THE OFFICE OF THE
Data Protection Authority

The Data Protection (Bailiwick of Guernsey) Law, 2017

Self-Assessment Questionnaire
Processors

Using this Questionnaire

1. In order to provide a practical starting point for organisations, the Commissioner has compiled this questionnaire to assist in working towards compliance under the Law. This questionnaire contains a number of questions that senior management and directors of organisations can use to assess the basic level of compliance that currently exists within that organisation and to highlight those areas which are likely to require attention. It is also a starting point for the record of processing activities that processors are required to hold under the Law. **It is for your internal use only.**

2. The document is protected so you will only be able to add, edit and delete text in the space given for answers.

3. Additional information to support some of the questions in this document can be found in the Processors' Self-Assessment Notes.

THIS DOCUMENT IS PURELY FOR GUIDANCE AND DOES NOT CONSTITUTE LEGAL ADVICE OR LEGAL ANALYSIS. IT IS INTENDED AS A STARTING POINT ONLY, AND ORGANISATIONS MAY NEED TO SEEK INDEPENDENT LEGAL ADVICE WHEN REVIEWING, ENHANCING OR DEVELOPING THEIR OWN PROCESSES AND PROCEDURES OR FOR SPECIFIC LEGAL ISSUES AND/OR QUESTIONS.

SA-2	Data Protection - Processors SELF-ASSESSMENT QUESTIONNAIRE		
Name of Organisation			
Registration Number(s) (if registered)			
Department			
Contact Name			
Products and/or services provided			
Number of sites/ locations to be covered			
Number of full-time staff		**Number of part-time staff**	
Name of Data Protection Officer (if any)		**Number of sub-contractors**	
Date questionnaire completed		**Completed by**	

Table of Contents

A DATA COLLECTION

Question 1	What personal data are processed? (e.g. name, address, telephone number etc.)
Question 2	Why are these personal data processed? For what purpose/purposes are they used?
Question 3	Within the Law, the term "special category data" replaces the existing term "sensitive personal data". It also encompasses more data types than the previousdefinition. *(See Note 2 in the Processors' Self-Assessment Notes for more information on "sensitive personal data" and "special category" data)* With the expanded definition in mind, is any special category data held or processed (e.g. medical/health data, ethnic origin etc.)? If so, for what purpose?

B GOVERNANCE

Question 4	Do you have a Data Protection Officer?
Question 5	If so, to whom does the Data Protection Officer report?
Question 6	What responsibilities does the Data Protection Officer have?
Question 7	If you do not currently have a Data Protection Officer, are you planning to appoint someone?
Some organisations are mandated to have a Data Protection Officer. ***(See Note 3 in the Processors' Self-Assessment Notes for more information as to whether your organisation require a Data Protection Officer)***	
Question 8	Are written agreements in place between your organisation and the controller that outline how personal data should be processed?
If no, you must now ensure that they are put in place in order to meet the requirements of the Law although it falls to the controller to ensure a contract is in place and the controller would be at fault if there was not. **If yes, each agreement will require review against the new requirements within the Law. Processors became accountable and liable under the Law and as such you may require extra information and direction from the controller to ensure you are compliant.**	
Question 9	Is a central record of processing activities maintained in a format that can be used to demonstrate processing activities to the controller?

The Law requires organisations to hold records of their processing activities, including the categories of processing and details of any transfers of data outside the Bailiwick.
Question 10 If yes, how often is this reviewed and updated?

C STORAGE AND ARCHIVING

Question 11	How does your organisation store personal data on behalf of a controller? (e.g. on computer or manual files or both and/or on personal devices?) Set out details of all databases/filing systems containing personal data.
Question 12	If personal data is stored on computer is this located within the organisation or elsewhere? If elsewhere, identify the third party storing the data, detailing where and how the data are stored.
If the personal data is being held by a third party, the third party is acting as a sub-processor. Ensure you complete the Using Sub-Processors section of this self-assessment to assess this relationship.	
Question 13	If personal data is stored manually is this within the organisation or elsewhere? If elsewhere, identify the third party (sub-processor) storing the data, detailing where and how the data are stored.
If the personal data is being held by a third party, the third party is acting as a sub-processor. Ensure you complete the Using Sub-Processors section of this self-assessment to assess this relationship.	
Question 14	If your organisation processes special category data on behalf of a controller, is such data stored separately from any other personal data or subject to any specific marking, security or handling rules/restrictions?
Question 15	In what format or in what medium is the archived data stored?

