JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

GUIDANCE NOTE

Administrative Fines

Part 4 of the Data Protection Authority (Jersey) Law 2018

MAY 2018 • V1 • WWW.JERSEYOIC.ORG

CONTENTS

INTRODUCTION

1. The Data Protection (Jersey) Law (**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 **Authority**) which will replace the Office of the Information Commissioner. The Information Commissioner (the **Commissioner**) is the Chief Executive Officer of the Authority.

3. This is part of a series of guidance to help organisations fully understand their obligations, as well as to promote good practice.

OVERVIEW

- This guidance applies to data controllers (and in certain circumstances, processors), as defined under Art.1(1) of the DPJL. It sets out the circumstances in which the Authority will consider it appropriate to issue an administrative fine under the DPAJL. It also explains how the amount of the fine will be determined.

- The Authority's objective in imposing an administrative fine is to promote compliance with the DPJL and DPAJL and such must be sufficiently effective to act both as a sanction and as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others.

- The amount of the administrative fine depends on the nature of the breach: in respect of any matters set out in Art.26(1)(a)-(b) the administrative fine must not exceed £5,000,000[1] and for the matters specified in Art.26(1), must not exceed £10,000,000[2]. Art.27(2) of the AL sets out that *"An administrative fine must not exceed £300,000 or 10% of the person's total global annual turnover or total gross income in the preceding financial year, whatever is the higher."*

- The Authority will take into account the factors set out at Art.26(2) of the DPAJL including the nature, gravity and duration of the breach, the effect of the breach on the data subjects, and previous contraventions and the degree of cooperation with the Authority.

- Where the Authority intends to issue an administrative fine it will first serve notice in writing stating that the Authority is proposing to make an order for the payment of an administrative fine. This will specify the proposed amount of the fine and allow the recipient a period of 28 days (beginning on the date of the notice) within which the recipient can make written representations to the Authority.

- A data controller or processor on whom an administrative fine is served may appeal to the Royal Court of Jersey against that fine and/or the amount of the fine specified.

- The Commissioner will consider amending or replacing this guidance in light of further experience of its application.

[1] ART.27(1)(A) OF THE DPAJL

[2] ART.27(1)(B) OF THE DPAJL

ADMINISTRATIVE FINES

Who is eligible for a fine?

5. The DPAJL refers to 'person concerned' in Article 26 which is defined in paragraph (11) meaning *"the controller or processor against whom an administrative fine is ordered"*. Any controller or processor who is registered with the Authority (note: all entities controlling and processing personal data must be registered. Further information on registration can found in the Commissioner's note on Registration) and who breaches the requirements of proper processing of personal data under the law.

6. The DPJL and DPAJL apply to the whole of the Bailiwick of Jersey. The power to impose an administrative fine is part of the Authority's overall regulatory regime which includes the power to conduct an inquiry under Art.21 of the AL and, following any breach determination, to issue a reprimand[3], a warning[4] or make any other order under Art.25(3) of the DPAJL including restricting, limiting or ceasing (for a specified period or until specified action is taken) a controller or processors' processing operations, or suspending any transfers of personal data to a recipient in any other jurisdiction.

7. The proceeds raised from an administrative fine will not be kept by the Authority (or the Commissioner), but will form part of the annual income of the States.

8. The power to impose administrative fines applies to any controller or processor in the private, public and not for profit sectors. They will not be imposed on an employee who was acting on the instructions of the employer.

9. As a general rule, a person with substantial financial resources is more likely to attract a higher monetary penalty than a person with limited resources for a similar contravention of the DPJL.

The aim of the Authority in imposing an administrative fine

10. The Authority's underlying objective in imposing an administrative fine is to promote compliance with the DPJL and any administrative fine must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening organisation and by others.

11. The Authority will seek to ensure that the imposition of an administrative fine is appropriate and the amount of that penalty is reasonable and proportionate, given the particular facts of the case and the underlying objective in imposing the administrative fine.

