**Data Protection Provisions**

1. **Definitions**

In these data protection provisions the following definitions shall apply:

|  |  |
| --- | --- |
| "**Applicable Law**" | means the law of the United Kingdom |
| **" Controller", "Processor" and "Data Subject"** | shall have the meaning given to those terms in the applicable Data Protection Laws; |
| "**Data Protection Impact Assessment**" | means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data; |
| "**Data Protection Laws**" | means (a) any law, statute, declaration, directive, regulation, or other legislative enactment (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the GDPR and all legislation enacted in the UK in respect of the protection of personal data; including the UK GDPR as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003; and; (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time; |
|  |
|  |
| "**Data Processing Particulars**" | means, in relation to any Processing under this Agreement:  (a) the subject matter and duration of the Processing;  (b) the nature and purpose of the Processing;  (c) the type of Personal Data being Processed; and  (d) the categories of Data Subjects;  as set out in Schedule 1. |
|  |
|  |
|  |
| "**Data Subject Request**" | means an actual or purported request from a Data Subject exercising his rights under the Data Protection Laws in relation to Personal Data including without limitation: the right of access by the Data Subject, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability and the right to object; |
| "**GDPR**" | means the General Data Protection Regulation (EU) 2016/679; |
| "**ICO**" | means the UK Information Commissioner's Office, or any successor or replacement body from time to time; |
| "**ICO Correspondence**" | means any correspondence or communication (whether written or verbal) from the ICO in relation to the Processing of Personal Data; |
| **"Losses"** | means all losses, fines, penalties, liabilities, damages, costs, charges, claims, amounts paid in settlement and expenses (including legal fees (on a solicitor/client basis), disbursements, costs of investigation (including forensic investigation), litigation, settlement (including ex gratia payments), judgment, interest and penalties), other professional charges and expenses, disbursements, cost of breach notification including notifications to the data subject, cost of complaints handling (including providing data subjects with credit reference checks, setting up contact centres (e.g. call centres) and making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise; |
| "**Permitted** **Purpose**" | means the purpose of the Processing as specified in the Data Processing Particulars; |
| "**Personal Data**" | means any personal data (as defined in the Data Protection Laws) Processed by either Party in connection with this Agreement, and for the purposes of this Agreement includes Sensitive Personal Data (as such Personal Data is more particularly described in Schedule 1 (*Data Processing Particulars*)); |
| "**Personal Data Breach**" | has the meaning set out in the Data Protection Laws; |
| **"Personal Data Breach Particulars"** | means the information that must be included in a Personal Data Breach notification, as set out in Article 33(3) of the GDPR; |
| "**Personnel**" | means all persons engaged or employed from time to time by the Supplier in connection with this Agreement, including employees, consultants, contractors and permitted agents; |
| "**Processing**" | has the meaning set out in the Data Protection Laws (and "**Process**" and "**Processed**" shall be construed accordingly); |
|  |  |
| "**Security Requirements**" | means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws (including, in particular, the seventh data protection principle of the DPA and/ or the measures set out in Article 32(1) of the GDPR (taking due account of the matters described in Article 32(2) of the GDPR)) as applicable; |
| **"Sensitive Personal Data"**  **“Third Party Request”** | means Personal Data that reveals such special categories of data as are listed in Article 9(1) of the GDPR; |
| **“UK GDPR”** | means a written request from any third party for disclosure of Personal Data where compliance with such a request is required or purported to be required by law or regulation; and  Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act of 2018. |

2.      DATA PROTECTION

**2.1**Arrangement Between the Parties

2.1.1         The Parties shall each Process the Personal Data.  The Parties acknowledge that the factual arrangements between them dictate the classification of each Party in respect of the Data Protection Laws.  Notwithstanding this, the Parties anticipate that, in respect of the Personal Data, as between the Customer and the Supplier for the purposes of this Agreement, the Customer shall act as the Controller and the Supplier shall act as the Processor, as follows:

a)      The Customer shall be the Controller where it is Processing Personal Data in relation to the Permitted Purpose; and

b)     the Supplier shall be the Data Processor where it is Processing Personal Data in relation to the Permitted Purpose in connection with the performance of its obligations under this Agreement.

2.1.1        Each of the Parties acknowledges and agrees that Schedule 1 (*Data Processing Particulars*) to this Agreement is an accurate description of the Data Processing Particulars.

2.1.2        Nothing within this Agreement relieves the Supplier of its own direct responsibilities and liabilities under the Data Protection Laws.

