JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

GUIDANCE NOTE

Rights of data subjects

Articles 27-39 and 71 of the Data Protection (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 DPAJL 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

RIGHTS OF DATA SUBJECTS

The DPJL

4. Part 6 of the DPJL gives rights to individuals in respect of personal data held about them by others. The rights are:
   a. Right to be informed (Art.12)
   b. Right to subject access (Arts.28-30)
   c. Right to rectification (Art.31)
   d. Right to erasure (Art.32)
   e. Right to restriction of processing (Art.33)
   f. Right to data portability (Art.34)
   g. The right to object to processing for the purpose of public functions or legitimate interests (Art.35), for direct marketing purposes (Art.36) and for historical or scientific purposes (Art.37)
   h. Right regarding automated individual decision-making and profiling (Art.38).

RIGHT TO BE INFORMED

5. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the DPJL and is set out at Art.12.

6. Getting this correct can help you to comply with other aspects of the DPJL and build trust with people, but getting it wrong can leave you open to fines and/or other enforcement action and lead to reputational damage..

7. You must provide individuals with information including:
   a. your purposes for processing their personal data;
   b. your retention periods for that personal data; and
   c. who it will be shared with. This is called the "specified information".

When should the information be provided?

8. If you collect personal data directly from the data subject, you must provide the specified information to (or make it readily available) to individuals at the time you collect their personal data from them.[1]

9. If, however, you obtain personal data from other sources, you must provide individuals with the specified information before the "relevant time". This is either:
   a. within a reasonable period of obtaining the data and no later than 4 weeks;
   b. no later than the time of the first communication with the data subject (if the personal data is to be used for communication with that individual); or
   c. no later than the point at which the individual's personal data are first disclosed, if disclosure to another recipient is planned.

10. You must actively provide privacy information to individuals. You can meet this requirement by putting the information on your website, but you must make individuals aware of it and give them an easy way to access it.

Does the specific information always have to be provided?

11. There are a few circumstances when you do not need to provide people with the specified information.

12. When collecting personal data from individuals, you do not need to provide them with any information that they already have.

13. When obtaining personal data from other sources, you do not need to provide individuals with the specified information if:
   a. the individual already has the information;
   b. providing the information to the individual would be impossible;
   c. providing the information to the individual would involve a disproportionate effort;

[1] ART.12(1)

d. providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
e. you are required by law to obtain or disclose the personal data; or
f. you are subject to an obligation of professional secrecy regulated by law that covers the personal data.[2]

What information needs to be provided to the data subject?

14. Art.12(4) of the DPJL says that the specified information that must be provided to the data subject is all of the following:
    a. The name and contact details of your organisation together with contact details of your representative (if applicable);
    b. The contact details of your data protection officer (if any);
    c. The purposes for which the data are intended to be processed and the legal basis for the processing;
    d. An explanation of the legitimate interests pursued by you or by a third party for the processing (if processing is based on those interests);
    e. The recipients or categories of recipients of the personal data (if any);
    f. The details of transfers of the personal data to any third countries or international organisations and whether or not there is an adequate level of protection for the rights and freedoms of data subjects (if applicable);
    g. The retention periods for the personal data (or if that is not possible, the criteria used to determine that period);
    h. The rights available to individuals in respect of the processing;
    i. The right to withdraw consent (if applicable);
    j. The details of the existence of automated decision-making, and any meaningful information about the logic involved in such decision-making as well as the significance and envisaged consequences of such processing for the data subject (if applicable);
    k. A statement regarding the right to lodge a complaint with a supervisory authority;
    l. The details of whether individuals are under a statutory or contractual obligation, or requirement necessary to enter into a contract to provide the personal data and the possible consequences of failing to provide such data;
    m. The source of the personal data (if the personal data is not obtained from the individual it relates to); and
    n. Any further information that is necessary, having regard to the specific circumstances in which the data are or are to be processed to enable fair processing.

How should the information be provided?

15. You should think about intended audience when providing the specified information. If you collect or obtain children's personal data, you must take particular care to ensure that the information you provide them with is appropriately written, using clear and plain language.

16. For all data subjects the specified information must be provided to them:
    a. In intelligible form;
    b. Using clear language.

[2] ART.12(6)

17. It is often most effective to provide privacy information to people using a combination of different techniques including:
    a. A layered approach - short notices containing key privacy information that have additional layers of more detailed information.
    b. Dashboards - preference management tools that inform people how their data is used and allow them to manage what happens with it.
    c. Just-in-time notices - relevant and focused privacy information delivered at the time individual pieces of information about people are collected.
    d. Icons - small, meaningful, symbols that indicate the existence of a particular type of data processing.
    e. Mobile and smart device functionalities – including pop-ups, voice alerts and mobile device gestures or QR codes.

18. User testing is a good way to get feedback on how effective the delivery of your privacy information is.

Review

19. You must regularly review, and where necessary, update your privacy information and you must bring any new uses of an individual's personal data to their attention before you start the processing.