[3] ART.25(1)(a)
[4] ART.25(2)(b)

What happens before the Authority makes a breach determination (including issuing an administrative fine)

12. Where the Authority proposes to make:

    a. A breach determination
    b. An order under Art.25(3); or
    c. An order for the payment of an administrative fine

    The Authority must give the person concerned a notice in writing (a **Notice**).

13. The Notice must:

    a. State that the Authority is proposing to make a determination or order (including setting out the amount of any administrative fine);
    b. Set out the terms of and the grounds for the proposed determination;
    c. State that the person concerned may make written or oral representation to the Authority (in the manner specified in the Notice) within 28 days[5]; and
    d. Give notice of the right of appeal to the Royal Court in the event that the Authority makes the proposed determination or order.

Representations to the Authority

14. The purpose of the Notice is to set out the Authority's proposal and to enable the person concerned to make representations to the Authority.

15. The person concerned may wish to comment on the facts and views set out by the Authority in the Notice or to make general remarks on the case and provide documents or other relevant information, such as details of their finances. For example, if a personal data breach was caused entirely by a processor used by the data controller, the data controller may wish to provide the Authority with a full explanation of the circumstances that led to the breach, a copy of the processing agreement in place and the steps taken by the data controller to ensure compliance with the security guarantees in the agreement.

16. The person concerned should also inform the Authority if there is any confidential or commercially sensitive information that should be redacted from any information the Authority may decide to publish about the decision to impose an administrative fine.

17. The Authority must consider any representations made in response to the Notice before giving further consideration to the proposed determination or order.

18. Having taken full account of the representations made by the person concerned and any other relevant matters, the Authority will decide whether or not to impose an administrative fine and, if so, the level of such.
    The administrative fine should not be substantially different to the amount proposed in the Notice unless the representations of the person concerned can justify a reduction.

[5] 28 days starts on the date of the notice.

Level of fines

19. The Authority (and the Commissioner's) underlying objective in imposing administrative fines is to promote compliance with the DPJL. Such must be sufficiently effective to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others. The Authority will seek to ensure that the imposition of a monetary penalty is appropriate and the amount of that penalty is reasonable and proportionate, given the facts of the case and the underlying objective in imposing the administrative fine.

Factors the Authority will take into account when deciding whether to issue an administrative fine

20. In deciding whether it is appropriate to impose an administrative fine and in determining the amount of such, the Authority will take full account of the specific facts and the circumstances of the contravention and of any representations made..

21. In particular, the Authority must have regard to the following matters[6]:

    a. The nature, gravity and duration of the contravention of the DPJL, taking into account the nature, scope and purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

    b. Whether the contravention was intentional or negligent;

    c. Any action taken by the person concerned to mitigate the loss, damage or distress suffered by data subjects;

    d. The degree of responsibility of the person concerned taking into account technical and organisational measures implemented by the person concerned;

    e. Any relevant previous contraventions;

    f. The degree of cooperation with the Authority, in order to remedy the breaches and mitigate the possible adverse effects of the contraventions;

    g. The categories of personal data affected by the contravention;

    h. The manner in which the contravention became known to the Authority, in particular whether, and if so to what extent, the person concerned notified the contravention to the Authority;

    i. Where the Authority has previously made an order against the person concerned following a breach determination with regard to the same subject matter, compliance with any measures required to be taken by the order;

    j. Compliance (or not) with any code or evidence of certification in respect of the processing concerned;

    k. Any other aggravating or mitigating factor applicable to the circumstances of the case (i.e. financial benefits gained, or losses avoided, directly or indirectly from the contravention).

[6] ART.26(2)(a)-(k)

Level of fines (continued)

The nature, gravity and duration of the contravention

22. Almost all of the obligations of the controllers and processors are categorised according to their nature in the provisions of Art.26(1)(a)-(d) of the DPAJL. In setting up two different maximum amounts of administrative fine, this clearly indicates that a breach of certain provisions of the DPJL may be more serious than for others.

23. The more serious the breach and the longer it goes on for, the more likely it is that any administrative fine will be higher.