2.1.3        Each Party shall make due notification to any relevant regulator.

2.1.4        the Supplier undertakes to the Customer that it will take all necessary steps to ensure that it operates at all times in accordance with the requirements of the Data Protection Laws and the Supplier will, at its own expense, assist the Customer in discharging its obligations under the Data Protection Laws as detailed in this Paragraph 2. The Supplier shall not, whether by act or omission, cause the Customer to breach any of its obligations under the Data Protection Laws.

2.2     **Data Processor Obligations**

2.2.1        To the extent that the Supplier Processes any Personal Data as a Processor for and on behalf of the Customer (as the Controller) it shall:

a)                only Process the Personal Data for and on behalf of the Customer for the purposes of performing its obligations under this Agreement, and only in accordance with the terms of this Agreement and any documented instructions from the Customer;

b)               keep a record of any Processing of the Personal Data it carries out on behalf of the Customer;

c)                unless prohibited by law, notify the Customer immediately (and in any event within twenty-four (24) hours of becoming aware of the same) if it considers, in its opinion (acting reasonably) that it is required by Applicable Law to act other than in accordance with the instructions of the Customer, including where it believes that any of the Customer’s instructions under Paragraph 2.2.1(a) infringe any of the Data Protection Laws;

d)               take, implement and maintain appropriate technical and organisational security measures which are sufficient to comply with at least the obligations imposed on the Customer by the Security Requirements and where requested provide to the Customer evidence of its compliance with such requirements.

e)               within thirty (30) calendar days of a request from the Customer, allow its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the Customer (and/ or its representatives, including its appointed auditors) in order to ascertain compliance with the terms of this Paragraph 2, and provide reasonable information, assistance and co-operation to the Customer, including access to relevant Personnel and/ or, on the request of the Customer, provide the Customer with written evidence of its compliance with the requirements of this Paragraph 2;

f)                 not disclose Personal Data to a third party (including a sub-contractor) in any circumstances without the Customer's prior written consent, save in relation to Third Party Requests where the Supplier is prohibited by law or regulation from notifying the Customer, in which case it shall use reasonable endeavours to advise the Customer in advance of such disclosure and in any event as soon as practicable thereafter;

g)                promptly comply with any request from the Customer to amend, transfer or delete any Personal Data;

h)               notify the Customer promptly (and in any event within forty-eight (48) hours) following its receipt of any Data Subject Request or ICO Correspondence and shall:

(i)                         not disclose any Personal Data in response to any Data Subject Request or ICO Correspondence without first consulting with and obtaining the Customer’s prior written consent; and

(ii)                        provide the Customer with all reasonable co-operation and assistance required by the Customer in relation to any such Data Subject Request or ICO Correspondence;

i)                 notify the Customer promptly (and in any event within twenty-four (24) hours) upon becoming aware of any actual or suspected, threatened or ‘near miss’ Personal Data Breach in relation to the Personal Data (and follow-up in writing) and shall:

(i)                         conduct or support the Customer in conducting such investigations and analysis that the Customer reasonably requires in respect of such Personal Data Breach;

(ii)                        implement any actions or remedial measures necessary to restore the security of compromised Personal Data; and

(iii)                      assist the Customer to make any notifications to the ICO and affected Data Subjects;

j)                 comply with the obligations imposed upon a Processor under the Data Protection Laws;

k)                use all reasonable endeavours to assist the Customer to comply with the obligations imposed on the Customer by the Data Protection Laws, including:

(i)                         compliance with the Security Requirements;

(ii)                        obligations relating to notifications required by the Data Protection Laws to the ICO and/ or any relevant Data Subjects;

(iii)                      undertaking any Data Protection Impact Assessments (and, where required by the Data Protection Laws, consulting with the ICO and/or any other relevant Regulator in respect of any such Data Protection Impact Assessments); and

(iv)                     notifying the Customer within 24 hours after becoming aware of a Personal Data Breach;

l)                 Upon the earlier of:

(i)                         termination or expiry of this Agreement (as applicable); and

(ii)                        the date on which Personal Data is no longer relevant to, or necessary for, the Permitted Purpose,

the Supplier shall cease Processing all Personal Data and return and/ or permanently and securely destroy so that it is no longer retrievable (as directed in writing by the Customer) all Personal Data and all copies in its possession or control and, where requested by the Customer, certify that such destruction has taken place except to the extent required by Applicable Law to retain the Personal Data;

m)            not transfer or otherwise process (and not instruct or permit a third party to transfer or otherwise process) Personal Data to a country outside of the UK without obtaining the Customer’s prior written consent;

2.3     Supplier Personnel

2.3.1        The Supplier shall take all reasonable steps to ensure the reliability and integrity of any of the Personnel who shall have access to Personal Data (including, without limitation, ensuring such Personnel shall have undergone reasonable levels of training in Data Protection Laws and in the care and handling of Personal Data), and ensure that each member of Personnel shall have entered into appropriate contractually-binding confidentiality undertakings.

