JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

GUIDANCE NOTE

Criminal Offences and Civil Remedies

Data Protection Authority (Jersey) Law 2018

MAY 2018 • V1 • WWW.JERSEYOIC.ORG

CONTENTS

Introduction and overview 3

Criminal offences under the DPJL 5

Criminal offences under the DPAJL 9

Civil remedies available to data subjects 10

More information 12

INTRODUCTION AND OVERVIEW

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. The Data Protection Authority (Jersey) Law 2018 ("**DPAJL**") establishes the Data Protection Authority (the **Authorit**y) (which replaces the Office of the Information Commissioner). The Information Commissioner (the **Commissioner**) is the Chief Executive Officer of the Authority.

3. The DPJL gives data subjects rights to bring complaints and seek judicial remedies and it also brings forward certain criminal offences. Similarly, the DPAJL places certain other obligations on controllers and processors and also brings forward criminal offences in certain circumstances.

4. The offences the DPJL brings forward are:
   a. Unlawfully obtaining personal data (Art.71 of the DPJL);
   b. Requiring a person to produce certain records (Art.72 of the DPJL);
   c. Providing false information (Art.73 of the DPJL); and
   d. Obstruction (Art.74 of the DPJL).

   Under the DPJL, most of the offences are punishable by fine, except where expressly provided.

5. The offences the DPAJL brings forward are:
   a. Failing to register with the Authority as a controller or processors (Art.17(6) of the DPAJL);
   b. Failing to comply with an order made by the Authority following a breach determination (Art.25(8) of the DPAJL).

   Under the DPAJL, the above offences are punishable by fine.

6. Individuals also have a number of civil remedies available to them under the DPJL namely:
   a. The right to lodge a complaint with the Authority where their data has been processed in a way that does not comply with the DPJL;
   b. The right to bring civil proceedings against controllers in the Royal Court; and
   c. The right to compensation from a relevant controller or processor for loss, damage or distress resulting from infringement of the DPJL.

   This note deals with the right to issue civil proceedings and the right to compensation only. For information regarding the lodging of complaints with and enforcement by the Authority (including fining powers) please see our separate guidance note.

Who can bring criminal proceedings?

7. Proceedings for a criminal offence under the DPJL can only be commenced by Her Majesty's Attorney General. The Authority and/or the Commissioner cannot bring prosecutions personally as a matter of Jersey law.

Who can bring civil proceedings?

8. A data subject can bring proceedings personally and there is also provision for a data subject to be represented by a "data protection organization" (this meaning any non-profit organisation properly constituted in accordance with relevant law that has objectives in the public interest and is active in the field of the protection of data subject rights).

In which Court can proceedings be brought?

9. Generally speaking, the seriousness of the criminal offence will determine whether or not such offences are dealt with in the Magistrate's or the Royal Court. The maximum fine that may be imposed by the Magistrate's Court is £10,000 and the maximum term of imprisonment that may be imposed is 12 months. The Royal Court has no upper limit either in terms of fine or prison sentence.

10. On conviction of an offender, the Court may order any data apparently connected with the crime to be forfeited, destroyed or erased.

11. In respect of civil proceedings, these would be brought in the Royal Court.

CRIMINAL OFFENCES UNDER THE DPJL

The Offences

12. Unlawfully obtaining personal data (Art.71)

a. It is an offence for a person, knowingly or recklessly, without the consent of the controller to:

i. obtain or disclose personal data or the information contained in the personal data; or

ii. procure the disclosure to another person of the information contained in the personal data.

b. The DPJL provides specific exemptions to liability for this offence where the person can show:

i. that the obtaining, disclosing or procuring:

» was necessary to prevent or detect crime; or

» was required or authorised by any enactment, rule of law or by order of the Court,

ii. that he acted in the reasonable belief that he had the legal right to obtain, disclose or procure the disclosure;

iii. that he acted in the reasonable belief that the controller would have consented to their obtaining, disclosing or procuring the data if the controller had known; or

iv. that in the circumstances, the obtaining, disclosing or procuring was in the public interest.

