JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

GUIDANCE NOTE

Duties of Data Controllers

Data Protection (Jersey) Law 2018

MAY 2018 • V1 • WWW.JERSEYOIC.ORG

CONTENTS

Introduction 3

Overview 4

General duties of Data Controllers 5

More information 9

INTRODUCTION

1. The Data Protection (Jersey) Law 2018 (**DPJL**) is based around six principles of 'good information handling'. These principles give people (the data subjects) specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

2. An overview to the main provisions of the DPJL can be found in the [**Guide to Data Protection**] (the **Guide**).

3. This is part of a series of guidance, which goes into more detail than the Guide, to help organisations fully understand their obligations, as well as to promote good practice.

4. This guidance relates only to the DPJL.

OVERVIEW

- This guidance applies to data controllers, as defined under Art.1 of the DPJL.
- Data controllers are subject to a number of statutory duties under the DPJL. This guidance sets out those general duties as part of an overall principle of accountability.

GENERAL DUTIES OF DATA CONTROLLERS

6. Art.1 of the DPJL defines a controller as:

   "the natural or legal person, public authority, agency or other body that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, and where those purposes and means are determined by the relevant law, the controller or the specific criteria for its nomination may be provided by law".

7. Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.

8. The term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other.

9. Art.6(1) of the DPJL, places specific obligations on data controllers as follows in that a data controller:
   a. is responsible for, and must be able to demonstrate compliance with, the data protection principles in the manner provided for in this Law;

      This means that a data controller based in Jersey must be able to show what steps they have taken to comply with the Data Protection Principles. This will include, but is not limited to, the development and implementation of policies and procedures in relation to all aspects of data handling. For example, this might include:

      - policies and procedures to ensure data security and confidentiality;
      - subject access policy and procedures;
      - policies on the use of CCTV equipment;
      - privacy policies and fair processing statements;
      - retention and destruction policies;

   b. if established in Jersey, may process personal data or cause it to be processed only if the controller is registered under Article 17 of the Data Protection Authority (Jersey) Law 2018 (the Authority Law);

      The DPJL requires all Jersey-based data controllers to register with the Commissioner. Whilst there may be an exemption available to data controllers in terms of paying registration fees, this does not preclude data controllers from the requirement to register.

c. must pay such charges to the Authority as Regulations under Article 18 of the Authority Law may prescribe;

The Authority will move to a risk-based, tiered model of registration, which means that whilst some lower risk data controllers will continue to pay a nominal fee per year, data controllers processing higher risk personal data will be required to pay a much higher fee dependent upon which tier they are assessed as falling within.

d. in planning and implementing the processing of personal data, must ensure that appropriate safeguards for the rights of data subjects are put in place by design and by default in accordance with Article 15 of the DPJL;

This means data controllers will need to think carefully about how they intend to process personal information. In particular, data controllers will need to consider and demonstrate both the technical and organisational measures they have implemented to ensure their means of processing personal information operate in a privacy-friendly way, safeguards the rights of data subjects and meets compliance with the data protection principles.

Such measures will need to take account of the technology available, cost, risks to the individual. Thought will need to be given to the nature and scope of the data processing, who may have access to the data, the purpose for which it is to be processed and the length of time the information will be kept for. Data controllers may also wish to explore the possibility of certification (once available) in order to evidence their compliance with Article 15.

e. must comply with the record-keeping requirements and disclose the records covered by those requirements on request to the Authority;

Article 14 of the DPJL requires data controllers to maintain a written record of its processing activities. In broad terms, these records should include, but are not limited to, the following:

- Name and contact details of the data controller;
- Details of any joint data controller (with whom personal data are shared for a common purpose);
- Details of any representative of the data controller;
- Details of the Data Protection Officer (if appointed);
- The purposes of the data processing;
- A description of the categories of data subjects and personal data processed;
- A description of to whom the data controller intends to disclose personal data;
- Details of any third countries or international organisations to which personal data will be transferred;
- Details of the safeguards in place with those third countries or international organisations to protect the data;
- Details of the envisaged retention periods for the different categories of personal data;
- A general description of the security measures (both technical and organisational) in place to protect the data.

[1] Not all such exemptions apply to public authorities. Public Authorities should check the DPJL.

