THE OFFICE OF THE
Data Protection Authority

The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the **Law**")

Explanatory Information for Self-Assessment Questionnaire Controllers

---

This document provides additional information to assist in completing the controllers' self-assessment questionnaire.

Table of Contents

March 2020

Note 1 - Personal data

Personal data is information that relates to an identified or identifiable living individuals, i.e. their personal information. Personal data includes both facts and opinions about the individual, as well as information regarding the intentions of the data controller towards the individual.

Personal data encompasses information that is processed electronically, information that is initially processed in hard copy form with an intention to process it electronically and manual records held in a filing system defined as "any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis".

Note 2 - European Union (EU) Countries

The following are EU countries :-

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden

Note 3 - Special Category Data

The Law replaced the concept of **sensitive personal data** with **special category data**.

Special Category Data	Sensitive Personal Data
Racial or ethnic origin Political opinion Religious or philosophical belief Trade union membership Health data Data concerning an individual's sex life or sexual orientation Genetic data* Biometric data* Criminal data	Racial or ethnic origin Political opinions Religious or other beliefs Trade union membership Physical or mental health or condition Sexual life Offences or alleged offences Criminal proceedings

* where used to uniquely identify a natural person

Note 4 - Data Collection Notices

The following must be given to individuals at time of data collection :-

- Identity and contact details of the controller and representative (where applicable)
- Contact details of the data protection officer (where applicable)
- Whether any special category data are being processed
- Details of the source of the data
- The purposes and legal basis of the processing
- Details of legitimate interests where that is relied upon
- Recipients or categories of recipients
- Details of transfers to authorised jurisdictions not in the EU and relevant safeguards
- Details of any transfers to unauthorised jurisdictions and relevant safeguards
- Details of retention period for the data or the criteria used to determine retention period
- The existence of each data subject right
- Where consent is relied upon, details of the right to withdraw consent
- The right of complaint to the data protection regulator
- Information about the logic where decisions are based on automated processing
- Whether the provision of the personal data is part of a statutory or contractual requirement and possible consequences of failing to provide the personal data

Note 5 - Conditions for Processing to be Lawful – Schedule 2

Please view the conditions for lawful processing guidance note on our website.

Note 6 - Consent

Under the Law consent has been redefined. The new standard for consent includes the following :-

- Controllers must be able to show consent was given
- Consent must be
    - Freely given
    - Specific
    - Informed
    - Unambiguous
- It has to be a positive indication of agreement

Consent as the lawful processing condition provides the individual with stronger rights, including the right to withdraw that consent at any time.

Note 7 - Data Protection Officers (DPOs)

The Law created a legal requirement for certain organisations to have a Data Protection Officer and lays down set tasks for that DPO.

The organisations that will require DPOs are :

- Public authorities (except for courts acting in their judicial capacity)
- Controllers or processors whose **core activities** require the regular and systematic monitoring of data subjects on a **large scale**
- Controllers or processors whose core activities consist of processing on a **large scale** of special category data and/or personal data relating to criminal convictions and offences.

Recital 97 of the General Data Protection Regulation (GDPR) specifies that the **core activities** of a controller relate to 'primary activities and do not relate to the processing of personal data as ancillary activities'. 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals. Article 29 Working Party guidance goes on to say that whilst all organisations carry out certain activities, for example paying their employees or having standard IT support activities these are examples of support functions; activities that support the core activity. Whilst it is true to say that these activities are necessary or essential they are not the core activity, but rather ancillary functions.

Please see our guidance note on large scale processing for more information.

Note 8 - Transfer

A transfer occurs where data is moved from one jurisdiction to another where it is held, stored or acted upon. It is not the same as transit, where data simply passes through a country on its way to another jurisdiction.

Transfer frequently takes the form of the movement of data electronically but data would also be transferred where it was collected on paper and sent overseas to be processed electronically or stored in a relevant filing system. Putting personal data on a web site may involve transfers to the other countries in which the web site is accessed.

Note 9 - European Economic Area (EEA) Countries & 'Adequate' Jurisdictions

The European Economic Area comprises EU Member States (as follows) :-

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden

Plus Iceland, Liechtenstein and Norway

Jurisdictions with 'adequacy' for the purposes of the Directive 95/46/EC :-

- Andorra
- Argentina
- Canada (restricted)
- Faeroe Islands
- Guernsey
- Isle of Man
- Israel
- Japan (private sector)
- Jersey
- New Zealand
- Switzerland
- Uruguay
- US Privacy Shield

The adequacy of each jurisdiction will be reassessed in accordance with the GDPR although it is unclear at this time when this will take place. As such, the list of adequate jurisdictions may change.

The United Kingdom is deemed an authorised jurisdiction for data transfers under the Law until 31 December 2020.
