**DCC HEADED LETTER**

[Contractor Name]

[Address]

[Date]

Dear Sirs,

**TO ALL CONTRACTORS WITH RELEVANT DATA PROTECTION OBLIGATIONS**

**URGENT ACTION NEEDED**

New data protection legislation is due to come into force on **25th May 2018**, which will apply to any public or private organisation processing personal data.

Accordingly, there are also a number of changes that will affect commercial arrangements, both new and existing, with suppliers. The new General Data Protection Regulations (the “**Regulations**”) specify that any processing of personal data, by a Processor, should be governed by a contract with certain provisions included.

We have identified the following existing contracts involving the processing of personal data (and which will be in place after 25 May 2018) that require updating in order to bring them into line with the Regulations. This will involve updating contract terms based on the generic standard clauses published in Procurement Policy Note 03/17. The amendments will also ensure that specifications and service delivery schedules in the affected contracts reflect the roles and responsibilities between the Controller and the Processor as required by the Regulations.

[insert or attach list of relevant contracts]

Any organisation required to comply with the Regulations 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 the UK public sector. We expect all suppliers to manage their own costs in relation to compliance.

As the Data Controller, we will not accept liability clauses where you are indemnified against fines under GDPR as the Processor. The legal penalty regime has been extended directly to Processors to ensure better performance and enhanced protection for personal data. That means indemnifying Processors for any GDPR fines or court claims undermines these principles.

Our Commercial Teams will contact you in the coming weeks to start work on varying existing contracts. You may also have received similar communications from commercial teams across the public sector.

In the meantime, we attach, in Schedule 1 below, the draft of the proposed variation letter and the new contract terms (together, the “**Variation Letter**”) that will replace the old data protection provisions in your existing contract(s) with us.

We have attached the Variation Letter so that you know, as early as possible, what changes we are intending to make to the above contract(s).

**It will be helpful, in particular, if you can review the table in Annex 1 (on the last page) of the Variation Letter**. We will be contacting you to discuss this table and we will need your help with the completion of the data processing detail within it. This table needs completing between us before we can legally change the contract with you. Your assistance will be appreciated, as this will speed up the process of these required changes and reduce the time needed to complete the legal documents.

Yours faithfully,

[Name]

[Title]

For and on behalf of Derbyshire County Council

**Schedule 1**

DCC HEADED LETTER

[Contractor address]

[date]

Dear Sirs,

**VARIATION AGREEMENT – General Data Protection Regulations (GDPR)**

**URGENT ACTION NEEDED**

As you are aware, we recently wrote to you about changes that Derbyshire County Council need to make concerning the new data protection legislation (General Data Protection Regulations (GDPR)), which is due to come into force on 25th May 2018.

For the purpose of this Letter, the following definitions shall apply:

**Agreement** - means any contractual agreements in force between the Council and the Contractor.

**Commencement Date** - means with effect from 25th May 2018 (or such earlier date agreed between us).

**Contractor** - means the contractor set out at the head of this Variation Letter.

**Council** - means Derbyshire County Council.

**GDPR Terms** - means the new contractual clauses that shall apply to the Agreement and are set out in Annex 1 (attached).

**Letter** - means this variation agreement letter.

**Parties** - means the Council and the Contractor.

**Services** - means the services that are provided by the Contractor under the Agreement.

Accordingly, with effect from the Commencement Date, the GDPR Terms as set out in this Letter will apply to the Agreement between the Parties and replace any existing data protection obligations, and the Agreement shall be deemed to be varied accordingly. All definitions used in this Letter shall, have the same meanings as those terms used in the Agreement, unless otherwise provided by this Letter. The Agreement shall remain in full force and effect so far as still relevant to be carried out and, in the event of any conflict between the Agreement and this Letter, this Letter shall prevail.

This Letter shall remain in force for the duration of the Agreement, whereupon, on termination or expiry of the Agreement, this Letter shall terminate automatically.

No provision of the Agreement shall be construed as to exclude the terms of this Letter.

This Letter may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one Letter.

This Letter and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes and claims) shall be governed by and construed in accordance with the Agreement and the Parties agree to submit to the exclusive jurisdiction of the courts set out in the Agreement.

Please sign the duplicate of this letter and return it by post marked for my attention at the address below within 21 days of the date of this letter.

