THE OFFICE OF THE
Data Protection Authority

The Data Protection (Bailiwick of Guernsey) Law, 2017

Self-Assessment Questionnaire
Controllers

Using this Questionnaire

1. In order to provide a practical starting point for organisations, the Commissioner has compiled this questionnaire to assist in 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 controllers 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 Controllers' 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-1	Data Protection - Controllers 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 INTRODUCTION

Question 1	Does your organisation process personal data on individuals? This can be staff as well as clients and other people. *(See Note 1 in the Controllers' Self-Assessment Notes for the definition of personal data)*
If no, unless you intend to process personal data in the future, data protection legislation does not apply so you can stop this self-assessment now. **If yes, please continue onto Question 2.**	
Question 2	Does your organisation process data on behalf of another, for which the other organisation remains the controller?
If yes, your organisation is a processor. There is a separate self-assessment questionnaire for the activities of a processor as, under the Law, processors became accountable and liable for their action. It is recommended that both questionnaires are completed. **This self-assessment should be completed for the personal data your organisation processes for which it is the controller.**	

B DATA COLLECTION

Question 3	What personal data are collected? (e.g. name, address, telephone number etc.)
Question 4	Why are these personal data held? For what purpose/purposes are they used?
Question 5	Within the Law, the term "special category data" has replaced the previous term "sensitive personal data". It also encompasses more data types. *(See Note 3 in the Controllers' 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?
Question 6	How is personal data collected? (e.g. face to face, telephone call, email, web form etc.)
Question 7	Who is this personal data collected from? (e.g. individuals themselves, third parties, intermediaries)
Question 8	a. What form of notice (privacy notice/data collection statement) is given to individuals when the information is collected? It may be helpful to **attach** copies to this form. b. How often is each notice reviewed or changed? c. Who reviews or changes each notice?

Under the Law, data collection notices need to be more extensive with full detail provided to individuals at the time of collection. ***(See Note 4 in the Controllers' Self-Assessment Notes for more information on data collection notices)***	
Question 9	For each purpose outlined in Question 5, determine which of the lawful processing conditions is relied upon for the collection and processing of the relevant personal data? *(See Note 5 in the Controllers' Self-Assessment Notes for the lawful processing conditions)*
Question 10	Where consent is relied upon, is there sufficient clarity for the individual to know what has been consented to?
Under the Law consent is redefined ***(See Note 6 in the Controllers' Self-Assessment Notes for the new definition of consent)*** **and organisations must be able to demonstrate consent has been provided. If the consent currently obtained for processing meets the new standard, that consent remains valid. Where it falls below the new standard such consent will cease to be applicable and either another lawful processing condition should be used or the consent reobtained in a manner that meets the new standard.**	

C GOVERNANCE

Question 11	Do you have a Data Protection Officer?
Question 12	If so, to whom does the Data Protection Officer report?
Question 13	What responsibilities does the Data Protection Officer have?
Question 14	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 7 in the Controllers' Self-Assessment Notes for more information as to whether your organisation requires a Data Protection Officer)***	
Question 15	Is a central record of processing activities maintained, in which the lawful processing conditions and fair processing elements are clearly identified?
The Law requires organisations to hold records of their processing activities, including details of the lawful processing conditions being relied upon and the fair processing measures.	
Question 16	If yes, how often and by whom is this reviewed and updated?

D DATA QUALITY

Question 17	Who in your organisation has responsibility for reviewing personal data for relevance and accuracy and keeping personal data up to date?
Question 18	How often are these activities carried out?
Question 19	Who has the authority to alter, add or delete personal data?

E STORAGE AND ARCHIVING

Question 20	How does your organisation store personal data? (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 21	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 your personal data is being held by a third party the third party is acting as a processor. Ensure you complete the Using Processors section of this self-assessment to assess this relationship.	
Question 22	If personal data is stored manually 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 your personal data is being held by a third party the third party is acting as a processor. Ensure you complete the Using Processors section of this self-assessment to assess this relationship.	
Question 23	If your organisation processes special category data, is such data stored separately from any other personal data or subject to any specific marking, security or handling rules/restrictions?
Question 24	Does your organisation archive files, i.e. move data from live systems into longer-term storage?

Data protection requirements do not cease when personal data is archived. The data protection principles and other compliance obligations must still be complied with.	
Question 25	What are the archiving policies and procedures in operation in your organisation?
Question 26	Who authorises archiving?
Question 27	In what format or in what medium/media is the archived data stored?
Question 28	Where is the archived personal data stored? If it is stored on third party premises, identify that third party and where and how it is stored.
If your personal data is being held by a third party the third party is acting as a processor. Ensure you complete the Using Processors section of this self-assessment to assess this relationship.	

F SECURITY

Question 29	Describe in outline the security procedures in operation in your organisation to keep your personal data secure. Describe any physical, administrative, technological or other procedures used.
Question 30	Who has access to personal data within the organisation/outside the organisation?
Question 31	Who authorises and controls such access?
Question 32	Do you have policies and procedures in place for detecting and dealing with breaches? If so, what are they?
Question 33	How do you check that there has been no internal unauthorised access to personal data? What personal data audit facilities/mechanisms are in place?
Question 34	Do you have policies and procedures in place for reporting breaches to: a. Your Board (or equivalent) b. The Commissioner; and c. the individual whose data has been breached (data subject)? If so, what are they?

Under the Law, personal data breaches need to be reported to the ODPA within 72 hours of discovery. Furthermore, where there exists a high risk to the rights and freedoms of any individual whose personal data have been compromised, the organisation must take steps to let those individuals know. Organisations need to be clear how they will achieve this and should have processes in place to fulfil these requirements. Further information can be found here.