Intentional or negligent

24. The paper produced by the Article 29 Working Party that sets out guidelines for the application and setting of administrative fines notes that *"In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law".* The Commissioner agrees with this statement.

25. Similarly, the Commissioner also agrees with the statement that "*intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine. The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case... Other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence.*"

Example 1

The CEO of a large organisation knows that there has been a breach of security and is advised by his head of IT that there was a flaw in the computer system in that the software used by the company is out of date and no longer supported. The head of IT recommends a new computer system. The CEO refuses to authorise the purchase of the new software because he thinks it is too expensive. Unfortunately, the company suffers another breach in identical circumstances to the same breach.

Example 2

An organisation has received a number of unsubscribe requests from individuals to their marketing emails. In spite of the clear requests made by the individuals to remove their contact details from the organisation's database. The organisation then decides to send an email to those individuals to see whether or not they want to opt in to their communications.

Level of fines (continued)

Action taken to mitigate the loss, damage or distress

26. The steps an organisation takes following discovery of a breach will be extremely important in determining the type of penalty to impose on an organisation and an organisation is obliged to take whatever steps necessary to reduce the consequences of the breach for the individuals concerned. Responsible behaviour would be taken by the Authority when deciding what sanction is appropriate as well as the level of any administrative fine.

The degree of responsibility of the controller or processor

27. The degree of responsibility will be assessed against:

a. The technical measures implemented by the organisation;

b. The organisational measures implemented by the organisation;

c. The security measures implemented by the organisation;

d. The relevant policies and procedures in place and applied in the organisation.

28. The Authority will also take account of any best practice procedure or methods that exist including any industry standards.

Any previous contraventions?

29. The track record of an organisation will be assessed when considering an appropriate sanction. The Authority will consider whether or not the organisation has committed an identical or substantially similar contravention previously. Repeat offenders should expect a more severe sanction than a first time offender.

Categories of the personal data affected

30. Key matters for the Authority when determining an appropriate sanction will include:

a. Whether or not the contravention involved any special category data;

b. Whether data subjects are directly identifiable from the information;

c. Whether the dissemination or the personal data would cause loss, damage or distress to the individual;

d. Whether the data was protected (i.e. was it encrypted?)

Variation of administrative fine

31. The Authority may, of its own motion or on the application of the person concerned:

a. Vary the amount of fine; or

b. Vary the number, amounts and times of the instalments by which the fine is to be paid.

Right of Appeal

32. A controller or processor affected by any determination or order of the Authority (including the making of an order for payment of an administrative fine) may appeal to the Royal Court, in accordance with Art.32 of the DPAJL on the grounds that "*in all the circumstances of the case the decision was not reasonable*".[7]

Public statements

33. Following the issuing of an administrative fine, and "Where the Authority considers that because of the gravity of the matter or other exceptional circumstances, it would be in the public interest to do so" the Authority may issue a public statement about any aspect of the issuing of the administrative fine, including the circumstances that gave rise to it (Art.14 of the DPAJL).

34. Such statement may include:

    a. Details of any personal data breach

    b. Information describing or identifying any data subject whose personal data is or has been the subject of a personal data breach;

    c. Information as to the nature and the progress or any complaint, investigation or inquiry; or

    d. The outcome of any complaint, investigation or inquiry,

35. Before issuing a public statement, the Authority must:

    a. Consult any individual whose personal data would be made public by that public statement, or who is otherwise likely to be identifiable from the statement; and

    b. Give written notice of the contents of the statement to any controller and any processor that is likely to be identifiable from the statement[8].

36. The public statement will be published on the Commissioner's website with any confidential or commercially sensitive information redacted.

How to pay

37. The administrative fine is not kept by the Authority but must be paid to and forms part of the income of the Government of Jersey.

Failure to pay

38. If an organisation fails to pay the administrative fine, the Authority may take steps to recover the fine as a debt owed to the Authority. This will be pursued as a civil matter.

[7] ART.33(2)

[8] ART.14(4)(a)-(b) of the AL

MORE INFORMATION

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

40. 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.

41. 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.

42. 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