**Supplier Due Diligence Questionnaire**

**The Supplier is the Data Processor**

|  |
| --- |
|  |
| As part of the provision of the (proposed) Service(s), we understand you will process personal data on our behalf as a “**processor**.”  To give us comfort that you are able to do this compatibly with data protection legislation, we kindly ask you to complete our attached Supplier Due Diligence Questionnaire and send your response to procurement@frc.org.uk. If, in providing your service, you will not process any personal data on our behalf, please explain why this is the case in your response to Question 2. | |
|
|
|
|

|  |  |  |
| --- | --- | --- |
|  | **Question** | **Answer** |
| **General** | | |
|  | Data protection contact details. |  |
|  | Brief description of service provided and personal data you will process on the FRC’s behalf. |  |
| **Sub-Processors** | | |
|  | Third parties to whom you will disclose FRC personal data. |  |
|  | Your process for choosing sub-processors and auditing their compliance. |  |
| **Overseas transfers** | | |
|  | Geographic location(s) in which you / your sub-processors will process our personal data including for storage and back up purposes. |  |
|  | How transfers of our personal data out of the UK or the EEA – including to sub-processors - will be made compatibly with data protection legislation. |  |
|  |  |  |
| **Data Subjects** | | |
|  | Details of how you can delete, amend and extract our personal data and restrict its use upon request. |  |
|  | Process and timing for notifying us if you receive a request from a data subject of our personal data. |  |
| **Security and breaches** | | |
|  | Technical and organisational security measures (including security certifications) in place to secure our personal data. |  |
|  | Process and timing for notifying us if our personal data is involved in a data breach. |  |
|  | Have you had to notify the ICO of a personal data breach within the last 12 months? |  |
|  | If yes, please confirm what steps have been taken to prevent a recurrence of that or similar breaches. |  |
| **UK GDPR compliance** | | |
|  | As data controller the obligation is on the FRC to have GDPR compliant processor terms in place. Our standard Data Processing Terms are below. Please confirm if you have any objection to entering into these terms. |  |
|  | Details of how your service is GDPR compliant (in particular with the principles in Articles 5) plus copies of any relevant data protection impact assessments. |  |

**Personal Data Processing**

|  |  |
| --- | --- |
| Description | Details |
| Data protection contact details | Name:  Email:  Telephone: |
| **FRC’s** Data protection contact details | DPO - [*privacy@frc.org.uk*](mailto:privacy@frc.org.uk) |
| Identity of Controller for each Category of Personal Data | The supplier is the Data Processor. |
| Duration of the Processing | For example,  Throughout the duration of the Agreement.  Up to xx years after the expiry or termination of the Agreement |
| Nature and purposes of the Processing | For example  To facilitate the fulfilment of the Supplier’s obligations arising under this Agreement specifically     * TBA * TBA   Furthermore including   * Ensuring effective communication between the Supplier and FRC * Maintaining full and accurate records in accordance with any Record Keeping and Reporting provisions under the Agreement. |
| Type of Personal Data | For example, including but not limited to Name, Email, Telephone, Membership, Race, Sex, Religion, Education, Images, data monitoring usage, biometrics political opinion. |
| Categories of Data Subject | For example, including but not limited to FRC’s (contact persons/representatives); Customers; Staff; Directors; Current staff; Potential staff; Contractor / Consultant ; Temporary agency worker |
| Plan for return and destruction of the data once the Processing is complete | For examples, Data will be retained for the delivery of the contract. It will then be securely destroyed according to ISO27001 compliant practices. |

