



## **REVISED DATA PROTECTION CONTRACT CLAUSES**

General Terms and Conditions of Contract for the Supply of Services – Clauses 17.25 and 17.26 ‘DATA PROTECTION’ are superseded and replaced with the following: -

### **DEFINITIONS:**

<b>Authority</b>	Conwy County Borough Council.
<b>Business Working Day</b>	Means any day other than a Saturday and Sunday or public holiday in England and Wales.
<b>Confidential Information</b>	Any information which has been designated in writing by either Party as being confidential or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information which relates to all Personal Information and sensitive Personal Information within the meaning of the Data Protection Act 1998 and Section 124 of the Police Act 1997 in relation to the business, affairs, properties, assets, trading practices, Service Developments, trade secrets, personnel, Person and suppliers of either Party, and the Commercially Sensitive Information.
<b>Contractor</b>	Means the Organisation appointed under the Contract to provide the Service.
<b>Contractor’s Personnel</b>	Means any Staff members, directors, officers, employees, volunteers, agents, consultants, self-employed individuals or Sub-contractors engaged and considered to be essential to the work being performed under this Contract.
<b>Personal Information</b>	Shall have the same meaning as set out in the GDPR and DPA 2018 and relates only to Personal Data, or any part of such Personal Data, of which the Authority is the Data Controller and in relation to which the Contractor is providing the Service under this Contract.
<b>Data Controller</b>	Shall have the same meaning as set out in the Data Protection Legislation.
<b>Data Processor</b>	Shall have the same meaning as set out in the Data Protection Legislation.
<b>Data Protection Legislation</b>	Shall have the meaning of the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) in force in the UK from 25 May 2018 and all applicable laws and guidance relating to the processing of Personal Information and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.
<b>Data Subject</b>	Means any living person who is the subject of Personal Information as defined in the DPA.
<b>GDPR and DPA</b>	Means General Data Protection Regulation and Data Protection Act 2018 the extent that they relate to processing of Personal Information and privacy.
<b>Sub-contract</b>	Means a contract between the Contractor and the Sub-contractor to perform all of part of the Contract.
<b>Sub-contractor</b>	Means an organisation or agent appointed by the Contractor or with whom the Contractor contracts to provide any part of the Service and any of that organisation’s contractors who may be providing the Service.
<b>Sub-processor</b>	Means an organisation, agent or servant who is called upon by the Contractor to be engaged with the delivery of the Service.

## **DATA PROTECTION**

The Parties shall comply with their obligations under the Data Protection Legislation at all times and in particular as set out below.

### **Information Governance – General Responsibilities**

The Parties acknowledge their respective obligations arising under the Data Protection Legislation and will assist each other as necessary to enable each other to comply with these obligations.

The Contractor shall (and shall ensure that any Sub-contractor or third party shall) comply at all times with the Data Protection Legislation and their obligations as a Data Processor or Data Controller as the case may be and shall not perform its obligations under this Contract in any such way as to cause the Authority to breach their obligations under the Data Protection Legislation.

The Authority shall be the Data Controller and the Contractor shall be the Data Processor of the Personal Information unless it is agreed or is apparent from the nature of the processing that the Contractor shall be a Data Controller in which case the Parties shall comply with the provisions of the Data Protection Legislation in relation to Data Controllers or Joint Data Controllers as the case may be.

The Contractor shall comply with its obligations under the Data Protection Legislation and all statutory re-enactments or modifications thereof, any regulations, rules, orders and any codes of practice or any guidelines issued by the Information Commissioner.

The Contractor shall have a Data Protection Policy and Procedures in place that will take account of but not limited to usage fax, email, manual document disposal; physical security; homeworking; retention of information; system access; dealing with disclosures over the telephone; archiving; data back up and retrieval; incident reporting and training.

