UK Data Protection Act 2018 / EU GDPR: Project Framework

Introduction

To demonstrate an organisation's understanding of and commitment to full compliance with GDPR, one approach is to prepare a framework document to proactively communicate this information to both Data Subjects and customers. Each of the sections within this framework should be populated with organisation-specific content, and the italic text removed.

Be aware that some sections may require two different responses: one for situations where the organisation is acting a "Data Controller" for their own personal data and the other for situations where it is acting as a "Data Processor" and is undertaking data processing activities under the lawful instructions of another data controller.

Note: references to EU GDPR should also be read as being the equivalent clauses under the UK's Data Protection Act 2018, or other applicable national legislation for non-UK organisations, or for UK organisations providing services into other EU countries. "Art.xx" references are to the applicable articles as recorded within the EU General Data Protection Regulation 2016/679.

1. Principles of Personal Data Processing (Art.5)

Statements around the organisation's acknowledgement of and intention to ensure full compliance with the EU GDPR. Initial statements about lawfulness of processing, purposes of processing, retention of processing records, principles of data minimisation and the organisation's requirement to select "demonstrably compliant" data processors.

Commitment by the organisation to willingly assist and co-operate with its customers with meeting their own obligations under GDPR.

2. Data Protection by Design and by Default (Art.25)

Acknowledgment of the requirements of Article 25 where the processing of personal data is likely to pose a high risk to the rights or freedoms of a Data Subject. Make commitments to indicate that the organisation proactively seeks to identify and remove risks from its personal data processing activities and systems. Make reference to responses for DPIA (section 3), Security of Processing (section 6) and Records of Processing Activities (Art.30).

3. Data Protection Impact Assessments (Art.35)

To ensure that "Data Processing by Design and by Default" can be achieved, explain that the organisation conducts formal Data Protection Impact Assessments to identify and remove any risk associated with the data processing. Such records are required by the ICO, and would be reviewed during any investigation, e.g. following a data breach. Whilst there is no obligation to share publicly, if the organisation is seeking to be transparent with its customer/Data Subjects, these could be provided upon application to the Data Protection Officer (section 12).

4. Lawfulness of Processing (Art.6)

Referring to privacy notices and impact assessments, each personal data processing activity needs to satisfy at least one of the legal bases defined in Art.6. This is an opportune place to highlight which ones apply to the organisation:

- *Processing is carried out in accordance with the specific consent provided by the Data Subject*
- *Processing of personal data is necessary for the performance of a contract with the Data Subject*
- *Processing is necessary for compliance with legal obligations on the Data Controller*
- *Processing is necessary to protect the vital interests of the Data Subject*
- *Processing is necessary for tasks carried out in the public interest*
- *Processing is necessary for the legitimate interests of the Data Controller*

5. Security of Processing (Art.32)

Provide an overview of the range of technical and organisational controls which the organisation has implemented to deliver secure processing and remove risks to the personal data being processed. As an example, these might include:

- *Approach to risk management (e.g. that specified in Sections 6 & 8 of ISO27001:2013)*
- *Personnel security controls, competencies, validations, training*
- *Security controls which ensure the confidentiality/integrity/availability of personal data*
- *Resilience of processes and systems (e.g. BCP/DR plans, redundancies, failovers etc.)*
- *Technical controls including encryptions, pseudonymisation, anonymisation*
- *Security testing and evaluations (config checks, pen tests, CREST/CHECK tests etc.)*
- *Details of external validation activities, or compliance with an approved code of conduct*

6. Records of Processing Activities (Art.30)

For all the organisation's activities which process personal data:

- *Name and contact details of the Data Controller and DPO (if applicable, see section 12)*
- *Declared purposes of the processing of personal data*
- *Categories of Data Subjects and categories of personal data*
- *Categories of data recipients who may receive the personal data*
- *Details of any international data transfers (see section 7)*
- *Data retention periods and erasure methods*
- *Summary of technical and organisational controls*
- *Details of all data processing undertaking by processors*
- *Availability of such records to the supervisory authority on request (ICO)*

Note: unless there is a risk to the rights or freedoms of Data Subjects, the processing is not occasional, or the data includes special categories, organisations employing under 250 persons may be exempt from much of this section.

7. Personal Data Transfers to Third Countries (Art.44)

A summary of how the organisation intends to move personal data outside of the EU/EEA, if applicable, and including:

- *Details of transfers based on adequacy decisions (see Art.45)*
- *Details of transfers subject to appropriate safeguards (see Art.46)*
- *Details of transfers subject to binding corporate rules (see Art.47)*

8. Data Controller & Data Processor

Responsibilities of the Data Controller (Art.24)

Explain how the organisation undertakes data processing activities for which it is the Data Controller: e.g. for its own personnel, or for direct engagement with the public. Detail how the organisation selects its data processors (if applicable) to ensure that they are "demonstrably compliant" with GDPR. Include references to lawfulness and security of data processing (sections 4 and 5), Data Subject rights (section 9) and data breach management (section 10).

Responsibilities of the Data Processor (Art.28)

Explain how the organisation undertakes data processing activities where it is the Data Processor on behalf of another data controller (if applicable).

