



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.**

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

### Table of Contents

<b>A</b>	<b>DATA COLLECTION</b> .....	<b>3</b>
<b>B</b>	<b>GOVERNANCE</b> .....	<b>4</b>
<b>C</b>	<b>STORAGE AND ARCHIVING</b> .....	<b>6</b>
<b>D</b>	<b>SECURITY</b> .....	<b>8</b>
<b>E</b>	<b>DESTRUCTION OF DATA AND TERMINATION OF CONTRACT</b> .....	<b>9</b>
<b>F</b>	<b>USING SUB-PROCESSORS</b> .....	<b>10</b>
<b>G</b>	<b>TRANSFERS OF PERSONAL DATA</b> .....	<b>12</b>
<b>H</b>	<b>TRAINING</b> .....	<b>13</b>

## A DATA COLLECTION

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

## B GOVERNANCE

<b>Question 4</b>	Do you have a Data Protection Officer?
<b>Question 5</b>	If so, to whom does the Data Protection Officer report?
<b>Question 6</b>	What responsibilities does the Data Protection Officer have?
<b>Question 7</b>	If you do not currently have a Data Protection Officer, are you planning to appoint someone?
<p><i>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)</i></p>	
<b>Question 8</b>	Are written agreements in place between your organisation and the controller that outline how personal data should be processed?
<p><b>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.</b></p> <p><b>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.</b></p>	
<b>Question 9</b>	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

<b>Question 11</b>	<p>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?)</p> <p>Set out details of all databases/filing systems containing personal data.</p>
<b>Question 12</b>	<p>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.</p>
<p><b>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.</b></p>	
<b>Question 13</b>	<p>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.</p>
<p><b>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.</b></p>	
<b>Question 14</b>	<p>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?</p>
<b>Question 15</b>	<p>In what format or in what medium is the archived data stored?</p>

**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

<b>Question 17</b>	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.
<b>Question 18</b>	Who has access to personal data within the organisation/outside the organisation?
<b>Question 19</b>	Who controls and authorises such access?
<b>Question 20</b>	Do you have policies and procedures in place for detecting and dealing with breaches? If so, what are they?
<b>Question 21</b>	How do you check that there has been no internal unauthorised access to personal data? What data audit facilities/mechanisms are in place?
<b>Question 22</b>	Do you have policies and procedures in place for reporting breaches to the controller? If so, what are they?
<p><b>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.</b></p>	

## **E      DESTRUCTION OF DATA AND TERMINATION OF CONTRACT**

<b>Question 23</b>	Under the contract with the controller, are you responsible for the destruction of the personal data?
<b>Question 24</b>	How is personal data destroyed?
<b>Question 25</b>	Who authorises destruction? Who carries out destruction? What agreements are in place with contractors who provide shredding etc. facilities/services?
<b>Question 26</b>	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

<b>Question 27</b>	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.
<b>Question 28</b>	Who authorises these processing activities?
<p><b>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.</b></p>	
<b>Question 29</b>	Are written agreements in place covering these arrangements?
<p><b>Each agreement will require review against the requirements within the Law. Processors become accountable and liable under the Law and as such may require extra information or assistance from controllers to ensure they are compliant.</b></p> <p><b>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.</b></p>	
<b>Question 30</b>	Outline the security measures under which each sub-processor must operate
<b>Question 31</b>	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**

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

## 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