The record keeping requirements do not apply in the case of organizations with fewer than 250 employees unless the processing –

i. is likely to result in a risk to the rights and freedoms of data subjects;
ii. is not occasional; or
iii. includes special category data or relates to criminal convictions or related security measures.

f. where a processor is appointed, must appoint a processor only in accordance with Article 19;

This means that a data controller can outsource business activities to another organisation to act on their behalf (known as a data processor), but must only use data processors who provide sufficient guarantees to implement appropriate technical and organisational measures that meet compliance with the DPJL and protect the rights of the data subject.

The data controller is also responsible for ensuring that a robust processing contract or other legally binding instrument is in place with the data processor. This may include setting out the following:

» The duration of the processing;
» The nature and purpose of the processing;
» The type of personal data to be processed;
» The categories of data subjects affected;
» The obligations and rights of the data controller

In addition, the contract must stipulate that the data processor:

» Only acts on the instructions of the data controller;
» Ensures that only authorised persons process the personal data, and in accordance with robust confidentiality agreements;
» Takes all measures necessary to ensure the security of the personal data in accordance with Article 21 of the DPJL;
» Only engages another data processor with the prior authorisation of the data controller;
» Assists wherever possible with the data controllers obligation to respond to the exercising of rights by data subjects;
» Assists the data controller in ensuring compliance with data protection impact assessments (Article 16 DPJL), breach notifications (Article 20 DPJL) and data security (Article 21 DPJL);
» Deletes or returns personal data as required by the data controller upon conclusion of the processing contract;
» Provides any information necessary to the data controller and contributes to audits and inspections instigated by the data controller;
» Inform data controllers if an instruction contravenes the DPJL or principles contained therein;
» Provide assurances to the data controller that they will remain liable to the controller in the event that the processing activities are further outsourced;

g. must report any personal data breach in the manner and to the extent required by Article 20 unless Part 7 applies;

Data controllers are required to report a personal data breach in writing to the Commissioner within 72 hours of having become aware of the breach.

(Detailed guidance on breach reporting can be found in a separate guidance note).

h. must appoint a data protection officer where so required by Article 24;

Data controllers are required to appoint a Data Protection Officer (DPO) if they are:

- A Public Authority (except for the courts acting in their judicial capacity);
- Carrying out the core activities of their business which require the systematic monitoring of customers on a large scale;
- Processing special category data on a large scale as part of their core activities (Eg. Medical practices, vetting bureaus);
- Required to by law.

i. must co-operate with any requests of the Authority under this Law or the Authority Law; and

The Commissioner has a number of powers afforded to them under the Data Protection (Jersey) Law 201- and the Data Protection Authority (Jersey) Law 201-. That means the Commissioner may request certain information from you, or require you to take certain steps to meet compliance with the law as part of the exercise of their duties. Data controllers are required to co-operate with the Commissioner at all times.

j. must comply with any order of the Authority under Article 25 of, and notice of the Authority under paragraph 1 of Schedule 1 to, the Authority Law.

Orders under Article 25 of the Data Protection Authority (Jersey) Law 201- relate to sanctions that may be imposed by the Commissioner following the determination of a breach. The notice under paragraph 1 of Schedule 1 relates to the Commissioner's power to issue an Information Notice. This notice is a request for information from a data controller or processor for the purposes of determining whether or not to investigate a complaint, conduct an inquiry, conduct an investigation, determine an order or exercise any of their other powers under the law.

10. Adherence to a code or evidence of certification may provide evidence that an individual controller has complied with a particular obligation under this Law.

A number of providers (local and international) provide mechanisms for certification which can assist in evidencing that you maintain a particular set of standards for compliance with the Law. Similarly, data controllers may choose to sign up to any applicable codes of practice which may set out standards deemed to assist in demonstrating compliance with certain provisions of the Law. However, at the time of writing, the European Data Protection Board has not officially certified any courses, mechanisms or standards thus far. Controllers must therefore exercise caution and conduct thorough due diligence checks before committing to any certification scheme or qualification.

MORE INFORMATION

12. Additional guidance is available on our guidance pages with more information on other aspects of the DPJL.

13. This guidance has been developed drawing on the Commissioner's experience. It will be reviewed and considered from time-to-time in line with new decisions by the Commissioner and/or the Jersey courts.

14. It is a guide to our general recommended approach, although each individual case will likely be different and will be decided on the particular circumstances of the case.

15. If you need any further information about this, or any other aspect of the DPJL, please contact us or see our website www.jerseyoic.org

Jersey Office of the Information Commissioner
2nd Floor
5 Castle Street
St Helier
Jersey JE2 3BT

Telephone number: +44 (0) 1534 716530
Email: enquiries@jerseyoic.org