The Contractor undertakes to:

Treat as confidential all Personal Information which may be derived from or obtained in the course of the Contract or which may come into the possession of the Contractor or the Contractor's Personnel as a result of or in connection with the Service;

Provide all necessary precautions to ensure that all such information is treated as confidential by the Contractor and the Contractor's Personnel;

Ensure that the Contractor's Personnel are aware of the provisions of the Data Protection Legislation and that any personal information obtained in the course of the performance of this Contract shall not be disclosed or used in any unlawful manner;

Indemnify the Authority against any loss arising under the Data Protection Legislation caused by any action, authorised or unauthorised, taken by the Contractor or the Contractor's Personnel;

Have in place adequate mechanism to ensure that any Sub-contractors to whom the personal information is disclosed comply with their obligations under this Contract to keep Personal Information and information secure and confidential in accordance with the Data Protection Legislation;

Designate a Data Protection Officer (if required) by the Data Protection Legislation;

### **The Contractor as a Data Processor**

Notwithstanding the general obligations, where the Contractor is processing Personal Information as a Data Processor, the Contractor shall:

Comply with applicable laws of Data Protection Legislation;

Act on a written instruction of the Authority and process Personal Information in accordance with Schedule A to this Contract unless otherwise required by law;

Obtain a commitment of confidentiality from anyone it allows to process the Personal Information, unless they are already under such a duty by law;

Make appropriate measures to ensure the security of processing;

Assist the Authority in providing access and allowing Data Subjects to exercise their rights under Data Protection Legislation;

Assist the Authority in meeting its Data Protection Legislation obligations in relation to the security of processing, the notification of Personal Information breaches and Data Protection impact assessments;

Implement appropriate technical and organisational measures to protect the Personal Information against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure;

Be able to demonstrate that the Contractor's Personnel associated with the performance of the Contract are aware of their personal responsibilities under the Data Protection Legislation to maintain the security of the Personal Information;

Take reasonable steps to ensure the reliability of the Contractor's Personnel who may have access to the Personal Information and use all reasonable endeavours to ensure that such individuals have sufficient skills and training in the use, care and handling of Personal Information;

Ensure that the Contractor's Personnel who may be required in the course of their duties to have access to Personal Information have undergone instruction relating to the care and handling of Personal Information and are honest, reliable and competent in handling of Personal Information;

Not disclose the Personal Information to any third parties in any circumstances other than with the written consent of the Authority or in compliance with a legal obligation imposed upon the Authority; and co-operate with the Authority and enable the Authority to comply with any request under the Data Protection Legislation;

Ensure that Personal Information shall be returned to the Authority within seven (7) days' of request or; under the Authority written instruction, be safely and securely transferred to another Contractor in accordance with the Data Protection Legislation at the end of this Contract;

The Contractor shall identify the Personal Information required for processing as part of the performance of this Contract and unless otherwise required by law, the Contractor shall process the Personal Information in accordance with Schedule A to this Contract (Processing Personal Information and Data Subjects) including the following:

The subject matter;

The duration of the processing;

The nature and purpose of the processing;

The type of Personal Information;

The categories of Personal Information;

The retention of Personal Information;

The security of Personal Information;

The storage of Personal Information;

The training of Staff;

The Contractor shall permit the Authority to inspect and audit the Contractor's processing activities in accordance with the Data Protection Legislation monitoring checklist as introduced and amended from time to time during the term of the Contract and shall comply with all reasonable requests or direction by the Authority to vary and / or procure that the Contractor is in full compliance with its obligations under this Contract. The Contractor shall:

Not process, cause or permit the Personal Information to be transferred outside of the European Economic Area without prior written consent of the Authority;

Ensure that all Contractor's Personnel required to access the Personal Information are informed of the confidential nature of the Personal Information and comply with the obligations set out in this clause (Data Protection);

Be processed for the sole purpose of undertaking the Contractor's obligations under the Contract and for no other purpose;