RIGHT OF SUBJECT ACCESS

20. Art.28 provides that upon making a request individuals will have the right to obtain from the data controller:
    a. Confirmation as to whether or not their personal data is being processed;
    b. A copy of their personal data in intelligible format; and
    c. To be given information as to:
        i. The purposes for which their information is being processed by or on behalf of the controller;
        ii. The categories of personal data concerned;
        iii. The recipients or classes of recipients to whom the information is or may be disclosed (including recipients in third countries or international organisations);
        iv. The retention period (or, if not possible, the criteria used to determine the retention period);
        v. The existence of the data subject's rights of rectification, erasure or restriction or processing or the right to object to such processing;
        vi. The right to lodge a complaint with the Authority;
        vii. Information as to the source of personal data if not collected directly from the data subject; and
        viii. The existence of automated decision-making (including meaningful information about the logic involved).

21. You may be providing much of this information already in your privacy notice.

22. Requests made in relation to health records must also be dealt with in accordance with Art.29.

How should a request be made?

23. There is no specified format for a subject access request and you cannot require individuals to use a specially designed form. Many organisations produce subject access request forms, and whilst you may invite individuals to use such a form you must make it clear that this is not compulsory and you must not try to use this as a way of extending the time limit for responding. Standard forms can make it easier for you to recognise a subject access request and make it easier for the individual to include all the details you might need to locate the information they want.

24. However, any request in writing must be considered as a valid request, whatever the format. Requests may also be made verbally and can be made to any part of your organisation (including by social media) and does not have to be to a specific person or contact point.

25. This presents a challenge as any of your employees could receive a valid request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

26. Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

27. If you have reasonable doubts about the identity of the data subject, you can ask that additional information is provided by the data subject in order to confirm their identity and you are not obliged to respond to the request unless supplied with that further information[3]. This is to avoid personal data about one individual being sent to another accidentally or as a result of deception. The level of checks you should make may well depend on the possible harm and distress which inappropriate disclosure of the information could cause to the individual concerned.

Example 1

A GP practice receives a subject access request from someone claiming to be a former patient. The name on the request matches a record held by the practice, but there is nothing else in the request to enable the practice to be confident that the requestor is the patient to whom the record relates. In this situation, it would be reasonable for the practice to ask for more information before responding to the request. The potential risk to the former patient of sending their health records to the wrong person is such that the practice is right to be cautious. They could ask the requestor to provide more information, such as a date of birth, a passport or a birth certificate.

Can requests be made on behalf of others?

28. The DPJL does not prevent an individual making a subject access request via a third party (i.e. a solicitor on behalf of a client). In such cases, you must be satisfied that the third party making the request is entitled to act on behalf of the data subject and the burden rests with the third party to prove that they have the necessary consent of the data subject.

Can I require an individual to make a subject access request?

29. Art.72 of the DPJL makes it a criminal offence to require an individual to exercise their subject access rights to gain access to information about their criminal convictions and cautions and provide that information to a person. This may be used, for example, to provide as supporting evidence regarding a job application or before entering into a contract for goods, facilities or services to the public.

30. A person who contravenes this provision is guilty of an offence and liable to a fine of level 3 on the standard scale.

31. There is an appropriate way of accessing an individual's criminal records (when it is legitimate to do so) through the criminal records disclosure regime. Organisations can request basic checks which would divulge unspent convictions, or standard checks, which would include spent and certain unspent convictions, cautions, reprimands and final warnings (though details of the latter may be filtered out in some cases). Enhanced checks would disclose all of the information held in a standard check plus certain relevant information held by the police on an individual.

[3] ART.27(7)

32. An individual providing the results of a subject access request, rather than using the appropriate channels, 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, for instance, between spent and unspent convictions.

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 they must make a subject access request in order to gain this information and they will only be appointed if it is supplied. The employer is likely to have committed an offence under subsection 72(1)(a) of the DPJL.

Example 3

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.

33. Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong, for example, to a parent or guardian. Therefore, it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

34. Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should respond to the child rather than a parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:
    a. the child's level of maturity and their ability to make decisions like this;
    b. the nature of the personal data;
    c. any court orders relating to parental access or responsibility that may apply;
    d. any duty of confidence owed to the child or young person;
    e. any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
    f. any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
    g. any views the child or young person has on whether their parents should have access to information about them.

35. Art.11(4) of the DPJL refers to a child over the age of 13 being able to give valid consent for the purposes of an information society service. You must not confuse this provision as meaning that a child over the age of 13 is taken as being able to provide consent for any other of the other provisions contained in the DPJL. The provisions of Art.11(4) relate solely to the obtaining of consent in respect of an information society service.

How should the information be provided?

36. If the request is made electronically, you must provide the information in a commonly used electronic format where possible, unless otherwise requested by the data subject[4].

Can fees be charged for dealing with a subject access request?

37. No. You must provide a copy of the information free of charge[5]. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive[6].

38. You may also charge a reasonable fee to comply with requests for further copies of information that has already been provided in response to that particular request[7]. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.

How long do we have to comply?

39. Information must be provided without delay and at the latest within 4 weeks of receipt of the request[8].

40. You will be able to extend the period of compliance by a further 8 weeks where requests are complex or numerous. If this is the case, you must inform the individual within 4 weeks of receipt of the request and explain why the extension is necessary.

