

## **DATA PROTECTION ADDENDUM TO THE CONDITIONS OF CONTRACT FOR THE SUPPLY OF GOODS AND SERVICES (JUNE 2020)**

This data protection addendum (“**Addendum**”) is incorporated by reference into Wessex Water’s Conditions of Contract for the Supply of Goods & Services (June 2020) and sets out the terms that apply when Personal Data is Processed by the Supplier. The purpose of this Addendum is to ensure that such Processing is conducted in accordance with Data Protection Legislation.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Conditions of Contract for the Supply of Goods & Services (June 2020).

If there is any conflict between the terms of the Purchase Order and the terms of this Addendum in relation to the Processing of Personal Data, the terms of this Addendum shall prevail.

### **1. Definitions**

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

<b>Applying Laws</b>	European Union or United Kingdom laws to which the Supplier is subject;
<b>Claim</b>	any claim, action or demand (whether for damages, an injunction or otherwise) made against the Company arising out of or in connection with a breach of clause 2 (Data Processing Obligations) (whether by the Supplier or by the Supplier’s employees, representatives, agents or sub-contractors). If a number of Claims (whether made by the same claimant or multiple claimants) arise directly or indirectly out of the same cause or event or a series of connected causes or events, those claims shall be treated as a single Claim, which shall be deemed to have arisen on the happening of the first cause or event in question;
<b>Controller</b>	has the meaning set out in the Data Protection Legislation;
<b>Data Protection Legislation</b>	laws and regulations that apply in relation to the Processing of Personal Data including (without limitation) the GDPR, the UK GDPR and the Data Protection Act 2018 and any replacement legislation coming into effect from time to time together with any codes of practice or other guidance issued by a Regulatory Authority;
<b>Data Subject</b>	means a data subject as defined by the Data Protection Legislation;

<b>GDPR</b>	the General Data Protection Regulation (EU) 2016/679;
<b>Permitted Purposes</b>	Processing the Personal Data for the purpose of, and to the extent required for, the provision of the Goods and/or Services;
<b>Permitted Recipient</b>	a director, employee or professional advisor of the Supplier or an agent, temporary worker or permitted sub-contractor used by the Supplier in the provision of the Services who has a legitimate need to receive and Process Personal Data for the Permitted Purposes;
<b>Personal Data</b>	personal data (as such term is defined in the Data Protection Legislation) that is Processed by the Supplier in connection with the provision of the Goods and/or Services;
<b>Processor, Process, Processed or Processing</b>	have the meanings set out in the Data Protection Legislation;
<b>Regulatory Authority</b>	any competent data protection or privacy authority by which the Company is regulated;
<b>Third Country/Countries</b>	all countries outside of the scope of the data protection laws of the European Economic Area (EEA), excluding countries that have been approved by the European Commission from time to time as having adequate data protection laws;
<b>UK GDPR</b>	The GDPR as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

## 2. Data Processing Obligations

- 2.1. For the purpose of Data Protection Legislation, the Company is the Controller and the Supplier is the Processor of the Personal Data.
- 2.2. When Processing Personal Data, the Supplier undertakes to the Company that it shall:
  - 2.2.1. taking into account the nature of the Processing and the information available to the Supplier, provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Regulatory Authorities or other competent data privacy authorities, which the Company is required to undertake under Article 35 or 36 of the GDPR or the UK GDPR or equivalent provisions of any other Data Protection Legislation;
  - 2.2.2. Process the Personal Data only to the extent necessary for the Permitted Purposes;
  - 2.2.3. not Process the Personal Data other than on the Company's documented instructions, including with regard to transfer of Personal Data to a Third Country or an international organisation, unless required to do so by Applying Laws, in which case the Supplier shall to the extent permitted by Applying Laws inform the Company of that legal requirement before the relevant Processing of that Personal Data;

- 2.2.4. keep a record of any Processing of Personal Data it carries out on behalf of the Company;
- 2.2.5. comply with Data Protection Legislation when Processing the Personal Data and not knowingly do or omit to do or permit anything to be done which causes the Company to breach the Data Protection Legislation or any relevant enactments, regulations, orders, standards and other similar instruments relating to the Processing of the Personal Data;
- 2.2.6. taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk;
- 2.2.7. immediately after becoming aware of any breaches of any Applying Laws, enactments, regulations, orders, standards and other similar instruments relating to the Processing of the Personal Data (including the Data Protection Legislation) notify and provide sufficient information to the Company to allow the Company to meet any obligations to report or inform Data Subjects of such breach under the Data Protection Legislation. The Supplier shall co-operate with the Company to assist in the investigation, mitigation and remediation of such breach and shall provide further information where so required by a Regulatory Authority;
- 2.2.8. restrict access to the Personal Data to Permitted Recipients (and in the case of any access by any employee, ensure that access to the Personal Data is limited to such part or parts of the Personal Data as is strictly necessary for performance of that employee's duties), ensure that all such Permitted Recipients are subject to confidentiality undertakings or professional or statutory obligations of confidentiality and impose upon such persons obligations of confidentiality and security at least equivalent to those contained in the Purchase Order and not disclose any Personal Data to any other person without the prior written consent of the Company;
- 2.2.9. ensure that all Permitted Recipients have undertaken training in the laws relating to handling Personal Data and are aware both of the Supplier's duties and their personal duties and obligations under such laws and the Purchase Order. The Supplier shall keep training records to show training is being provided adequately for a minimum of 6 years from the date of the training. The Supplier shall produce such training records, where necessary, following a request from the Company to allow it to defend Claim(s);
- 2.2.10. take reasonable steps to ensure the reliability of all Permitted Recipients who have access to the Personal Data;
- 2.2.11. promptly notify the Company of any unauthorised, unlawful or accidental Processing, disclosure, loss of, damage to, access to or destruction of the Personal Data or if the Personal Data is or becomes corrupted or unusable, and give to the Company all assistance reasonably required by the Company in such respect;
- 2.2.12. promptly amend, transfer, vary and/or delete any Personal Data held by or on behalf of the Supplier upon request from the Company;
- 2.2.13. promptly notify the Company of any request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited;