Yours faithfully,

**[NAME]**

**[TITLE]**

**For and on behalf of J McElvaney, Director of Legal Services**

**Derbyshire County Council**

**Agreed and accepted for and on behalf of the Contractor**

|  |
| --- |
| **……………………………………......** |
| **Signed** |
|  |
| **……………………………………......** |
| **Name** |
|  |
| **…………………………………….....** |
| **Title** |
|  |
| **……………………………………....** |
| **Date** |

**ANNEX 1 - GDPR TERMS**

**DEFINITIONS USED IN THE GDPR TERMS:**

**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; and (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 Contractor 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;

**Schedule**: means the schedule attached to this Annex 1 forming part of this Letter and titled: ‘Schedule of Processing, Personal Data and Data Subjects’; and

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

1. **DATA PROTECTION**
   1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Council is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is listed in the Schedule by the Council and may not be determined by the Contractor.
   2. The Contractor shall notify the Council immediately if it considers that any of the Council's instructions infringe the Data Protection Legislation.
   3. The Contractor 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:
2. a systematic description of the envisaged processing operations and the purpose of the processing;
3. an assessment of the necessity and proportionality of the processing operations in relation to the Services;
4. an assessment of the risks to the rights and freedoms of Data Subjects; and
5. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
   1. The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:
6. process that Personal Data only in accordance with the Schedule, unless the Contractor is required to do otherwise by Law. If it is so required, the Contractor shall promptly notify the Council before processing the Personal Data, unless prohibited by Law;
7. ensure that it has in place Protective Measures, which have been reviewed and approved by the Council as appropriate to protect against a Data Loss Event having taken account of the:
8. nature of the data to be protected;
9. harm that might result from a Data Loss Event;
10. state of technological development; and
11. cost of implementing any measures;
12. ensure that:
13. the Contractor Personnel do not process Personal Data except in accordance with this Agreement (and in particular, the Schedule);
14. it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:
15. are aware of and comply with the Contractor’s duties under this clause;
16. are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;
17. 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
18. have undergone adequate training in the use, care, protection and handling of Personal Data.
19. 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:
20. the Council or the Contractor 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;
21. the Data Subject has enforceable rights and effective legal remedies;
22. the Contractor 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
23. the Contractor complies with any reasonable instructions notified to it in advance by the Council with respect to the processing of the Personal Data;
24. at the written direction of the Council, delete or return Personal Data (and any copies of it) to the Council on termination of the Agreement unless the Contractor is required by Law to retain the Personal Data.
    1. Subject to clause 1.6, the Contractor shall notify the Council immediately if it:
25. receives a Data Subject Access Request (or purported Data Subject Access Request);
26. receives a request to rectify, block or erase any Personal Data;
27. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
28. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
29. 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
30. becomes aware of a Data Loss Event.
    1. The Contractor’s obligation to notify under clause 1.5 shall include the provision of further information to the Council in phases, as details become available.
    2. Taking into account the nature of the processing, the Contractor 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:
31. the Council with full details and copies of the complaint, communication or request;
32. such assistance as is reasonably requested by the Council to enable the Council to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
33. the Council, at its request, with any Personal Data it holds in relation to a Data Subject;
34. assistance, as requested by the Council, following any Data Loss Event;
35. 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. The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:
36. the Council determines that the processing is not occasional;
37. 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; and
38. the Council determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
    1. The Contractor shall allow for audits of its Data Processing activity by the Council or the Council’s designated auditor.
    2. The Contractor shall designate a data protection officer if required by the Data Protection Legislation.
    3. Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Contractor must:
39. notify the Council in writing of the intended Sub-processor and processing;
40. obtain the written consent of the Council;
41. 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
42. provide the Council with such information regarding the Sub-processor as the Council may reasonably require.
    1. The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.
    2. 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).
    3. 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 Contractor, amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner’s Office.
    4. The Parties agree that any term or condition of the Agreement that attempts to limit the liability of the Contractor with respect to any claims it may receive from the Council following any fine, costs damages, costs or any other claim (the “Losses”) imposed on the Council from the Information Commissioner’s Office (or such successor organisation or regulator thereof) shall have no effect, and, accordingly, notwithstanding any other terms or conditions of the Agreement, the Contractor shall indemnify the Council in full for any Losses imposed on the Council from the Information Commissioner’s Office.

**Annex 1 - Schedule of Processing, Personal Data and Data Subjects**

1. The Contractor shall comply with any further written instructions with respect to processing by the Council.
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, by way of examples only: 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]* |