What if sending out copies will be expensive or time consuming? Can a request be refused?

41. In some cases, dealing with a subject access request will be an onerous task. This might be because of the nature of the request, the amount of personal data involved or because of the way in which certain information is held.

42. You cannot refuse to comply with a request simply because it relates to large amounts of data but you may be able to consider whether the request is manifestly vexatious, unfounded or excessive (in particular because they are repetitive). In such circumstances you can:
    a. charge a reasonable fee taking into account the administrative costs of providing the information; or
    b. refuse to respond[9].

[4] ART.27(3)
[5] ART.27(5)
[6] ART.27(6)
[7] ART.28(3)(b)
[8] ART.27(1)
[9] ART.27(6)

43. The terms "vexatious", "unfounded" and "excessive" are not defined in the DPJL (nor in the GDPR). The meaning of "vexatious" was, however, considered in the case of Information Commissioner v. Devon County Council & Dransfield [2012] UKUT 440 (an appeal under the Freedom of Information Act 2000) where the Tribunal held that "vexatious" could be defined as the *"...manifestly unjustified, inappropriate or improper use of a formal procedure"*[10]. On appeal[11], the Court also observed that:

> "...the emphasis should be on an objective standard and that the starting point is that vexatiousness primarily involves making a request which has no reasonable foundation, that is, no reasonable foundation for thinking that the information sought would be of value to the requester or to the public or any section of the public... 'The decision maker should consider all the relevant circumstances in order to reach a balanced conclusion as to whether a request is vexatious.'

44. Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without delay and at the latest within 4 weeks of receipt of the request[12].

Third party information

45. A particular problem arises for data controllers who may find that in complying with a subject access request they will disclose information relating to that individual other than the data subject who can be identified from that information, including the situation where the information enables that third party to be identified as the source of the information. The DPJL recognises this problem and sets out only two circumstances[13] in which the data controller is obliged to comply with the subject access request in such circumstances, namely:
    a. Where the other individual has consented to the disclosure of the information to the person making the request; or
    b. It is reasonable in all the circumstances to do so without the consent of the other individual.

46. In helping you to decide whether it is reasonable in all the circumstance to comply with the request without the consent of the third party, you must have regard to:
    a. The type of information that you would disclose;
    b. Any duty of confidentiality owed to the individual;
    c. Any steps taken by the controller to seek the consent of the other individual;
    d. Whether the other individual is capable of giving consent; and
    e. Any express refusal of consent by the other individual[14].

47. If the data controller is satisfied that the data subject will not be able to identify the other individual from the information, taking into account any other information which, in the reasonable belief of the data controller, is likely to be in (or to come into) the possession of the data subject, then the data controller must provide the information.

48. If the data controller can protect the identity of the other individual by deleting/redacting names or other identifying information, the data controller must provide the information in this way[15].

[10] See para.27 of Dransfield.
[11] Dransfield v. Information Commissioner and Devon County Council [2015] EWCA Civ 454.
[12] ART.27(4)
[13] ART.28(4)
[14] ART.28(7)(a)-(d)
[15] Art.28(6)

The role of a data processor

49. Responsibility for complying with a subject access request lies with the data controller. The DPJL does not allow any extension to the relevant time limit in cases where a controller has to rely on a data processor to provide the information needed to respond to the request.

Example 4

An employer is reviewing staffing and pay, which involves collecting information from and about a representative sample of staff. A third-party data processor is analysing the information.

The employer receives a subject access request from a member of staff. To respond, the employer needs information held by the data processor. The employer is the data controller for this information and should instruct the data processor to retrieve any personal data that relates to the member of staff.

50. Any contractual agreement (or other legal act) in place between a controller and processor must stipulate that the processor:

"19(4)...(e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights set out in Part 6..."

Health Records

51. Special rules apply where providing subject access to information about an individual's physical or mental health would be likely to cause serious harm to them or to another person's physical or mental health. These rules are set out at Art.29 of the DPJL, and their effect is to exempt personal data of this type from subject access to the extent that its disclosure would be likely to cause such harm (see Art.61(2) of the DPJL). To apply this exemption, there needs to be an assessment of the likelihood of the disclosure causing serious harm. Unless you are a health professional, you must consult the appropriate health professional who is or was most recently responsible for the clinical care of the individual concerned before deciding whether the exemption applies. This requirement to consult does not apply if the individual has already seen or knows about the information concerned.

52. If the data controller intends to rely upon an existing opinion obtained within the previous 30 weeks, the controller must consider whether it is reasonable in all the circumstances to consult the appropriate health professional again.

RIGHT TO RECTIFICATION

What is the right to rectification?

53. Under Art.31 of the DPJL individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

54. This right has close links to the accuracy principle of the DPJL (Article 8(1)(d)). However, although you may have already taken steps to ensure that the personal data was accurate when you obtained it, this right imposes a specific obligation to reconsider the information's accuracy upon request.

What do we need to do?