Ensure that none of the Contractor's Personnel publish, disclose or divulge any of the Personal Information to any third party unless directed in writing by the Authority  
not disclose Personal Information to any third parties in any circumstances other than with the written consent of the Authority or in compliance with a legal obligation imposed upon by the Authority;

Ensure Personal Information is not be copied and / or retained in any form by the Contractor upon expiration or early termination of the Contract except as required by law and if this is the case shall be kept secure at all times;

The Contractor shall notify the Authority within 2 Business Working Days:

If it receives a request from a Data Subject or a third party to have access to a Person's Personal Information; or

If it receives a complaint or request relating to the Authority's obligations under the Data Protection Legislation or;

In the event of any breach or alleged breach of the Data Protection Legislation;

The Contractor shall implement and maintain appropriate technical and organisational measures so as to prevent the destruction damage loss or alteration of any Personal Information or the unauthorised or unlawful processing of any Personal Information. The Contractor shall provide to the Authority such information as may be required to confirm that the Contractor is complying with such obligations, including but not limited to the following;

A copy of the registration to the Information Commissioner under the Act;

Copy/s of all information security policies / procedures covering the use of information technology, mobile devices, home working etc;

Shall permit any authorised representative of the Authority to have access to any site at which Personal Information is processed to monitor the implementation, operation or existence of such policies and procedures;

The Contractor shall ensure that it does nothing which places the Authority in breach of the Data Protection Legislation and shall have or establish appropriate systems, policies and procedures to ensure compliance. The compliance of this clause will be monitored as part of the Authority's monitoring activities.

For avoidance of doubt, in the event of the Contractor's termination of the Contract, the Personal Information relating to this Contract shall be:

Returned to the Authority within seven days' of request or;

Archived or destroyed in accordance with Contractor's Data Protection Policy and Procedures;

as agreed between the Authority and the Contractor.

The Contractor's retention of Personal Information as part of their Data Protection Policy and Procedures should:

Apply to both electronic and manual records;

Justify the retention of records based on the type and any business or legislative need;

Set out how any exceptions to retention schedules are applied and reviewed;

Specify who is responsible for destroying records;

List appropriate disposal methods and security requirements;

Set out the requirements for recording records as destroyed; and

Require periodic review to ensure the retention schedule is correctly applied;

Be in compliance with the Authority's retention procedures.

### **Contractor's engagement of Sub-contractors and Sub-processors**

Prior to allowing any Sub-contractor to process any Personal Information related to the Contract, the Contractor shall:

Notify the Authority in writing of the intended Sub-contractor and processing;  
Obtain the written consent of the Authority;  
Enter into a written agreement with the Sub-contractor which shall give effect to the terms set out in Schedule A and provisions of this clause (Data Protection);  
Provide the Authority such information regarding the Sub-contractor as the Authority may require;

In the event that the Contractor engages as part of the performance of this Contract a Sub-contractor who will process Personal Information in the capacity of a Sub-processor, then the Contractor shall remain directly liable for the acts and omissions to the Authority to ensure compliance with this clause (Data Protection).

### **Notices in respect of Data Protection**

The Parties shall serve a notice pursuant to this Clause (Data Protection) in writing and each notice shall be delivered personally, or sent by pre-paid first class post, or by recorded delivery, or by commercial courier, to the address of the Parties as set out above.

### **Additional Contractor's Responsibilities**

Nothing in this Contract shall relieve the Contractor of its own direct responsibilities and liabilities under the Data Protection Legislation. In addition to the contractual obligations, the Contractor as a Data Processor shall have the following direct responsibilities in accordance with Article 28.2 of the GDPR:

Not to use a Sub-processor without the prior written authorisation of the Data Controller;  
To co-operate with supervisory authorities (such as the ICO);  
To ensure the security of its processing;  
To keep records of processing activities;  
To notify any Personal Information breaches to the Data Controller;  
To employ a Data Protection officer (as applicable);  
To appoint (in writing) a representative within the European Union if needed;

The Contractor acknowledges that if it fails to meet any of these obligations, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.