Annex 9 – Data Protection Terms

Data Protection Terms for Data Processor Contracts

The General Data Protection Regulation (GDPR) becomes effective in the UK on 25 May 2018. As of this date, all data control and processing that takes place in the UK must be compliant with the provisions of the GDPR. The GDPR requirements include an obligation on data controllers to ensure that their data is not processed by third parties unless there is a written contract in place containing clauses compliant with the GDPR. There is also an obligation on data processors not to process third party data without the written authority of the data controller.

For any contract where the provisions of the Data Protection Legislation apply to personal data processed in relation to the performance of the contract, the following conditions supplement the conditions of the contract

1. **DEFINITIONS**

   1.1 **Applicable Laws**: means laws relating to the processing of Personal Data of any member of the European Union or of the European Union and applicable to the Contractor.

   1.2 **Data Protection Legislation**: means (i) until 25 May 2018, the Data Protection Act 1998 then from 25 May 2018 (ii) unless and until the GDPR is no longer directly applicable in the UK, the GDPR and any national implementing laws, regulations and secondary legislation, as amended from time to time, in the UK and then (iii) any successor legislation to the GDPR or the Data Protection Act 1998.

   1.3 **Personal Data**: means personal data as defined in the Data Protection Legislation.

2. **DATA PROTECTION**

   2.1 Both Parties shall comply with all applicable requirements of the Data Protection Legislation. This clause 2 is in addition to, and does not relieve, remove or replace, a Party's obligations under the Data Protection Legislation.

   2.2 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Contractor is the data processor and the Authority is the data controller (where data controller and data processor have the meanings as defined in the Data Protection Legislation). Schedule 1 sets out the scope, nature and purpose of processing by the data processor, the duration of the processing and the types of Personal Data and categories of data subject.

2.3   Without prejudice to the generality of clause 2.1, the data controller will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the data processor for the duration and purposes of this Contract.

2.4   Without prejudice to the generality of clause 2.1, the data processor shall, in relation to any Personal Data processed in connection with the performance of its obligations under this Contract:

2.4.1   process that Personal Data only on the written instructions of the data controller, including with regard to transfers of personal data to a third country or an international organisation, unless the data processor is required by the Applicable Laws to process Personal Data. Where the data processor is relying on the Applicable Laws as the basis for processing Personal Data, the data processor shall promptly notify the data controller of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the data processor from so notifying the data controller;

2.4.2   ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;

2.4.3   ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the data controller, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its 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 technical and organisational measures adopted by it);

2.4.4   not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the data controller has been obtained and the following conditions are fulfilled:

(a)   the data controller or the data processor have provided appropriate safeguards in relation to the transfer;

(b)   the data subject has enforceable rights and effective legal remedies;

(c)   the data processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

(d)   the data processor complies with reasonable instructions notified to it in advance by the data controller with respect to the processing of the Personal Data;

2.4.5   assist the data controller in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

2.4.6   notify the data controller without undue delay on becoming aware of a Personal Data breach;

2.4.7   at the written direction of data controller, delete or return all Personal Data and copies thereof to the data controller on termination of the Contract unless required by the Applicable Laws to store the Personal Data;

2.4.8   maintain complete and accurate records and information to demonstrate its compliance with this clause 2 and allow for audits by the data controller or the data controller's designated auditor; and

2.4.9   immediately inform the data controller if, in its opinion, an instruction infringes the Applicable Laws.

2.5   The data controller consents to the data processor appointing third-party processors of Personal Data under this Contract. As between the data controller and the data processor, the data processor shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this clause 2.5. The data processor confirms that:

2.5.1   it will notify the data controller of the identity of any proposed third-party processor prior to its appointment and will not appoint the third-party processor if the data controller objects in writing to the appointment; and

2.5.2   it will enter with the third-party processors into written agreements incorporating terms which are substantially similar to those set out in this clause 2.

2.6   The data controller may, at any time on not less than 30 days' notice, revise this clause 2 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 replaced by attachment to this Contract).

2.7   The provisions of this condition shall apply for the duration of the Contract and indefinitely after its expiry or termination.

SCHEDULE 1

THE PROCESSING OF PERSONAL DATA

This schedule sets out the scope, nature and purpose of the processing of Personal Data by the data processor on behalf of the data controller and constitutes the written instructions of the data controller referred to in clause 2.4.1. The data processor may only process Personal Data on behalf of the data controller in accordance with the requirements of clause 2 and this schedule.

1.   **THE SCOPE, NATURE AND PURPOSE OF PROCESSING**

1.1   The data processor may process Personal Data in order to [set out how the processor may process Personal Data, the purpose of that processing and any limitations on the processing that may be undertaken]

2.   **THE DURATION OF PROCESSING**

2.1   The data processor may process Personal Data for the duration of the Contract.

3.   **THE TYPES OF PERSONAL DATA**

3.1   The data processor may process Personal Data of the following types:

        (a)   [personal details]

        (b)   [family, lifestyle and social circumstances]

        (c)   [financial details]

        (d)   [employment and education details]

        (e)   [goods or services provided]

3.2   The data processor [may not process sensitive Personal Data] [may process sensitive Personal Data of the following types:

        (a)   [physical or mental health details]

        (b)   [racial or ethnic origin]

        (c)   [religious or philosophical beliefs]

        (d)   [trade union membership]

        (e)   [political opinions]

        (f)   [genetic data]

        (g)   [biometric data]

        (h)   [sex life and sexual orientation]]

4.   **THE CATEGORIES OF DATA SUBJECT**

4.1   The data processor may process Personal Data relating to the data controller's:

        (a)   [employees]

        (b)   [customers and clients]

        (c)   [suppliers and service providers]

        (d)   [advisors, consultants and other professional experts]

(e)   [complainants and enquirers].