**APPENDIX C – DATA PROTECTION**

1. This Appendix C applies where one Party processes data on behalf of another Party within the meaning of the Data Protection Legislation. Where this Appendix C applies, ‘the Controller’ means the Party which is the ‘controller’, and ‘the Processor’ means the Party which is the ‘processor’, in relation to such processing within the meaning of the GDPR.

1. In this Appendix C (including its Annexes):

“Data Loss Event” means any event that results, or may result, in unauthorised access to Personal Data held by the Processor 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 Protection Impact Assessment” means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data

“Data Protection Legislation” means (i) the General Data Protection Regulation (Regulation (EU) 2016/679) or “GDPR”, the Law Enforcement Directive (Directive (EU) 2016/680) ("LED") and any applicable national implementing Laws as amended from time to time (ii) the Data Protection Act 1998 and/or the Data Protection Act 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 Subject”, “Personal Data”, “Personal Data Breach”, “Processing” (and cognate terms) and “Data Protection Officer” have the meanings given in the GDPR

“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

“Joint Controllers” means two or more controllers (within the meaning of the GDPR who jointly determine the purposes and means of processing (and “Joint Control” shall be construed accordingly)

“Law” means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Controller is bound to comply

“Processor Personnel” means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-processor engaged in the performance of its obligations under this Agreement

“Protective Measures” means appropriate technical and organisational measures which may include but are not limited to: 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 such measures adopted by it including those outlined in Annex 1

“Sub-processor” means any third party appointed to process Personal Data on behalf of the Processor in relation to this Agreement

“Working Day” means any day which is not a Saturday, a Sunday or a public holiday in England

reference to a ‘paragraph’ or ‘Annex’ is to a paragraph of, or Annex to, this Appendix C (as the case may be).

1. The Processing that the Processor is authorised to do is as exhaustively set out in Annex 1 by the Controller and may not be determined by the Processor.

1. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

1. 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;

1. an assessment of the necessity and proportionality of the Processing operations in relation to the purposes of such operations;

1. an assessment of the risks to the rights and freedoms of Data Subjects; and

1. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under this Agreement:

1. Process that Personal Data only in accordance with Annex 1, 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;

1. ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which  the 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:
2. nature of the data to be protected;
3. harm that might result from a Data Loss Event;
4. state of technological development; and
5. cost of implementing any measures;

1. ensure that :
2. the Processor Personnel do not Process Personal Data except in accordance with this Agreement (and in particular Annex 1);
3. 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:
4. are aware of and comply with the Processor’s duties under this paragraph 6;
5. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
6. 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 Agreement; and
7. have undergone adequate training in the use, care, protection and handling of Personal Data;

1. not transfer Personal Data outside of the United Kingdom and European Union unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
2. 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;
3. the Data Subject has enforceable rights and effective legal remedies;
4. 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 endeavours to assist the Controller in meeting its obligations); and
5. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

1. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination or expiry of this Agreement unless the Processor is required by Law to retain the Personal Data.

1. Subject to paragraph 8, the Processor shall notify the Controller immediately if it:
2. receives a Data Subject Request (or purported Data Subject Request);
3. receives a request to rectify, block or erase any Personal Data;
4. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
5. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
6. 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
7. becomes aware of a Data Loss Event.

1. The Processor’s obligation to notify under paragraph 7 shall include the provision of further information to the Controller in phases, as details become available.

1. 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 relating to such obligations (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
2. the Controller with full details and copies of the complaint, communication or request;
3. such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
4. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
5. assistance as requested by the Controller following any Data Loss Event;
6. 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.

1. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Appendix C. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
2. the Controller determines that the Processing is not occasional;
3. the Controller determines that 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
4. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

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

1. Each Party shall designate its own Data Protection Officer if required by the Data Protection Legislation.

1. Before allowing any Sub-processor to Process any Personal Data related to this Agreement, 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 gives effect to the terms set out in this Schedule 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.

1. The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

1. The Controller may, at any time on not less than 30 Working Days’ notice, revise this Appendix C by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall take effect on the expiry of such notice period).

1. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Agency may on not less than 30 Working Days’ notice to the other Parties amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner’s Office (and any such amendment shall take effect on the expiry of such notice period).

1. Where the Parties include two or more Joint Controllers as identified in Annex 1 in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Annex 2 in replacement of paragraphs 1-16 for the Personal Data under Joint Control.

**APPENDIX C – ANNEX 1:** **SCHEDULE OF PROCESSING, PERSONAL DATA AND DATA SUBJECTS**

This Schedule shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Environment Agency’s Data Protection Officer are:

Anna Burns, Data Protection Officer

DataProtection@environment-agency.gov.uk

Horizon House, Deanery Road, Bristol BS1 5AH

2. The contact details of the [*name of party*]’s Data Protection Officer are: [Insert Contact details]

3. The Processor shall comply with any further written instructions with respect to Processing by the Controller.

4. Any such further instructions shall be incorporated into this Annex 1.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of the Controller and Processor | The Parties acknowledge that for the purposes of the Data Protection Legislation, [*name*] is the Controller and [*name*] is the Processor in accordance with Paragraph 1.    [**Guidance:** You may need to vary this section where (in the rare case) the Agency and the other Parties have a different relationship. For example where the Parties are Joint Controller of some Personal Data:    *“Notwithstanding paragraph 1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:*  ***[Insert*** *the scope of Personal Data in relation to which the purposes and means of Processing are determined by more than one of the Parties]*    *In respect of Personal Data under Joint Control, paragraphs 1 to 16 will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Annex 2 instead.”* |
| Subject matter of the processing | *[This should be a high level, short description of what the processing is about i.e. its subject matter.*    *Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public. ]* |
| 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 being Processed | *[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 EU or member state law to preserve that type of data | *[Describe how long the data will be retained for, how it will be returned or destroyed]* |