2.4     Appointing Sub-contractors

2.4.1        If the Customer has provided written consent to the Supplier permitting the Supplier to appoint a sub-contractor, the Supplier shall be permitted to disclose Personal Data to such sub-contractor for Processing in accordance with the Supplier's obligations under this Agreement, provided always that:

a)                the Supplier undertakes thorough due diligence on the proposed sub-contractor, including a risk assessment of the information governance-related practices and processes of the proposed sub-contractor, which shall be used by the Supplier to inform any decision on appointing the proposed sub-contractor;

b)               the Supplier provides the Customer with full details of the proposed sub-contractor including the results of the due diligence undertaken in accordance with Paragraph 2.4.1(a) before its appointment and the Customer has consented to such appointment in writing;

c)      the sub-contractor contract (as it relates to the Processing of Personal Data) is on terms which are substantially the same as, and in any case no less onerous than, the terms set out in these data protection provisions*;*

d)    the sub-contractor's right to Process Personal Data terminates automatically on expiry or termination of this Agreement for whatever reason.

2.4.2        Notwithstanding any consent or approval given by the Customer under Paragraph 2.4.1, the Supplier shall remain primarily liable to the Customer for the acts, errors and omissions of any sub-contractor to whom it discloses Personal Data, and shall be responsible to the Customer for the acts, errors and omissions of such sub-contractor as if they were the Supplier's own acts, errors and omissions to the extent that the Supplier would be liable to the Customer under this Agreement for those acts, errors and omissions.

2.5     Notwithstanding anything in this Agreement to the contrary, these data protection provisions shall continue in full force and effect for so long as the Supplier Processes any Personal Data.

3         Recoverable Loss

3.1     Notwithstanding any other clause, the Customer shall not be prevented from recovering any Losses it incurs.

4         INDEMNITY

4.1     The Supplier shall indemnify on demand and keep indemnified the Customer from and against:

4.1.1        any monetary penalties or fines levied by the ICO on the Customer;

4.1.2        the costs of an investigative, corrective or compensatory action required by the ICO and or of defending proposed or actual enforcement taken by the ICO;

4.1.3        any Losses suffered or incurred by, awarded against, or agreed to be paid by, the Customer pursuant to a claim, action or challenge made by a third party against the Customer (including by a Data Subject); and

4.1.4        except to the extent that Paragraphs 4.1.1 and/ or 4.1.2 and/ or 4.1.3 apply, any Losses suffered or incurred, awarded against, or agreed to be paid by, the Customer,

in each case to the extent arising as a result of a breach by the Supplier (or its sub-contractors) of this Agreement and/ or their respective obligations under the Data Protection Laws.

4.2     Nothing in this Agreement will exclude, limit or restrict the Supplier's liability under the indemnity set out in Paragraph 4.1.

5         INSURANCE

5.1     The Supplier agrees to obtain and keep in full force and effect at all times a policy or policies of insurance to cover all liabilities under this Agreement:

a)                it must cover liability arising to any person;

b)               it must apply in relation to the Processing of Personal Data; and

c)                it must have policy limits and provisions conforming to such requirements as the Customer may from time to time reasonably prescribe;

5.1.2        to deliver to the Customer upon request:

a)                copies of all applicable insurance policies taken out pursuant to the provisions of this Agreement; and

b)               evidence of premiums paid in relation to such insurance; and

5.1.3        to ensure that the Customer shall be entitled to the benefit under such insurance and that the Customer's interest will be noted on the policy.

**Schedule 1**

|  |  |
| --- | --- |
| **The subject matter of the Processing** | The supply of goods and/or services |
| **The nature of the Processing** | Obtaining details relating to employees, consultants, contractors and permitted agents of the Supplier.    Obtaining details relating to employees, consultants, contractors and permitted agents of the Customer. |
| **The duration of the Processing** | For the length of the supply of the relevant goods and/or services. |
| **The purpose of the Processing** | To provide the goods and/or services and to comply with the terms and conditions governing the supply of goods and/or services. |
| **The type of Personal Data being Processed** | Personal data - name, contact details, employment details including delivery address, email address, telephone numbers.  Payment Data – bank account, payment card details and details about payments to the Supplier from the Customer or credits from the Supplier to the Customer. |
| **The categories of Data Subjects** | Employees, consultants, contractors and permitted agents. |