55. If you receive a request for rectification you should take reasonable steps to satisfy yourself that the data is accurate and, if not, to rectify the data if necessary. You should take into account any arguments and evidence provided by the data subject.

56. What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, you should make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

57. You may also take into account any steps you have already taken to verify the accuracy of the data prior to the challenge by the data subject.

When is data inaccurate?

58. The DPJL does not give a definition of the term accuracy. However, the Commissioner considers that personal data is likely to be inaccurate if it is incorrect or misleading as to any matter of fact.

What should we do about data that records a mistake?

59. Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individuals' data.

Example 5

If a patient is diagnosed by a GP as suffering from a particular illness or condition, but it is later proved that this is not the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be rectified.

What should we do about data that records a disputed opinion?

60. It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

What should we do while we are considering the accuracy?

61. Under Art.33(1)(a) an individual has the right to request restriction of the processing of their personal data where they contest its accuracy and for such period as it takes for you to check that it is accurate.

What should we do if we are satisfied that the data is accurate?

62. You should let the individual know if you are satisfied that the personal data is accurate, and tell them that you will not be amending the data. You should explain your decision, and inform them of their right to make a complaint to the Authority; and their ability to seek to enforce their rights through a judicial remedy.

63. You should also place a note on your system recording the fact that the individual challenged the accuracy of the data (and their reasons for doing so) and your decision recording your reasons as to why you refused their application.

Can we refuse to comply with the request for rectification for other reasons?

64. You can refuse to comply with a request for rectification if the request is manifestly vexatious, unfounded or excessive (in particular where the request is repetitive in nature).

65. If you consider that a request is manifestly vexatious, unfounded or excessive you can:
    a. request a "reasonable fee" to deal with the request; or
    b. refuse to deal with the request.

66. You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual without undue delay and within 4 weeks. You do not need to comply with the request until you have received the fee.

What should we do if we refuse to comply with a request for rectification?

67. You must inform the individual without undue delay and within 4 weeks of receipt of the request about:
    a. the reasons you are not taking action;
    b. their right to make a complaint to the Authority; and
    c. their ability to seek to enforce this right through a judicial remedy.

Does the request need to be in a specified format?

68. No, the DPJL does not specify how to make a request for rectification. Therefore, an individual can make a request for rectification verbally or in writing. It can be made to any part of your organisation and does not have to be to a specific person or contact point.

69. Similarly, a request to rectify personal data does not need to mention the phrase 'request for rectification' or Art.31 of the DPJL to be a valid request. As long as the individual has challenged the accuracy of their data and has asked you to correct it, or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request under Art.31. 70. This presents a challenge as any of your employees could receive a valid verbal request. However, you have the legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore, you may need to consider which of your staff who regularly interact with individuals may need specific training so they know how to identify and deal with a request.

71. Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request.

Can we charge a fee?

72. No, in most cases you cannot charge a fee to comply with a request for rectification.

73. However, as noted above, if the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

74. You must act upon the request without undue delay and at the latest within 4 weeks of receipt.

75. You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date 4 weeks later.

Example 6

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 2 October to comply with the request.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

Can we extend the time to respond to a request?

76. You can extend the time to respond by a further 8 weeks if the request is complex or you have received a number of requests from the individual. You must let the individual know without undue delay and within 4 weeks of receiving their request and explain why the extension is necessary.

77. The circumstances in which you can extend the time to respond can include further consideration of the accuracy of disputed data - although you can only do this in complex cases - and the result may be that at the end of the extended time period you inform the individual that you consider the data in question to be accurate.

78. However, it is the Commissioner's view that it is unlikely to be reasonable to extend the time limit if:
    a. it is manifestly unfounded or excessive;
    b. an exemption applies; or
    c. you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

79. If you have doubts about the identity of the person making the request, you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

80. You must let the individual know without undue delay and within 4 weeks that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Do we have to tell other organisations if we rectify personal data?

81. Yes; if you have disclosed the personal data to others, you must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

82. The DPJL defines a recipient as “any person to whom the data are disclosed, whether a third party or not, but does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the relevant law”. In practice, this means a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

RIGHT TO ERASURE

What is the right to erasure?

83. Under Art.32 of the DPJL individuals have the right to have personal data erased. This is also known colloquially as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

84. Individuals have the right to have their personal data erased if:
    a. the personal data are no longer necessary for the purpose which you originally collected or processed it for;
    b. you are relying on consent as your lawful basis for processing the data, and the individual withdraws their consent;
    c. you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
    d. you are processing the personal data for direct marketing purposes and the individual objects to that processing;
    e. you have processed the personal data unlawfully (i.e. in breach of the lawfulness principle set out in Art.8(1)(a) of the DPJL;
    f. you have to do it to comply with a legal obligation; or
    g. you have processed the personal data to offer information society services to a child who is unable to give valid consent under Art.11(4) of the DPJL.

How does the right to erasure apply to data collected from children?

85. There is an emphasis on the right to have personal data erased if the request relates to data collected from children who are unable to give valid consent. This reflects the enhanced protection of children's information, especially in online environments, under the DPJL.