Question 16	Where is the archived data stored? If it is stored on third party premises, identify that third party and where and how it is stored?
If the data is being held by a third party, the third party is acting as a sub-processor. Ensure you complete the Using Sub-Processors section of this self-assessment to assess this relationship.	

D SECURITY

Question 17	Describe in outline the security procedures in operation in your organisation to keep all personal data processed on behalf of a controller secure. Describe the physical, administrative and technological procedures used and any specific requirements each controller may have.
Question 18	Who has access to personal data within the organisation/outside the organisation?
Question 19	Who controls and authorises such access?
Question 20	Do you have policies and procedures in place for detecting and dealing with breaches? If so, what are they?
Question 21	How do you check that there has been no internal unauthorised access to personal data? What data audit facilities/mechanisms are in place?
Question 22	Do you have policies and procedures in place for reporting breaches to the controller? If so, what are they?
Under the Law, data breaches need to be reported to the Commissioner's Office within 72 hours of discovery by the controller. Processors need to ensure they communicate any breaches or compromises of data to the controller as soon as possible.	

E DESTRUCTION OF DATA AND TERMINATION OF CONTRACT

Question 23	Under the contract with the controller, are you responsible for the destruction of the personal data?
Question 24	How is personal data destroyed?
Question 25	Who authorises destruction? Who carries out destruction? What agreements are in place with contractors who provide shredding etc. facilities/services?
Question 26	Are there clear instructions in the contract detailing what happens to the personal data at the end of the contract period?

F USING SUB-PROCESSORS

Question 27	Are any of your personal data processing activities carried out by third parties (sub-processors)? List them and describe the processes and location of the provider and the data.
Question 28	Who authorises these processing activities?
The Law states that a processor shall not engage the services of another processor as a sub-processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.	
Question 29	Are written agreements in place covering these arrangements?
Each agreement will require review against the requirements within the Law. Processors became accountable and liable under the Law and as such may require extra information or assistance from controllers to ensure they are compliant. **Processors engaging the services of a sub-processor will also need to ensure that sufficient guarantees of compliance are given by the sub-processor. In the event of a breach or data compromise, should the services of a sub-processor have been contracted by a processor, the processor will hold liability for this.**	
Question 30	Outline the security measures under which each sub-processor must operate
Question 31	Do the sub-processors used by your organisation use any other organisation to perform that service on their behalf? If so, list the organisation and any written arrangements in place with regards to the service these sub-contractors offer.

Under the Law if a processor employs another processor to perform a service on behalf of a controller they should obtain either specific or general written authorisation. The processor with which the controller has its agreement remains liable for the actions of any processor to which it sub-contracts.

G TRANSFERS OF PERSONAL DATA

Question 32	Do you transfer data a. cross-departmentally; and/or b. to third parties outside the organisation? *(See Note 4 in the Processors' Self-Assessment Notes for a definition of Transfer)*
Question 33	How is data transferred? (e.g. Encrypted email? Secure fax?)
Question 34	In what countries are those people to whom you disclose the information (whether inside the organisation or external) located?
Question 35	Where personal data is transferred outside the EEA, what measures are used to ensure compliance with the Law (Part X)? *(See Note 5 in the Processors' Self-Assessment Notes for a list EEA countries and adequate countries)*

H TRAINING

Question 36	Do the employees in your organisation receive training on data protection and other relevant law? If so, please describe the nature of the training given, when it is given and identify who is responsible for carrying out the training.
Question 37	Are refresher courses held? If so, please describe the nature of the training given, when it is given, identify who is responsible for carrying out the training and who is directed to attend.
Question 38	Are staff aware that unlawful access to and/or disclosure of personal data is prohibited?
Question 39	Have the following attended a data protection awareness session? a. The Board b. Senior management c. Security/IT team d. All other staff