- 2.2.14. promptly notify the Company of any request of a Regulatory Authority in relation to the Personal Data and co-operate and comply with the directions or decisions of any Regulatory Authority in relation to the Personal Data, and in each case within such timescale as would enable the Company to meet any time limit imposed by any Regulatory Authority (as applicable);
  - 2.2.15. taking into account the nature of the Processing, assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company's obligations to respond to requests for exercising the Data Subject's rights under the Data Protection Legislation;
  - 2.2.16. promptly notify the Company of any request from a Data Subject for access to that person's Personal Data and provide the Company with reasonable co-operation and assistance in complying with any such request;
  - 2.2.17. not respond to any request from a Data Subject or third party except on the documented instructions of the Company or as required by Applying Laws, in which case the Supplier shall to the extent permitted by Applying Laws inform the Company of that legal requirement before the Supplier responds to the request; and
  - 2.2.18. promptly on request, provide to the Company a copy of all Personal Data held or controlled by it in the format and on the media reasonably specified by the Company.
- 2.3. If the Supplier receives any complaint, notice or communication which relates to the Processing of the Personal Data or to either party's compliance with the Data Protection Legislation, it will immediately notify the Company and it shall provide the Company with full co-operation and assistance in relation to any such complaint, notice or communication.
  - 2.4. The Supplier shall not transfer the Personal Data to any Third Country without the prior express written consent of the Company.
  - 2.5. The Supplier shall co-operate with any Regulatory Authority requests relating to the Processing of Personal Data.
  - 2.6. The Supplier agrees to indemnify and keep indemnified the Company against all costs, expenses (including legal and other professional fees and expenses), losses, damages and other liabilities of whatever nature (whether contractual, tortious or otherwise) suffered or incurred by the Company and arising out of or in connection with any breach by the Supplier, its employees, representatives, agents or sub-contractors, of its obligations under these Data Processing Obligations. Any cap on liability provided under the Purchase Order shall not apply to the indemnity given by the Supplier under this clause 2.6.
  - 2.7. Subject to the Supplier being required to maintain such copies by law, upon expiry or termination of the Purchase Order (for any reason whatsoever), the Supplier shall at the request of the Company promptly return to the Company or destroy all Personal Data securely (regardless of form, and whether computerised or physical). The Supplier shall certify the deletion or destruction (as applicable) to the Company in writing.

- 2.8. The Supplier shall immediately notify the Company if, in its opinion, an instruction given by the Company to the Supplier under this clause 2 (Data Processing Obligations) infringes the GDPR, the UK GDPR or any other relevant Data Protection Legislation.
- 2.9. The Supplier shall make available to the Company all information necessary to demonstrate compliance with this clause 2 (Data Processing Obligations) and allow for and contribute to audits including inspections conducted by the Company or another auditor mandated by the Company in relation to the Processing of Personal Data and the implementation of technical and organisations measures by the Supplier as referred to in these Data Processing Obligations.
- 2.10. The Supplier may only authorise a third party (**sub-contractor**) to Process the Personal Data:
  - 2.10.1. provided that the Supplier has carried out adequate due diligence to ensure that the sub-contractor is capable of providing the level of protection required by the Purchase Order;
  - 2.10.2. subject to the Company's prior written consent where the Supplier has supplied the Company with full details of such sub-contractor;
  - 2.10.3. provided that the relationship between the Supplier and the sub-contractor is governed by a written contract which contains obligations in relation to the Processing of Personal Data that are at least as onerous as those set out in this Addendum; and
  - 2.10.4. provided that the sub-contractor's contract terminates automatically on termination of the Purchase Order for any reason.
- 2.11. Any sub-contracting or transfer of Personal Data permitted by the Company shall not relieve the Supplier from any of its liabilities, responsibilities and obligations to the Company under the Purchase Order and the Supplier shall remain fully liable for the acts and omissions of its sub-contractors.