about i.e. its subject matter]</i>
Duration of the processing	<i>[Clearly set out the duration of the processing including dates]</i>
Nature and purposes of the processing	<p><i>[Please be as specific as possible, but make sure that you cover all intended purposes.</i></p> <p><i>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.</i></p> <p><i>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</i></p>
Type of Personal Data being processed	<i>[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]</i>
Categories of Data Subject	<i>[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]</i>
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	<i>[Describe how long the data will be retained for, how it be returned or destroyed]</i>

I hereby accept the terms and conditions and Data Protection Schedule:

Signed

Print Name

.....

.....

Organisation

Position

.....

.....

Date

.....