86. Therefore, if you process data collected from children, you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

Do we have to tell other organisations about the erasure of personal data?

87. The DPJL specifies that you should tell other organisations about the erasure of personal data if the personal data has been made public (which would likely include in an online environment (for example on social networks, forums or websites)).

88. In those circumstances, taking account of available technology and the cost of implementation you must take reasonable steps to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable you should take into account available technology and the cost of implementation.

When does the right to erasure not apply?

89. The right to erasure does not apply if processing is necessary for one of the following reasons:
    a. to exercise the rights of freedom of expression and information;
    b. to comply with a legal obligation to which the data controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority;
    c. if the processing is necessary for public health purposes in the public interest (e.g. protecting against cross-border threats to health, and ensuring high standards of quality and safety of health care and of medicinal products or medical devices);
    d. where the processing is carried out for archiving or for statistical, scientific of historical research purposes in the public interest and where erasure is likely to render impossible or seriously impair the achievement of that processing; or
    e. for the establishment, exercise or defence of legal claims.

Can we refuse to comply with a request for other reasons?

90. You can refuse to comply with a request for rectification if the request is manifestly vexatious, unfounded or excessive (in particular where the request is repetitive in nature).

91. If you consider that a request is manifestly vexatious, unfounded or excessive you can:
    a. request a "reasonable fee" to deal with the request; or
    b. refuse to deal with the request.

92. You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual without undue delay and within 4 weeks. You do not need to comply with the request until you have received the fee.

What should we do if we refuse to comply with a request for rectification?

93. You must inform the individual without undue delay and within 4 weeks of receipt of the request about:
    a. the reasons you are not taking action;
    b. their right to make a complaint to the Authority; and
    c. their ability to seek to enforce this right through a judicial remedy.

Does the request need to be in a specified format?

94. No; the DPJL does not specify how to make a request for rectification. Therefore, an individual can make a request for rectification verbally or in writing. It can be made to any part of your organisation and does not have to be to a specific person or contact point.

95. Similarly, a request to rectify personal data does not need to mention the phrase 'request for rectification' or Art.32 of the DPJL to be a valid request. As long as the individual has challenged the accuracy of their data and has asked you to correct it, or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request under Art.32.

96. This presents a challenge as any of your employees could receive a valid verbal request. However, you have the legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore, you may need to consider which of your staff who regularly interact with individuals may need specific training so they know how to identify and deal with a request.

97. Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request.

Can we charge a fee?

98. No, in most cases you cannot charge a fee to comply with a request for rectification.

99. However, as noted above, if the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

100. You must act upon the request without undue delay and at the latest within 4 weeks of receipt.

101. You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date 4 weeks later.

Example 7

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 2 October to comply with the request.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

Can we extend the time to respond to a request?

102. You can extend the time to respond by a further 8 weeks if the request is complex or you have received a number of requests from the individual. You must let the individual know without undue delay and within 4 weeks of receiving their request and explain why the extension is necessary.

103. The circumstances in which you can extend the time to respond can include further consideration of the accuracy of disputed data - although you can only do this in complex cases - and the result may be that at the end of the extended time period you inform the individual that you consider the data in question to be accurate.

104. However, it is the Commissioner's view that it is unlikely to be reasonable to extend the time limit if:

a. it is manifestly unfounded or excessive;

b. an exemption applies; or

c. you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

105. If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

106. You must let the individual know without undue delay and within 4 weeks that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Do we have to tell other organisations if we rectify personal data?

107. Yes. If you have disclosed the personal data to others, you must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

108. The DPJL defines a recipient as "any person to whom the data are disclosed, whether a third party or not, but does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the relevant law". In practice, this means a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

RIGHT TO RESTRICTION OF PROCESSING

109. Art.33 of the DPJL gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

110. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time..

When does the right to restrict processing apply?

111. Individuals have the right to request you restrict the processing of their personal data in the following circumstances:
    a. the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
    b. the data has been unlawfully processed (i.e. in breach of the lawfulness principle) and the individual opposes erasure and requests restriction instead;
    c. you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
    d. the individual has objected to you processing their data under Art.35 and you are considering whether your legitimate grounds or reasons of public interest override those of the individual.

112. Although this is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:
    a. if an individual has challenged the accuracy of their data and asked for you to rectify it (Art.31), they also have a right to request you restrict processing while you consider their rectification request; or
    b. if an individual exercises their right to object under Arts.35,36 or 37, they also have a right to request you restrict processing while you consider their objection request.

113. Therefore, as a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

How do we restrict processing?

114. You need to have processes in place that enable you to restrict personal data if required. It is important to note that the definition of processing includes a broad range of operations including collecting, recording, organisation, structuring, dissemination and erasure of data. Therefore, you should use methods of restriction that are appropriate for the type of processing you are carrying out.

115. Whilst the DPJL is silent on the issue, Recital 67 to the GDPR suggests a number of different methods that could be used to restrict data, such as:
    a. temporarily moving the data to another processing system;
    b. making the data unavailable to users; or
    c. temporarily removing published data from a website.