c. A person will not be guilty of this offence if the personal data in question fall within the national security exemption at Art.41.

d. It should be noted that an offence under this section cannot be committed by a controller in respect of data of which he is the controller. However, a controller who discloses personal data of which he is the controller may breach Art.8(1)(a) of the DPJL if the disclosure is unfair or unlawful (and thus disclosed in breach of the data protection principles).

e. Where employees of a controller have authority to obtain and disclose personal data in the course of their employment (i.e. police or civilian officers who have access to certain databases for policing purposes), they will commit these offences if their use their own position to obtain, disclose or procure disclosure of personal data for their own purposes.

Example 1

Jane Doe, a former nursing auxiliary was fined for accessing a patient and her neighbour's medical records without a valid legal reason. She worked at the Hospital and unlawfully accessed the records of a patient who was also her neighbour when she had no legitimate reason for doing so. John Doe, who at the time worked for the Council, emailed personal data relating to 349 individuals, which included special category data of service users of the Adult Social Care Department, to his personal email address without his employer, the data controller's, consent.

f. A person found guilty of an offence under this article is liable to a fine (Art.75(1)).

13. Requirement to produce certain records illegal (Art.72)

a. The offence created under Art.72 of the DPJL is commonly known as "enforced subject access".

b. Unless one of the statutory exceptions apply, it is an offence for a person to require[1] another person or a third party to supply or produce a relevant record in connection with:

i. the recruitment of that other person as an employee (Art.72(1)(a));

ii. the continued employment of that person (Art.72(1)(b));

iii. any contract for the provision of services to him by that person (Art.72(1)(c));

or

iv. where a person is concerned with providing (for payment or not) goods, facilities or services to the public or a section of the public, as a condition of providing or offering to provide any goods, facilities or services to that other person (Art.72(2)).

Example 2

An individual applies for a position as a waiter at a restaurant but is told that they cannot be offered the position until they provide a copy of their criminal record. The employer states that the potential employee must make a subject access request in order to gain this information and they will only be appointed if the results of the subject access request are supplied to the employer. In making a request in such circumstances, the employer is likely to have committed an offence under Art.72(1)(a) of the DPJL.

Example 3

A shop owner decides to extend the size of their premises. A local builder submits the successful tender. The shop owner requires the builder to confirm whether or not they have ever been in prison and asks him to make a subject access request to the Prison Service and provide the shopkeeper with the results of the subject access request. In this instance, the shop keeper is likely to have committed an offence under Art.72(1)(c) of the DPJL.

Example 4

An individual makes an application for insurance to an insurance provider. The individual wants to be provided with a service. The insurer agrees to insure the individual but explains that it is a condition of the insurance that the individual must make a subject access request for their criminal record. The insurance company is likely to have committed an offence under Art.72(2) of the DPJL.

[1] "to make necessary" or "specify as compulsory" - https://en.oxforddictionaries.com/definition/require

c. The term "relevant record" is defined in Art.72(6) of the DPJL by reference to a table which lists certain data controllers and the subject-matter of subject access requests that may be made to them by data subjects. Generally, the term relates to records of cautions, criminal convictions and to certain social security records relating to the data subject. Enforced subject access will accordingly typically occur where a person wishes to see another individual's criminal record, but chooses not to use the established lawful system (i.e. via through the criminal records disclosure regime). The Rehabilitation of Offenders (Exceptions) (Jersey) Regulations 2002[2] lists the types of work, employment or professions on which an organisation can legally obtain a DBS check and the States of Jersey Police have more information about the disclosure and vetting services on their website[3].

d. An individual providing the results of a subject access request rather than using the appropriate channel set out above, runs the risk of greater, and sometimes excessive disclosure. This is because a subject access request requires all personal information to be disclosed (subject to some exemptions), and does not distinguish between spent and unspent convictions. Making this type of request is a right set out in the DPJL, but there is a distinction between someone doing so of their own volition and somebody being required to make such a request by someone else.