Provision and Adherence to Documented Processing Instructions (Art.29)

Provide details of how (i) as a Data Controller, the organisation issues lawful instructions to its "demonstrably compliant" data processors as to how they are authorised to process personal data, and (ii) as a Data Processor, how the organisation expects to receive formal written instructions from the data controller which specify how the processing of personal data is to be undertaken.

Authority to Use Sub-Processors (Art.28)

Details of which sub-processors may be involved with the Data Controller's proposed activities (in advance of a Data Subject's decision to use the service, if applicable). The need to seek Data Subject's/ Data Controller's approval (subject to context) for any changes to sub-processors once the data processing activity has commenced.

9. Data Subject Rights

Right of Access by Data Subjects (Art.15)

Designing and implementing a process by which a Data Subject can request details of any personal data that is being processed or stored by the organisation, including details of processing etc. The process needs to include validation of the individual's identity, fulfilment of the request within 30 days, and issuing a response.

Right to Rectification (Art.16)

Designing and implementing a process by which a Data Subject can request the correction or completion of personal data that is being processed or stored by the organisation. The process needs to include validation of the individual's identity, fulfilment of the request within 30 days, and issuing a confirmation.

Right to Erasure (Art.17)

Designing and implementing a process by which a Data Subject can request that their personal data is permanently deleted when it is no longer required (in specific circumstances). The process needs to include validation of the individual's identity, fulfilment of the request within 30 days, and issuing a confirmation.

Right to Restriction of Processing (Art.18)

Designing and implementing a process by which a Data Subject can request a restriction of the continued processing of their personal data, in specific circumstances. The process needs to include validation of the individual's identity, implementation of the restriction within 30 days, and issuing a confirmation.

Right to Object (Art.21)

Designing and implementing a process by which a Data Subject can object to the processing of their personal data for specific activities, including direct marketing and profiling. The process needs to include validation of the individual's identity, fulfilment of the request within 30 days, and issuing a confirmation.

Right to Data Portability (Art.20)

Designing and implementing a process by which a Data Subject can receive the personal data which they have provided to the Data Controller, in a commonly used and machine-readable format, and to have such data transmitted to another data controller where (a) the processing is based upon consent and (b) the processing is carried out by an automated means. The process needs to include validation of the individual's identity, fulfilment of the request within 30 days, and issuing a confirmation.

10. Data Breach Management

Notification to Supervisory Authority (ICO) (Art.33)

An explanation of how the organisation will monitor and detect data breaches (including loss, theft, compromise, unauthorised access etc) and the implementation of a process for the validation and reporting of the breach to the supervisory authority (ICO) within 72 hours of becoming aware of the breach.

Notification to Affected Data Subjects (Art.34)

Having detected a data breach, an explanation of how the organisation will notify affected Data Subjects. This will require a number of different approaches – perhaps individual contact for small numbers, or public announcements for breaches affecting significant numbers of Data Subjects.

11. Co-operation with Supervisory Authority (ICO) (Art.31)

A statement which confirms that the organisation will willingly co-operate with the supervisory authority (e.g. ICO in the UK) on all matters related to data protection tasks within GDPR.

P.S. – remember the ongoing registration/payment requirements as communicated by the ICO.

12. Data Protection Officer (Art.37-39)

Firstly, a determination of whether the organisation requires a Data Protection Officer as per the detailed requirements within Art.37 of GDPR:

- *Processing is carried out by a public authority or body*
- *Processing operations require regular monitoring of Data Subjects on large scale*
- *Processing uses large quantities of special categories of personal data (as per Art.9)*
- *Processing involves details of criminal convictions or records (as per Art.10)*

If not, then the organisation should consider which named role (not "DPO") should be used for interaction with Data Subjects etc.

If a DPO is required, an explanation of their function and role, and provide their contact details.

13. Glossary

To assist readers of this framework in understanding the foregoing sections, it is recommended that a short glossary of key terms and phrases is provided, including:

- *Adequacy Arrangements*
- *Anonymisation*
- *Binding Corporate Rules*
- *Children*
- *Codes of Conduct*
- *Consent*
- *Data Breach*
- *Data Controller*
- *Data Processing*
- *Data Processor*
- *Data Protection Impact Assessment (DPIA)*
- *Data Protection Officer (DPO)*
- *Data Subject*
- *Data Transfer*
- *EDPB*
- *EEA*
- *EU*
- *Fulfilment of a Contract*
- *ICO*
- *Joint Data Controllers*
- *Legitimate Interests*
- *Model Clauses*
- *Personal Data*
- *Privacy Notice/Policy*
- *Pseudonymisation*
- *Right of Access by Data Subjects*
- *Right to Data Portability*
- *Right to Erasure (Right to be Forgotten)*
- *Right to Object*
- *Right to Rectification*
- *Right to Restriction of Processing*
- *Sensitive Personal Data (Special Categories)*
- *Sub-Processor*
- *Subject Access Request*
- *Supervisory Authority*
- *Third Country*
- *Vital Interests of the Data Subject*

