GDPR - The General Data Protection Regulation

Generic Standard Clauses

Party: a Party to this Agreement
Agreement: this contract;
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 Contractor is bound to comply;
Contractor Personnel: means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any Sub-Contractor engaged in the performance of its obligations under this Agreement.**]**

GDPR CLAUSE DEFINITIONS:
The following definitions and those in bold in round brackets elsewhere will apply to this [Clause/ Contract/ Agreement].
Data Protection Legislation: (i) unless/until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK (ii) any successor legislation to the GDPR or the Data Protection Act 1998; the LED and any Applicable national implementing Laws as amended from time to time; the DPA 2018 to the extent that it relates to processing of personal data and privacy; and (iii) Applicable Law about the processing of personal data and privacy which includes The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), The Electronic Communications Data Protection Directive 2002/58/EC, The Privacy and Electronic Communications (EC Directive) Regulations 2003.
Data Protection Impact Assessment: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
Controller, **Processor, Process, Processing**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Data Protection Officer,** take the meaning given in the GDPR and their cognate terms shall be construed accordingly.
Data Loss Event: any event that results, or may result, in unauthorised access to Personal Data held by the Contractor 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 Subject Access Request: 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.
DPA 2018: Data Protection Act 2018
GDPR: the General Data Protection Regulation *(Regulation (EU) 2016/679)*
LED: Law Enforcement Directive *(Directive (EU) 2016/680)*
Protective Measures: appropriate technical and organisational measures which may include: pseudonym-ising 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 the such measures adopted by it.

Sub-processor: any third Party being any person appointed by or on behalf of the Contractor to process Personal Data on behalf of the Contractor related to this Agreement being to Process Personal Data on behalf of the Council in connection with the Contract;

1. DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, *the Council is the Controller and the Contractor is the Processor*. The only processing that the Contractor is authorised to do is listed in Schedule A by the Council and may not be determined by the Contractor.

1.2 Both Parties will comply with all applicable requirements of the Data Protection Legislation.

1.3 This clause 1.3 is in addition to, and does not relieve, remove or replace, a Party's obligations under the Data Protection Legislation.

1.4 Schedule A sets out the scope, nature and purpose of processing by the Contractor, the duration of the processing and the types of personal data and categories of Data Subject.

1.5 The Contractor shall notify the Council immediately if it considers that any of the Council's instructions infringe the Data Protection Legislation and shall not knowingly or negligently do or omit to do anything which places the Council in breach of the Council's obligations under the Data Protection Legislation..

1.6.1 The Contractor shall provide all reasonable assistance to the Council in the preparation of any Data Protection Impact Assessment prior to commencing any processing or at any time. Such assistance may, at the discretion of the Council, include:
> (a) a systematic description of the envisaged processing operations and the purpose of the processing;
> (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
> (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
> (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.6.2 The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:
> (a) process that Personal Data only in accordance with Schedule A, unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Council before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures to ensure a level of security appropriate to the risks, including, as appropriate, the measures referred to in Article 32(1) of the GDPR, which have been reviewed and approved by the Council as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature and scope as well as context and purposes of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Contractor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule A);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Contractor's duties under this clause;

(ii) are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;

(iii) 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 Council or as otherwise permitted by this Agreement; and

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU or European Economic Area unless the prior written consent of the Council has been obtained and the following conditions are fulfilled:

(i) the Council or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Council;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Contractor 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 Council in meeting its obligations); and

(iv) the Contractor complies with any reasonable instructions notified to it in advance by the Council with respect to the processing of the Personal Data;

(e) at the written direction of the Council, delete or return Personal Data (and any copies of it) to the Council on termination of the Agreement unless the Contractor is required by Law to retain the Personal Data.

1.6.3 Subject to clause 1.6, the Contractor shall notify the Council immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) 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

(f) becomes aware of a Data Loss Event.

1.6.4 The Contractor's obligation to notify under clause 1.5 shall include the provision of further information to the Council in phases, as details become available.

1.6.5 Taking into account the nature of the processing, the Contractor shall provide the Council with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Council) including by promptly providing:

(a) the Council with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Council to enable the Council to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Council, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Council following any Data Loss Event;

(e) assistance as requested by the Council with respect to any request from the Information Commissioner's Office, or any consultation by the Council with the Information Commissioner's Office.

1.6.6 The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause under the obligation in Articles 28(3)(h) and 30(2) GDPR. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:

(a) the Council determines that the processing is not occasional;

(b) the Council determines (or the Contractor is aware 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; and/or

(c) the Council determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.7 The Contractor shall allow for audits of its Data Processing activity by the Council or the Council's designated auditor.

1.8 The Contractor shall designate a data protection officer if required by the Data Protection Legislation.

1.9 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Contractor must:
      (a) notify the Council in writing of the intended Sub-processor and processing;
      (b) obtain the written consent of the Council;
      (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 1.9 (c) such that they apply to the Sub-processor; and
      (d) provide the Council with such information regarding the Sub-processor as the Council may reasonably require.

1.10 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

1.11 The Council may, at any time on not less than 30 Working Days' notice, revise this clause 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 incorporated by attachment to this Agreement) per Articles 28(6), 28(7) and 28(8) GDPR.

1.12 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Council may on notice to the Contractor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.13 Without prejudice to the rest of this clause 1.13, the Contractor shall, in relation to any Personal Data processed in connection with the performance by the Contractor of its obligations under this agreement process that Personal Data only on the written instructions of the Council unless the Contractor is required by the laws of any member of the European Union or by the laws of the European Union applicable to the Contractor to process Personal Data (Applicable Laws). Where the Contractor is relying on laws of a member of the European Union or European Union law as the basis for processing Personal Data, the Contractor shall promptly notify the Council of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Contractor from so notifying the Council.

1.14 The Contractor shall fully indemnify the Council in respect of all losses, liabilities, claims, actions, proceedings, demands, costs, charges or expenses arising out of or in connection with any civil claim made in respect information subject to the Data Protection Legislation , which claims would not have arisen but for some act, omission or negligence in breach of this condition on the part of the Contractor, its employees, agents or any subcontractor or anyone acting on its or their behalf.

1.15 The Parties agree that on the termination of the Contract/Agreement, the Processor and any Sub-Processor shall, at the choice of the Controller, return all personal data and copies thereof to the Council or shall destroy all the personal data and certify to the Council that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the

confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

1.16 The Contractor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Processor who may have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Contract, and to comply with Data Protection Legislation in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

Obligations after the termination of the Service
1.17 The provisions of this clause 1.17 shall apply during the continuance of the agreement and indefinitely after its expiry or termination.

1.18 The Parties agree that on the termination of the provision of the Service, the Data Processor and any Sub-processor shall, at the choice of the Data Controller, return all the personal data transferred and the copies thereof to the Data Controller or shall destroy all the personal data and certify to the Data Controller that it has done so, unless legislation imposed upon the Data Processor prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Processor warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.