G DESTRUCTION

Question 35	How long is personal data kept before being destroyed? Attach your retention schedule.
Question 36	How is personal data destroyed?
Question 37	Who authorises destruction? Who carries out destruction? What agreements are in place with contractors (processors) who provide shredding etc. facilities/services?
If your data is being held by a third party the third party is acting as a processor. Ensure you complete the Using Processors section of this self-assessment to assess this relationship.	

H USING PROCESSORS

Question 38	Are any of your personal data processing activities carried out by third parties (processors)? List them and describe the processes and location of the provider and the personal data.
Question 39	Who authorises these processing activities?
Question 40	Are written agreements in place covering these arrangements including the new data breach requirements?
If no, you must now ensure they are put in place in order to meet the requirements of the Law. **If yes, each agreement will require review against the new requirements within the Law. Processors are accountable and liable under the Law and as such may require extra information and direction from your organisation to ensure they are compliant.**	
Question 41	Outline the security measures under which each processor must operate
Question 42	Do the 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 to your organisation they need to have already obtained either specific or general written authorisation from your organisation. The processor with which your organisation has its agreement remains liable for the actions of any processor to which it sub-contracts.

I TRANSFERS OF PERSONAL DATA

Question 43	Do you transfer personal data a. cross-departmentally; and/or b. to third parties outside the organisation *(See Note 8 in the Controllers' Self-Assessment Notes for a definition of Transfer)*
Question 44	How is personal data transferred? (e.g. Encrypted email? Secure fax?)
Question 45	In what countries are those people to whom you disclose the information (whether inside the organisation or external) located?
Question 46	Where personal data is transferred outside the EEA, what measures are used to ensure compliance with the Law (Part X)? *(See Note 9 in the Controllers' Self-Assessment Notes for a list EEA countries and adequate countries)*
Similar provisions for transfers exist within Part X of the Law as those previously available under the eighth data protection principle. However, time should be taken to ensure your organisation is aware of the protection measures it uses for each type of data transfer and to determine if it is still appropriately protected.	

J DISCLOSURES TO THIRD PARTIES

Regular Data Sharing **Sharing that happens with some level of frequency and a pre-determined approach**	
Question 47	Does your organisation disclose any personal data to third parties on a regular basis? List the instances where this happens.
Question 48	For each of these instances, is there a data sharing agreement or similar document that governs the regular disclosure?
Question 49	If there are no data sharing agreements or similar, are there policies and procedures in place that explain how the sharing should be handled and which clearly set out respective obligations?
Question 50	Are individuals made aware that their personal data may be disclosed as part of regular data sharing? If not, which exemption is used to remove the need to make the individual aware?
If you do not inform an individual that their personal data may be disclosed on connection with a third party request (without a valid exemption removing this requirement) this may constitute unfair processing and be a breach of the first data protection principle. ***(See Note 4 in the Controllers' Self-Assessment Notes for more information on data collection notices)***	
Question 51	Which lawful processing condition from Schedule 2 of the Law may be relied upon for each instance of regular data sharing? *(See Note 5 in the Controllers' Self-Assessment Notes for lists of the lawful processing conditions)*

To share personal data it must be possible to identify which of the lawful processing conditions are relied on. To share without such a condition may constitute unlawful processing.

Non-Routine Data Sharing **Sharing that happens as a 'one off' and is often unforeseen or unprepared for**	
Question 52	Do you receive non-routine requests from third parties seeking data regarding individuals whether employees, clients or other individuals?
Question 53	How are non-routine requests handled and responded to? This should include a record of the decision making process.
Question 54	Is there a legislative basis cited by any of these third parties seeking information on a non-routine basis? If so, what is the legislative basis?
Question 55	Are there any procedural guidelines (internal or otherwise) to assist in dealing with non-routine requests from third parties?
Question 56	Are individuals made aware that their personal data may be disclosed in response to a non-routine request from a third party? If so, how are they made aware? If not, which exemption is used to remove the need to make the individual aware?

Not informing an individual that their personal data may be disclosed in connection with a third party request (without a valid exemption removing this requirement) may constitute unfair processing. ***(See Note 4 in the Controllers' Self-Assessment Notes for more information on data collection notices)***	
Question 57	Which lawful processing condition from Schedule 2 of the Law is proposed to be used for any disclosure of personal data in response to a non-routine request? *(See Note 5 in the Controllers' Self-Assessment Notes for lists of the lawful processing conditions)*
In order to share personal data it must be possible to identify which of the lawful processing conditions are relied on.	

K SUBJECT ACCESS PROCEDURES AND DATA SUBJECTS' RIGHTS

Question 58	What policies and procedures are in place within your organisation for responding to subject access requests? Who is your point of contact for such requests?
Question 59	What policies and procedures exist in your organisation for suppression, blocking or correction of personal data?
Question 60	Who authorises/oversees these activities?
Question 61	Are individuals able to amend/delete their own personal data?
Question 62	Are any decisions about individuals made by purely automated means, in other words by a computer without any human intervention?
Under the Law individuals' rights in relation to automated decision making, including profiling, are strengthened and so where such processing is undertaken by your organisation time should be taken to review this process and make sure it is compliant with the requirements of the Law.	

L TRAINING

Question 63	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 64	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 65	Are staff aware that unlawful access to and/or disclosure of personal data is prohibited?
Question 66	Have the following attended a data protection awareness session? a. The Board b. Senior management c. Security/IT team d. All other staff