116. It is particularly important that you consider how you store personal data that you no longer need to process but the individual has requested you restrict (effectively requesting that you do not erase the data).

117. If you are using an automated filing system, you need to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. You should also note on your system that the processing of this data has been restricted.

Can we do anything with the restricted data?

118. You must not process the restricted data in any way **except to store it** unless:
    a. you have the individual's consent;
    b. it is necessary for legal proceedings, obtaining legal advice or for the establishment, exercise or defence of legal rights;
    c. it is for the protection of the rights of another person (natural or legal); or
    d. it is for reasons of substantial public interest.

Do we have to tell other organisations about the restriction of personal data?

119. No; the DPJL does not state that if you have disclosed the personal data in question to others that you must contact each recipient and inform them of the restriction of the personal data.

When can we lift the restriction?

120. In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:
    a. the individual has disputed the accuracy of the personal data and you are investigating this; or
    b. the individual has objected to you processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and you are considering whether your legitimate grounds override those of the individual.

121. Once you have made a decision on the accuracy of the data, or whether your legitimate grounds override those of the individual, you may decide to lift the restriction. If you do this, you must inform the individual before you lift the restriction.

122. As noted above, these two conditions are linked to the right to rectification (Art.31) and the right to object (Arts.35, 36 and 37). This means that if you are informing the individual that you are lifting the restriction (on the grounds that you are satisfied that the data is accurate, or that your legitimate grounds override theirs) you should also inform them of the reasons for your refusal to act upon their rights under Articles 31, 35, 36 or 37. You will also need to inform them of their right to make a complaint to the Authority and their ability to seek a judicial remedy.

Can we refuse to comply with a request for other reasons?

123. You can refuse to comply with a request for restriction if the request is manifestly vexatious, unfounded or excessive (in particular where the request is repetitive in nature).

124. If you consider that a request is manifestly vexatious, unfounded or excessive you can:
    a. request a "reasonable fee" to deal with the request; or
    b. refuse to deal with the request.

125. You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual without undue delay and within 4 weeks. You do not need to comply with the request until you have received the fee.

What should we do if we refuse to comply with a request for rectification?

126. You must inform the individual without undue delay and within 4 weeks of receipt of the request about:
    a. the reasons you are not taking action;
    b. their right to make a complaint to the Authority; and
    c. their ability to seek to enforce this right through a judicial remedy.

Does the request need to be in a specified format?

127. No; the DPJL does not specify how to make a request for restriction. Therefore, an individual can make a request verbally or in writing. It can be made to any part of your organisation and does not have to be to a specific person or contact point.

128. Similarly, a request to erase personal data does not need to mention the phrase 'request for rectification' or Art.32 of the DPJL to be a valid request. As long as the individual has challenged the accuracy of their data and has asked you to correct it, or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request under Art.32.

129. This presents a challenge as any of your employees could receive a valid verbal request. However, you have the legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore, you may need to consider which of your staff who regularly interact with individuals may need specific training so they know how to identify and deal with a request.

130. Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request.

Can we charge a fee?

131. No, in most cases you cannot charge a fee to comply with a request for rectification.

132. However, as noted above, if the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

133. You must act upon the request without undue delay and at the latest within 4 weeks of receipt.

134. You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date 4 weeks later.

Example 8

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 2 October to comply with the request.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

Can we extend the time to respond to a request?

135. You can extend the time to respond by a further 8 weeks if the request is complex or you have received a number of requests from the individual. You must let the individual know without undue delay and within 4 weeks of receiving their request and explain why the extension is necessary.

136. The circumstances in which you can extend the time to respond can include further consideration of the accuracy of disputed data - although you can only do this in complex cases - and the result may be that at the end of the extended time period you inform the individual that you consider the data in question to be accurate.

137. However, it is the Commissioner's view that it is unlikely to be reasonable to extend the time limit if:
    a. it is manifestly unfounded or excessive;
    b. an exemption applies; or
    c. you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

138. If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

139. You must let the individual know without undue delay and within 4 weeks that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

RIGHT TO DATA PORTABILITY

140. The right to data portability give individuals the right to receive personal data they have provided to the a controller in a structured, commonly used and machine readable format. It also gives them the right t request that a controller transmits this data directly to another controller.

141. Under Art.34 of the DPJL, the right to data portability only applies:
   a. to personal data an individual has provided to a controller;
   b. where the processing is based on the individual's consent or for the performance of a contract; and
   c. when processing is carried out by automated means (i.e. excluding paper files).

142. Whilst the burden is on data controllers to comply with a request for portability, data processors have contractual obligations under the DPJL to assist the controller "by appropriate technical and organisational measures" with responding to requests by individuals to exercise their rights. It is desirable, therefore, that the data controller should "implement specific procedures in cooperation with its data processors to answer portability requests"[16].

143. In most cases, this will be obvious (e.g. information submitted by a data subject to a controller via an online form). The Art.29 Working Party, however, considers that this definition extends also to data resulting from the observation of that individual's activity. This might include:
   - history of website usage or search activities;
   - traffic and location data; or
   - 'raw' data processed by connected objects such as smart meters and wearable devices.

