**GDPR TOOLKIT TEMPLATE - CONTRACT CHANGE NOTICE TO INCORPORATE GDPR PROVISIONS**

[**Insert Buyer letterhead]**

**[Supplier Contract Manager Name**

**Supplier Name**

**Street name**

**Town**

**County/Country**

**Postcode]**

**[00 Month]** 2018

Dear **[Name of Supplier Contract Manager]**

**Re: Contract change notice to reflect new data protection laws: [name of contract] [reference number] [date]**

New data protection legislation is due to come into force during May 2018, which aims to protect the privacy of all EU citizens and prevent data breaches. It will apply to any public or private organisation processing personal data and brings new obligations on data controllers and data processors.

Established key principles of data privacy will remain relevant in the new Data Protection Legislation but there are also a number of changes that will affect commercial arrangements, both new and existing. The new General Data Protection Regulation (GDPR) which comes into force on 25 May 2018, specifies that **any processing of personal data by a Processor, should be governed by a contract with certain provisions included** as set out in the Regulation itself.

We have identified the above contract as requiring these provisions; it involves processing personal data and will be in place after 25 May 2018. To bring the contract into line with the new regulation, **this letter is a formal change notice to vary the contract [name of contract] [reference number] [date] (“the Contract”) to implement the GDPR clauses featured in** [**Procurement Policy Note 03/17**](http://www.gov.uk/government/publications/procurement-policy-note-0317)

**[Annex 1]** to this letter details the changes that will be made to current data protection clauses in the above listed contract, including a schedule that sets out roles and responsibilities - which is also a requirement within the regulation.

**Cost of Compliance**

Any organisation 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 the UK public sector. We expect you to manage your own costs in relation to compliance.

The legislative change Clause [insert clause number]under the Contract says that a Supplier is not entitled to relief of obligations or increase in prices as a result of a General Change of Law such as the introduction of the GDPR.

In order to ensure that all our commercial arrangements comply with the new statutory position, we may be required to suspend or terminate contracts with suppliers who fail to agree this variation before 25 May 2018.

**Action Required**

The Contract shall be varied in accordance with the terms set out in [Annex 1] to this letter.

This Variation must be agreed and signed by both Parties and shall only be effective from 25th May 2018 once signed by the Parties.

Words and expressions in this Variation shall have the meanings given to them in the Contract. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Authority

|  |  |
| --- | --- |
| Signature |  |
| Date |  |

Author’s name

Position/Title

Team Name

D +44 (0)xxx xxx xxxx

E contract.manager@governmentdepartment.gov.uk

Please ensure that his letter is signed by an authorised signatory on behalf of the Supplier and returned to the Buyer to accept the terms of this Variation:

|  |  |
| --- | --- |
| Signature |  |
| Date |  |
| Name |  |

[Guidance Note: Schedule Y shall be added in the form set out in this letter. This template is to be completed prior to the effective date of this Variation].

**Schedule Y Processing, Personal Data and Data Subjects**

* + 1. The contract details of the [Authority/Buyer] Data Protection Officer is:

**[Insert** Contact details]

* + 1. The contract details of the Supplier Data Protection Officer is:

**[Insert** Contact details]

* + 1. The Processor shall comply with any further written instructions with respect to processing by the Controller.
    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]* |

**ANNEX 1 - EXAMPLE TERMS AND CONDITIONS [TO BE ADAPTED BY BUYER ]**

[Guidance Note: Please consider the identity of the Controller and the Processor before issuing the variation. High risk contracts may require a bespoke version of this drafting.]

**Annex 1 – Varied Terms**

The Contract is varied as follows:

**Schedule 1 - Definitions**

The following definitions shall be deleted:

***“Processing”***

The following definitions shall be revised as follows:

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

***“Data Protection Legislation”*** *means:*

* + 1. *the GDPR, the LED and any applicable national implementing Laws as amended from time to time;*
    2. *the DPA to the extent that it relates to processing of personal data and privacy;*
    3. *all applicable Law about the processing of personal data and privacy;*

***“Data Subject Access Request”*** *means 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;*

***“Data Subject”*** *has the meaning given in the GDPR;*

***“DPA”*** *means the Data Protection Act 2018 as amended from time to time;*

***“Personal data”*** *has the meaning given in the GDPR;*

***“Staffing Information”*** *the reference to “DPA” shall be replaced with “Data Protection Legislation”*

The following new definitions shall be introduced:

***“Controller”*** *has the meaning give in the GDPR;*

***“Data Protection Officer”*** *has the meaning given in the GDPR;*

***“GDPR”*** *means the General Data Protection Regulation (Regulation (EU) 2016/679)*

***“LED”*** *means the 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;*

***“Processor”*** *has the meaning given in the GDPR;*

***“Processor Personnel”*** *all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any sub-contractor of the Processor;*

