Data Protection Policy

Reference: GDPR DOC 1.0
DocumentKits Issue No: 1.0
Organisation Issue No:
DocumentKits Issue Date: 15/11/2019
Organisation Issue Date:

1. Introduction

1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 Definitions used by the organisation (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

1.3 Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely

to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Policy statement

2.1 Board of Directors and management of Organisation Name, located at
Unit 1
Clive Court
Ely
Cambridgeshire
United Kingdom
CB7 4EA
are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Organisation Name collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.

2.3 The GDPR and this policy apply to all of Organisation Name's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation

processes from any source.

2.4 Organisation Name has established objectives for data protection and privacy, which are in PIMS and GDPR Objectives Record.

2.5 Data Protection Officer / GDPR Owner is responsible for reviewing the register of processing annually in the light of any changes to Organisation Name's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

2.6 This policy applies to all Employees/Staff

"and interested parties"

of Organisation Name such as outsourced suppliers. Any breach of the GDPR or this PIMS will be dealt with under Organisation Name's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.7 Partners and any third parties working with or for Organisation Name, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Organisation Name without having first entered into a data confidentiality agreement
"document reference,"

which imposes on the third party obligations no less onerous than those to which Organisation Name is committed, and which gives Organisation Name the right to audit compliance with the agreement.

Personal Information Management System (PIMS)

Policy statement

To support compliance with the GDPR, the Board of Directors has approved and supported the development, implementation, maintenance and continual improvement of a documented personal information management system ('PIMS') for Organisation Name.

All Employees/Staff of Organisation Name

"and certain external parties identified in the PIMS"

are expected to comply with this policy and with the PIMS that implements this policy. All Employees/Staff, and certain external parties, will receive
"be required to provide"

appropriate training. The consequences of breaching this policy are set out in Organisation Name's disciplinary policy and in contracts and agreements with third parties.

In determining its scope for compliance with BS 10012:2017 and the GDPR, Organisation Name considers:

- any external and internal issues that are relevant to the purpose of Organisation Name and that affect its ability to achieve the intended outcomes of its PIMS;
- specific needs and expectations of interested parties that are relevant to the implementation of the PIMS;
- organisational objectives and obligations;
- the organisations acceptable level of risk; and
- any applicable statutory, regulatory or contractual obligations.

The PIMS Scope Statement is documented here.

Organisation Name's objectives for compliance with the GDPR and a PIMS:

- are consistent with this policy
- are measurable
- take into account GDPR

"and BS 10012:2017 privacy requirements"

- and the results from risk assessments and risk treatments
- are monitored (in line with the Monitoring, Measurement, Analysis, Evaluation Procedure)
- are communicated (in line with the Communications Procedure)
- are updated as appropriate (in line with the Continual Improvement Procedure)

Organisation Name documents those objectives in the PIMS and GDPR Objectives Record.

In order to achieve these objectives, Organisation Name has determined:

- what will be done
- what resources will be required
- who will be responsible
- when it will be completed
- how the results will be evaluated

3. Responsibilities and roles under the General Data Protection Regulation

3.1 Organisation Name is a

"data controller and/or data processor"

under the GDPR.

3.2 Top Management and all those in managerial or supervisory roles throughout Organisation Name are responsible for developing and encouraging good information handling practices within Organisation Name; responsibilities are set out in individual job descriptions.

3.3 Data Protection Officer / GDPR Owner (Data Protection Officer Job Description and Data Protection Job Description Responsibilities), a role specified in the GDPR, should be a member of the senior management team, is accountable to Board of Directors of Organisation Name for the management of personal data within Organisation Name and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1 development and implementation of the GDPR as required by this policy; and
3.3.2 security and risk management in relation to compliance with the policy.

3.4 Data Protection Officer, who Board of Directors considers to be suitably qualified and experienced, has been appointed to take responsibility for Organisation Name's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Organisation Name complies with the GDPR, as do Manager/Executive (generic/line)'s in respect of data processing that takes place within

their area of responsibility.

3.5 The Data Protection Officer / GDPR Owner have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

3.6 Compliance with data protection legislation is the responsibility of all Employees/Staff of Organisation Name who process personal data.

3.7 Organisation Name's Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of Organisation Name generally.

3.8 Employees/Staff of Organisation Name are responsible for ensuring that any personal data about them and supplied by them to Organisation Name is accurate and up-to-date.

<<Sections 4 – 10 removed for sample purposes>>

11. Information asset register/data inventory

11.1 Organisation Name has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. Organisation Name's data inventory and data flow determines (Data Protection Impact Assessment Procedure, and Data Protection Impact Assessment (DPIA) Tool):

- business processes that use personal data;
- source of personal data;
    - volume of data subjects;
    - description of each item of personal data;
    - processing activity;
    - maintains the inventory of data categories of personal data processed;
    - documents the purpose(s) for which each category of personal data is used;
    - recipients, and potential recipients, of the personal data;
    - the role of the Organisation Name throughout the data flow;
    - key systems and repositories;
    - any data transfers; and
    - all retention and disposal requirements.

11.2 Organisation Name is aware of any risks associated with the processing of particular types of personal data.

11.2.1 Organisation Name assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) (Data Protection Impact Assessment Procedure and Data Protection Impact Assessment (DPIA) Tool) are carried out in relation to the processing of personal data by Organisation Name, and in relation to processing undertaken by other organisations on behalf of Organisation Name.

11.2.2 Organisation Name shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Organisation Name shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.2.4 Where, as a result of a DPIA it is clear that Organisation Name is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Organisation Name may proceed must be escalated for review to the Data Protection Officer / GDPR Owner.

11.2.5 The Data Protection Officer / GDPR Owner shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

11.2.6 Appropriate controls will be selected

"from Annex A of ISO 27001, ISO 27017, ISO 27018, etc., as appropriate"

and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Organisation Name's documented risk acceptance criteria and the requirements of the GDPR.

Document Owner and Approval

The Data Protection Officer / GDPR Owner is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) – electronic and physical – where this document is available"

Its approval status can be viewed in Master List of Document Approval.