   In particular, the guidance referred to sets out the views of the Art.29 Working Party, as follows:

   "A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":
   - Data actively and knowingly provided by the data subject (for example, mailing address, user name, age, etc.)
   - Observed data provided by the data subject by virtue of the use of the service or the device. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.

   In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as "provided by" the data subject. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as "provided by the data subject" and thus will not be within scope of this new right."

[16] See guidance on data portability issued by the Article 29 Working Party: file:///C:/Users/davida.blackmore/Downloads/wp242_rev01_enpdf.pdf

144. The Commissioner endorses this view.

145. It does not include any additional data that you have created based on the data an individual has provided to you. For example, if you use the data they have provided to create a user profile then this data would not be in scope of data portability. Nor will it apply to genuinely anonymous data. (However, pseudonymous data that can be clearly linked back to an individual (eg where that individual provides the respective identifier) is within scope of the right.)

146. You should note however that if this 'inferred' or 'derived' data is personal data, you will still need to provide it to an individual if they make a subject access request. Bearing this in mind, if it is clear that the individual is seeking access to the inferred/derived data, as part of a wider portability request, it would be good practice to include this data in your response.

How do I comply?

147. You must provide the personal data in a structured, commonly used and machine readable format. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

148. The information must be provided free of charge.

149. If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.

150. If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual. Generally speaking, providing third party data to the individual making the portability request should not be a problem, assuming that the requestor provided this data to you within their information in the first place. However, you should always consider whether there will be an adverse effect on the rights and freedoms of third parties, in particular when you are transmitting data directly to another controller.

What does 'structured' mean?

151. Structured data allows for easier transfer and increased usability. This means that software must be able to extract specific elements of the data. An example of a structured format is a spreadsheet, where the data is organised into rows and columns, ie it is 'structured'. In practice, some of the personal data you process will already be in structured form. In many cases, if a format is structured it is also machine-readable.

What does 'commonly used' mean?

152. This simply means that the format you choose must be widely-used and well-established. However, just because a format is 'commonly used' does not mean it is appropriate for data portability. You have to consider whether it is 'structured', and 'machine-readable' as well. Although you may be using common software applications, which save data in commonly-used formats, these may not be sufficient to meet the requirements of data portability.

What does 'machine-readable' mean?

153. 'Machine readable' data is data in a data format that can be automatically read and processed by a computer.

How long do we have to comply?

154. You must act upon the request without undue delay and at the latest within 4 weeks of receipt.

155. You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date 4 weeks later.

Example 9

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 2 October to comply with the request.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

Can we extend the time to respond to a request?

156. You can extend the time to respond by a further 8 weeks if the request is complex or you have received a number of requests from the individual. You must let the individual know without undue delay and within 4 weeks of receiving their request and explain why the extension is necessary.

157. The circumstances in which you can extend the time to respond can include further consideration of the accuracy of disputed data - although you can only do this in complex cases - and the result may be that at the end of the extended time period you inform the individual that you consider the data in question to be accurate.

158. However, it is the Commissioner's view that it is unlikely to be reasonable to extend the time limit if:

a. it is manifestly unfounded or excessive;

b. an exemption applies; or

c. you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

159. If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

160. You must let the individual know without undue delay and within 4 weeks that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

RIGHT TO OBJECT TO PROCESSING

How do I comply with the right to object if I process personal data for purpose of public functions or legitimate interests? (Art.35 of the DPJL)

161. Where you process data exclusively for the exercise of public functions or on the basis of legitimate interests (or a combination of the two), the data subject has an absolute right to object to the processing.

162. You must inform individuals of their right to object "at or before the time of the controller's first communication", "explicitly" and "separately from any other matters notified to the data subject".

163. A data subject must raise the objection by way of written notice to the controller. If the objection relates to information society services, notice can also be given by automated means.

164. Where you have received such written notice from the data subject you must stop processing the personal data unless:
    a. you can demonstrate compelling legitimate or public interest grounds for the processing, which override the interests, rights and freedoms of the individual; or
    b. the processing is necessary for the establishment, exercise or defence of legal claims.

165. If you are deciding whether you have compelling legitimate grounds which override the interests of an individual, you should consider the reasons why they have objected to the processing of their data and you need to balance the individual's interests, rights and freedoms with your own legitimate grounds. During this process you should remember that it is your responsibility to demonstrate that your legitimate grounds outweigh the rights of the individual.

166. If you are satisfied that you do not need to stop processing the personal data in question you should let the individual know. You should explain your decision, and inform them of their right to make a complaint to the Authority and of their ability to seek to enforce their rights through a judicial remedy.

How do I comply with the right to object if I process personal data for direct marketing purposes? (Art.36 of the DPJL)

167. Where you process data for direct marketing purposes, the data subject has an absolute right to object to the processing.

168. You must inform individuals of their right to object "at or before the time of the controller's first communication", "explicitly" and "separately from any other matters notified to the data subject".

169. A data subject must raise the objection by way of written notice to the controller. If the objection relates to information society services, notice can also be given by automated means.

