Protection of Personal Data
(Where Personal Data is being processed On behalf of the Authority)

DEFCON 532B
Edition 04/20

Definitions

1. In this Condition the following words and expressions shall have the meanings given to them, except where the context requires a different meaning:

a. '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 the Contract;

b. 'Data Loss Event' means any event that results in unauthorised access to Personal Data held by the Contractor under this Contract, and/or actual loss and/or destruction of Personal Data in breach of the Contract, including any Personal Data Breach;

c. 'Data Protection Legislation' means

(1) the GDPR and any applicable national implementing Laws as amended from time to time;

(2) the DPA 2018 to the extent that it relates to processing of personal data and privacy; and

(3) all applicable Law about the processing of personal data and privacy;

d. 'Data Protection Impact Assessment' means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;

e. 'Data Subject 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;

f. 'DPA 2018' means the Data Protection Act 2018;

g. 'GDPR' means the General Data Protection Regulation (Regulation (EU) 2016/679);

h. '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;

i. 'Protective Measures' means appropriate technical and organisational measures which may include (as appropriate):

(1) pseudonymising and encrypting Personal Data;

(2) ensuring confidentiality, integrity, availability and resilience of systems and services;

(3) ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident; and

(4) regularly assessing and evaluating the effectiveness of such measures adopted by it, including those set out in DEFFORM 532;

j. 'Sub-processor'" means any third Party appointed to process Personal Data on behalf of the Contractor related to the Contract;

k. The following expressions shall have the same meanings as in Article 4 of the GDPR:

(1) Controller;

(2) Processor;

(3) Data Subject;

(4) Personal Data;

(5) Personal Data Breach; and

(6) Data Protection Officer.

Data Protection

2. In connection with the Personal Data received under the Contract, each Party undertakes to comply with its obligations under Data Protection Legislation and in particular, but without limitation, each Party shall take appropriate technical and organisational measures against unauthorised or unlawful Processing of Personal Data provided to it by the other Party, and against accidental loss, alteration, unauthorised disclosure or destruction of or damage to that Personal Data.

3. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is listed in DEFFORM 532 by the Authority and may not be determined by the Contractor. The completed DEFFORM 532 shall form part of the Specification for the Contract.

4. The Contractor shall notify the Authority without undue delay if it considers that any of the Authority's instructions infringe the Data Protection Legislation. The Authority agrees that the Contractor shall not be required to provide legal advice to the Authority and that no notification (or absence of notification) by the Contractor will be construed as legal advice or a representation by the Contractor.

5. The Contractor shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any processing that is likely to result in a high risk to the rights and freedoms of Data Subjects. Such assistance may, at the discretion of the Authority, 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 provided under the Contract;

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.

6. The Contractor shall, in relation to any Personal Data processed in connection with its obligations under the Contract:

a. process that Personal Data only in accordance with DEFFORM 532, unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Authority before processing the Personal Data unless prohibited by Law;

b. ensure that it has in place Protective Measures, including those set out in DEFFORM 532, as appropriate to protect against a Data Loss Event, which the Authority may acting reasonably reject (but failure to reject shall not amount to approval by the Authority of the adequacy of the Protective Measures), having taken account of the:

(1) nature of the data to be protected;

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

(3) state of technological development; and

(4) cost of implementing any measures;

c. ensure that:

(1) subject to clause 6. a., the Contractor Personnel do not process Personal Data except in accordance with the Contract (and in particular DEFFORM 532);

(2) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data by ensuring that they undertake the Government's Baseline Personnel Security Standard or other standard as specified in the Contract and ensure that they:

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

(b) 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 Authority or as otherwise permitted by the Contract; and

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

d. not transfer Personal Data outside of the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:

(1) the Authority or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or DPA 2018 Article 73) as determined by the Authority;

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

(3) 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 Authority in meeting its obligations); and

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

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

7. Subject to clause 6, the Contractor shall notify the Authority without undue delay if, in connection with Personal Data processed under the Contract, it:

a. receives a Data Subject Request (or purported Data Subject 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;

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.

8. The Contractor's obligation to notify under clause 7 shall include the provision of further information to the Authority in phases, as details become available.

9. Taking into account the nature of the processing, the Contractor shall provide the Authority with assistance, insofar as possible, in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 7 (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:

a. the Authority with full details and copies of the complaint, communication or request;

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

c. the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;

d. assistance as requested by the Authority following any Data Loss Event;

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

10. The Contractor shall maintain complete and accurate records and information as necessary to fulfil its obligations under clause 9.

11. The Contractor shall allow for audits of its Data Processing activity by the Authority or the Authority's designated auditor as required to demonstrate the Authority's compliance with its obligations as a Controller. Such audits will be conducted in accordance with general audit conditions contained in the Contract.

12. The Contractor shall designate a Data Protection Officer if required by the Data Protection Legislation.

13. Before allowing any Sub-processor to process any Personal Data related to the Contract, the Contractor must:

a. notify the Authority in writing of the intended Sub-processor and processing;

b. obtain the written consent of the Authority;

c. enter into a written Contract with the Sub-processor which give effect to the terms set out in this Condition such that they apply to the Sub-processor; and

d. provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.

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

15. The Contractor may, at any time on not less than 30 Working Days' notice, revise this Condition 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 the Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Authority may on not less than 30 Working Days' notice to the Contractor amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

17. Any Contract amendments resulting from clause 15 and/or 16 shall be conducted in accordance with any change control procedure as set out in the Contract.