***“Personal Data Breach”*** *has the meaning given in the GDPR;*

***“Sub-processor”*** *any third party appointed to process Personal Data on behalf of the Processor related to this agreement;*

The Contract is varied as follows:

Clause [Z] Protection of Personal Data shall be replaced with the following provisions:

*Z.1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor unless otherwise specified in Schedule Y (Processing Personal Data). The only processing that the Processor is authorised to do is listed in Schedule Y (Processing Personal Data) by the Controller and may not otherwise be determined by the Processor.*

*Z.2 The Processor shall notify the Controller immediately if it considers that any of the Buyer’s instructions infringe the Data Protection Legislation.*

*Z.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:*

* + 1. *a systematic description of the envisaged processing operations and the purpose of the processing;*
    2. *an assessment of the necessity and proportionality of the processing operations in relation to the Services;*
    3. *an assessment of the risks to the rights and freedoms of Data Subjects; and*
    4. *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.*

*Z.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Call Off Contract:*

* + 1. *process that Personal Data only in accordance with Schedule Y (Processing Personal Data), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;*
    2. *ensure that it has in place Protective Measures which have been reviewed and approved by the Controller as appropriate to protect against a Data Loss Event having taken account of the:*
       1. *nature of the data to be protected;*
       2. *harm that might result from a Data Loss Event;*
       3. *state of technological development; and*
       4. *cost of implementing any measures;*
    3. *ensure that :*
       1. *the Processor Personnel do not process Personal Data except in accordance with this Call Off Contract (and in particular Schedule Y (Processing Personal Data));*
       2. *it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:*
          1. *are aware of and comply with the Processor’s duties under this Clause;*
          2. *are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;*
          3. *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 Controller or as otherwise permitted by this Call Off Contract; and*
          4. *have undergone adequate training in the use, care, protection and handling of Personal Data;*
    4. *not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:*
       1. *the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;*
       2. *the Data Subject has enforceable rights and effective legal remedies;*
       3. *the Processor 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 endeavors to assist the Controller in meeting its obligations); and*
       4. *the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;*
    5. *at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Call Off Contract unless the Processor is required by Law to retain the Personal Data.*

*Z.5 Subject to Clause Z.7, the Processor shall notify the Controller immediately if it:*

* + 1. *receives a Data Subject Access Request (or purported Data Subject Access Request);*
    2. *receives a request to rectify, block or erase any Personal Data;*
    3. *receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;*
    4. *receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Call Off Contract;*
    5. *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*
    6. *becomes aware of a Data Loss Event.*

*Z.6 The Processor’s obligation to notify under Clause Z.5 shall include the provision of further information to the Controller in phases, as details become available.*

*Z.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause Z.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:*

* + 1. *the Controller with full details and copies of the complaint, communication or request;*
    2. *such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;*
    3. *the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;*
    4. *assistance as requested by the Controller following any Data Loss Event;*
    5. *assistance as requested by the Controller with respect to any request from the Information Commissioner’s Office, or any consultation by the Controller with the Information Commissioner's Office.*

*Z.8. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:*

* + 1. *the Controller determines that the processing is not occasional;*
    2. *the Controller 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*
    3. *the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.*

*Z.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.*

*Z.10 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.*

*Z.11 Before allowing any Sub-processor to process any Personal Data related to this Call Off Contract, the Processor must:*

* + 1. *notify the Controller in writing of the intended Sub-processor and processing;*
    2. *obtain the written consent of the Controller;*
    3. *enter into a written agreement with the Sub-processor which give effect to the terms set out in this Clause 23.11 such that they apply to the Sub-processor; and*
    4. *provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.*

*Z.12. The Processor shall remain fully liable for all acts or omissions of any Sub-processor.*

*Z.13 The Buyer 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 Call Off Contract).*

*Z.14 The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Buyer may on not less than 30 Working Days’ notice to the Supplier to amend this Call Off Contract to ensure that it complies with any guidance issued by the Information Commissioner’s Office.*

*Clauses applicable to Joint Controllers only*

***[Guidance:*** *these clauses may be deleted where no Joint Control is envisaged]*

Z.15 In respect of Personal Data identified in Schedule Y (Authorised Processing Template) as under Joint Control Clause Z.1-Z.14 shall not apply and shall be replaced by a Data Sharing Agreement which must be entered into by both Parties.

In Call-Off Schedule 10 - Part D (Employment Exit Provisions) Paragraph 1 the reference to *“DPA”* shall be replaced with *“Data Protection Legislation”*