170. You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.

171. However, this does not automatically mean that you need to erase the individual's personal data, and in most cases it will be preferable to suppress their details. Suppression involves retaining just enough information about them to ensure that their preference not to receive direct marketing is respected in future.

How do I comply with the right to object if I process personal data for historic or scientific purposes? (Art.37 of the DPJL)

172. Where you process data for historical or scientific purposes, the data subject has an absolute right to object to the processing.

173. Where you have received such objection from the data subject you must stop processing the personal data unless:
    a. The purpose for which the data is processed relates to an objective that is in the public interest; and
    b. The public interest in processing the data outweighs the interests of the data subject.

RIGHT REGARDING AUTOMATED DECISION MAKING

What's new under the DPJL?

174. Profiling is now specifically defined in the DPJL

175. Solely automated individual decision-making, including profiling with legal or similarly significant effects is restricted.

176. There are three grounds for this type of processing that lift the restriction.

177. Where one of these grounds applies, you must introduce additional safeguards to protect data subjects.

178. The DPJL requires you to give individuals specific information about automated individual decision-making, including profiling.

179. There are additional restrictions on using special category and children's personal data.

What is automated individual decision-making and profiling?

180. Automated individual decision-making is a decision made by automated means without any human involvement. Examples of this include:
    a. an online decision to award a loan; and
    b. a recruitment aptitude test which uses pre-programmed algorithms and criteria.

181. Automated individual decision-making does not have to involve profiling, although it often will do.

182. Art.1 of the DPJL says that profiling:

> *"...means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour or movements."*

183. Organisations obtain personal information about individuals from a variety of different sources. Internet searches, buying habits, lifestyle and behaviour data gathered from mobile phones, social networks, video surveillance systems and the Internet of Things are examples of the types of data organisations might collect.

184. Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals. Based on the traits of others who appear similar, organisations use profiling to:

a. find something out about individuals' preferences;

b. predict their behaviour; and/or

c. make decisions about them.

185. This can be very useful for organisations and individuals in many sectors, including healthcare, education, financial services and marketing.

186. Automated individual decision-making and profiling can lead to quicker and more consistent decisions. But if they are used irresponsibly there are significant risks for individuals. The DPJL provisions are designed to address these risks.

What does the DPJL say about automated individual decision-making and profiling?

187. The DPJL restricts you from making solely automated decisions (including those based on profiling) that have a legal or similarly significant effect on individuals:

"The data subject has the right not to be subject to a decision based solely on automated processing that produces legal effects or similarly significantly affects him or her" (Art.38).

188. For something to be solely automated there must be no human involvement in the decision-making process.

189. The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the DPJL (or the GDPR), but the decision must have a serious negative impact on an individual to be caught by this provision.

190. A legal effect is something that adversely affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

When can we carry out this type of processing?

191. Solely automated individual decision-making (including profiling) with legal or similarly significant effects is restricted, although this restriction can be lifted in certain circumstances.

192. You can only carry out solely automated decision-making with legal or similarly significant effects if the decision is:

a. necessary for entering into, or performance of, a contract between the data subject and controller;

b. authorised by the relevant law to which the controller is subject and which also lays down suitable measures to safeguard the individual's rights and freedoms and legitimate interests; or

c. based on the individual's explicit consent.

193. In the cases referred to in a. and c., you must implement suitable measures to safeguard the individual's rights and freedoms and legitimate interests, In the cases referred to in a. and c., you must implement suitable measures to safeguard the individual's rights and freedoms and legitimate interests, including the right to obtain human intervention on the part of the controller, so that the individual can express their point of view and contest the decision.

194. If you're using special category personal data you can only carry out processing described in Article 22(1) if:
    a. you have the individual's explicit consent; or
    b. the processing is necessary for reasons of substantial public interest.

What else do we need to consider?

195. Because this type of processing is considered to be high-risk the DPJL requires you to carry out a Data Protection Impact Assessment (DPIA) to show that you have identified and assessed what those risks are and how you will address them.

196. As well as restricting the circumstances in which you can carry out solely automated individual decision-making, the DPJL also:
    a. requires you to give individuals specific information about the processing;
    b. obliges you to take steps to prevent errors, bias and discrimination; and
    c. gives individuals rights to challenge and request a review of the decision.

197. These provisions are designed to increase individuals' understanding of how you might be using their personal data. You must:
    a. provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
    b. use appropriate mathematical or statistical procedures;
    c. ensure that individuals can:
    d. obtain human intervention;
    e. express their point of view; and
    f. obtain an explanation of the decision and challenge it;
    g. put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors;
    h. secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.

What if Art.38 doesn't apply to our processing?

198. Art.38 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects. If your processing does not match this definition then you can continue to carry out profiling and automated decision-making.

199. However, you must still comply with the principles set out in Art.8 of the DPJL in that:
    a. You must identify and record your lawful basis for the processing.
    b. You need to have processes in place so people can exercise their rights.
    c. Individuals have a right to object to profiling in certain circumstances. You must bring details of this right specifically to their attention.

MORE INFORMATION

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

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

202. 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.

203. 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