e. It is the act of "requiring" an individual to make a subject access request that is the offence. The requirement is enough, and is not dependant on the withdrawal of the offer or employment or the provision of goods, facilities or services. Suggesting that it would be cheaper for an individual to make a subject access request (free) than going through an appropriate criminal record check and thus encouraging or incentivising the data subject to use their subject access rights to obtain the information would be sufficient to constitute a requirement.

f. Art.72(3) of the DPJL explains that it will not be a criminal offence for a person to request an individual to make a subject access request for their personal data if:

   i. that the imposition of the requirement was required or authorised by or under any enactment, rule of law or by order of a court (Art.72(3)(a)); or

   ii. that in the particular circumstances the imposition of the requirements was justified as being in the public interest (Art.73(3)(b)).

   In respect of the latter exemption, given the importance of subject access as a core right within the DPJL, there will need to be an extremely strong justification for enforced subject access to be justified as being in the public interest, supported by clear, specific and cogent evidence. This may be difficult to achieve as there is already clear public policy and laws relating to criminal record checking and rehabilitation and the availability of such information.

g. A person found guilty of an offence under this article is liable to a fine of level 3 on the standard scale (Art.72(4)). (Level 3 on the Criminal Justice (Standard Scale of Fines) (Jersey) Law 1993 is £10,000[4].)

14. False information (Art.73)

a. It is an offence for a person to either knowingly or recklessly provide the Authority (or any other person entitled to information under the DPJL, DPAJL or any Regulations made thereunder) with information that is false or misleading in a material way.

b. "Information" means that which has been provided in connection with an application under the DPJL or DPAJL (Art.73(2)(a)), or in purported compliance with a requirement under the DPJL and/or DPAJL and/or any Regulations or in circumstances in which the person providing the information intends or could reasonably expect to know, that the information will be used by the Authority for the purposes of carrying out their functions under the DPJL or DPAJL.

c. A person found guilty of an offence under this article is liable to imprisonment for a term of two years and to a fine.

[2] https://www.jerseylaw.je/laws/revised/Pages/08.840.50.aspx

[3] https://jersey.police.uk/accessing-information/personal-information-access/disclosure-and-barring-service/

[4] https://www.jerseylaw.je/laws/revised/Pages/08.360.aspx

15. Obstruction (Art.74)
    a. A person must not:
        i. intentionally obstruct or impede;
        ii. interfere with, cause or knowingly permit to be interfered with anything done by;
        iii. fail to give assistance or information that is reasonably required;
        iv. fail to produce record when required to do so;
        v. fail to cooperate with the exercise of any power under Sched.1 of the DPAJL

        the Authority or any person acting in the execution or enforcement of the DPJL or DPAJL.
    b. A person found guilty of an offence in respect of parts i and ii above is liable to imprisonment for a term of two years and to a fine. In all other cases, a person found guilty of an offence is liable to a fine.

Personal liability where the data controller is a company or corporate body

16. If a company or other organisation commits a criminal offence under the DPJL (specifically in respect of Arts.7174), any director, manager, secretary or similar officer or someone purporting to act in such capacity is personally guilty of an offence in addition to the corporate body if:
    a. The offence was committed with his/her consent or connivance; or
    b. The offence is attributable to any neglect on his/her part.

CRIMINAL OFFENCES UNDER THE DPAJL

17. Registration of controllers and processors (Art.17(1))
    a. It is an offence for a controller or processor to process personal data without registration.
    b. An offence under this article is punishable by way of a fine.

18. Failing to comply with an order made by the Authority following a breach determination (Art.25(8))
    a. If the Authority makes a breach determination against a controller or processor and makes an order under Art.25(3)(a)-(f) of the DPAJL, the recipient commits an offence if they fail to comply with the order within any time frame specified for its compliance.
    b. An offence under this article is punishable by way of a fine.