**Data Processing Clause**

1. Data Protection
   1. *Definitions:* In this Clause, the following terms shall have the following meanings:
2. "**controller**", "**processor**", "**data subject**", "**personal** **data**" and "**processing**" (and "**process**") shall have the meanings given in Applicable Data Protection Law;
3. "**Applicable Data Protection Law**" shall mean UK Data Protection law and, where relevant, EU Data Protection Law;
4. "**EU Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU** **GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iii) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;
5. "**UK Data Protection Law**" means: (i) the EU GDPR as saved into domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK** **GDPR**"); (ii) the Data Protection Act 2018; and (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003, in each case as may be amended, repealed, revoked or replaced from time to time; and
6. “**Service Provider**” means you/your company/ the Supplier.
   1. *Relationship of the parties:* In connection with this agreement for supplies/services, as applicable, to the Financial Reporting Council ("**FRC**") the FRC (the controller) appoints Service Provider as a processor to process the personal data identified in clause 1.3 below and in the Agreement. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.
   2. *Personal Data (the “****Data****”):* The Parties acknowledge that the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects are set out further in the Agreement (for these purposes Agreement includes any quote, purchase order or documentation which describes the provision of the relevant supplies/services).
   3. *Purpose limitation:* Service Provider shall process the Data as a processor and only as necessary to perform its obligations under the Agreement and strictly in accordance with any documented instructions of FRC (the "**Permitted Purpose**"), except where otherwise required by law(s) that are not incompatible with Applicable Data Protection Law. In no event shall Service Provider process the Data for its own purposes or those of any third party. Service Provider shall immediately inform FRC if it becomes aware that FRC's processing instructions infringe Applicable Data Protection Law.
   4. *International transfers:* Service Provider shall not transfer the Data (nor permit the Data to be transferred) outside of the United Kingdom or, where applicable, the European Economic Area ("**EEA**") unless (i) it has first obtained FRC's prior written consent; and (ii) it takes such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law, including but not limited to: (i) transferring the Data to a recipient in a country that the Secretary of State or the European Commission (as applicable) has decided provides adequate protection for personal data, (ii) to a recipient that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law, , or (iii) to a recipient that has executed standard contractual clauses adopted or approved by the Secretary of State or the Information Commissioner or, where relevant, the European Commission.
   5. *Confidentiality of processing:* Service Provider shall ensure that any person that it authorises to process the Data (including Service Provider's staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a duty of confidentiality. Service Provider shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.
   6. *Security:* Service Provider shall implement appropriate technical and organisational measures to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Incident**"). Such measures shall include (without limitation), as appropriate:
7. the pseudonymisation and encryption of personal data;
8. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
9. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
10. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

and any additional measures reasonably requested by the FRC.

* 1. *Subprocessing:* Service Provider shall not subcontract any processing of the Data to a third party subprocessor without the prior written consent of FRC. Notwithstanding this and subject to clause 1.5, FRC consents to Service Provider engaging third party subprocessors to process the Data provided that: (i) Service Provider provides at least 30 days' prior notice of the addition or removal of any subprocessor (including details of the processing it performs or will perform and details of the adequate protections in place for transfers to or by the intended third party processor out of the United Kingdom or the EEA as applicable), which may be given by emailing to [gdprcontracts@frc.org.uk](mailto:gdprcontracts@frc.org.uk) details of such addition or removal; (ii) Service Provider imposes data protection terms on any subprocessor it appoints that protect the Data to the same standard provided for by this clause 1.8; and (iii) Service Provider remains fully liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor. If FRC refuses to consent to Service Provider's appointment of a third party subprocessor on reasonable grounds relating to the protection of the Data, then either Service Provider will not appoint the subprocessor or FRC may elect to suspend or terminate the Agreement without penalty.
  2. *Cooperation and data subjects' rights:* Service Provider shall provide all reasonable and timely assistance including by appropriate technical and organisational measures to FRC to enable FRC to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Service Provider, Service Provider shall promptly inform FRC providing full details of the same.
  3. *Data Protection Impact Assessment:* If Service Provider believes or becomes aware that its processing of the Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall promptly inform FRC and provide FRC with all such reasonable and timely assistance as FRC may require in order to conduct a data protection impact assessment in accordance with Applicable Data Protection Law including, if necessary, to assist FRC to consult with the Information Commissioner's Office.
  4. *Security incidents:* Upon becoming aware of a Security Incident, Service Provider shall inform FRC without undue delay and shall provide all such timely information and cooperation as FRC may require in order for FRC to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Service Provider shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep FRC informed of all developments in connection with the Security Incident.
  5. *Deletion or return of Data:* Upon termination or expiry of the Agreement, Service Provider shall (at FRC's election) destroy or return to FRC all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing). This requirement shall not apply to the extent that Service Provider is required by any applicable Law to retain some or all of the Data, in which event Service Provider shall isolate and protect the Data from any further processing except to the extent required by such law until deletion is possible.
  6. *Audit:* You agree to provide reasonable assistance including the provision of information upon the FRC’s reasonable request to enable the FRC to audit data protection compliance, for example but not limited to, cooperation with a competent data protection authority; or if the FRC believes a further audit is necessary due to a Security Incident suffered by Service Provider.

**[OPTIONAL]**

**Annex**

**Security Measures**

**[List any agreed security measures here.]**