19. Personal liability where the data controller is a company or corporate body
    a. If the above offences are committed with the consent or connivance of:
        i. A person who is a partner of a limited liability partnership (LLP), or director, manager, secretary or other similar officer;
        ii. In the case of any other partnership, a partner;
        iii. In the case of any other unincorporated body, any officer of that body who is bound to fulfil any duty of which the offence is a breach or, if there is no such officer, any member of the committee or other similar governing body; or
        iv. Any person purporting to act in any capacity described above

    then such person is also guilty of the offence and liable in the same manner as the relevant body to the penalty provided for that offence.

20. Aiding and abetting
    a. A person who aids, abets, counsels or procures the commission of an offence under the DPAJL is also guilty of an offence and liable in the same manner as the principal offender.

CIVIL REMEDIES FOR DATA SUBJECTS

21. An individual who suffers loss, damage or distress as a result of any contravention of the transparency and subject rights provisions may bring proceedings against the controller responsible for the contravention in the Royal Court and is entitled to compensation. Art.1(1) of the DPJL defines "transparency and subject rights provisions" as follows:

    "(a) the first data protection principle set out in Article 8(1)(a), to the extent that it requires data to be processed transparently;

    (b) the provisions as to information to be provided to a data subject under Article 12; and

    (c) the rights of data subjects set out in Part 6."

22. Under Part 6 of the DPJL, data subjects are entitled (subject to certain exceptions):

    a. to receive certain minimum information from the controller about the processing of their data and a copy of the data itself (the **right of access**);

    b. to have rectified any inaccurate date concerning him or her or to have incomplete personal data completed (the **right of rectification**);

    c. to have their personal data erased without undue delay under certain circumstances (the **right of erasure**[5]);

    d. to obtain from the controller a restriction of processing where specific circumstances apply;

    e. to receive from the controller certain data in a structured, commonly-used and machine readable format (the **right to data portability**);

    f. to object to processing in certain circumstances; and

    g. not to be subject to a decision based solely on automated processing when it has a legal effect or other significant effect on the data subject.

23. All applications for compensation must be made to the Royal Court of Jersey: the Authority has no power to award compensation (even if, for example, the Commissioner has made an assessment that it is likely that the processing has not or is not being carried out in compliance with the provisions of the DPJL).

24. A controller or processor who proves that they are not responsible for the event giving rise to the loss, damage or distress are exempt from any liability to pay.

[5] Known colloquially and sometimes referred to as the "right to be forgotten".

How much with the Royal Court award if a claim for compensation is successful?

25. There are no guidelines as to appropriate levels of compensation for a claim under the DPJL and it is difficult to predict the Royal Court's approach to such until such cases have come before the Court for determination. The judge and jurats hearing the case will have a discretion in such matters and will take into account many factors when considering the appropriate level of compensation likely including the seriousness of the breach and the effect upon the data subject.

Who will pay the compensation?

26. Controllers are liable only for loss, damage or distress caused by processing which is not in compliance with the DPJL.

27. Processors are only liable for damage caused by any processing in breach of obligations specifically imposed on processors by the DPJL (Art.69(3)(a)), or caused by processing that is outside or contrary to lawful instructions of the controller (Art.69(3)(b)).

28. Where one or more controllers or processors are involved in the same processing that caused the loss, damage or distress, each controller and processor is jointly and severally liable for the loss, damage and distress (Art.69(4)). However, a controller or processor is entitled to reimbursement if they pay out compensation and part of the compensation corresponds to that other controller or processor's responsibility for the loss, damage or distress.

What other civil powers does the Royal Court have?

29. The Royal Court may also make such other orders as it considers appropriate in the circumstances of the case including:
    a. the granting of an injunction (including an interim injunction) to restrain any actual or anticipated contravention;
    b. making a declaration that the controller is responsible for the contravention or that a particular act, omission or course of conduct on the part of the controller would result in a contravention; and
    c. requiring the controller to give effect to the transparency and subject rights provisions.

MORE INFORMATION

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

21. 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.

22. 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.

23. If you need any further information about this, or any other aspect of the DPJL or DPAJL, 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