EIRs Guidance

Regulation 11: Personal Data

Briefing

Scottish Information Commissioner

Contents

Glossary and abbreviations

Term used	Explanation
Data controller	A natural or legal person who determines the purposes for which (and the means by which) personal data are processed. Data controllers must comply with the data protection principles. Every Scottish public authority subject to the EIRs is a data controller.
Data protection principles	The six principles in Article 5 of the GDPR which data controllers must comply with. For the purposes of the EIRs, principle a. is the most important. This requires personal data to be processed lawfully, fairly and in a transparent manner.
Data subject	A living individual who can be identified, directly or indirectly, by information.
DPA 2018	Data Protection Act 2018. The Act came into force on 25 May 2018.
EIRs	Environmental Information (Scotland) Regulations 2004
FOI	Freedom of Information
FOISA	Freedom of Information (Scotland) Act 2002
GDPR	EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR came into force in 2018 (no longer applicable in the UK).
ICO (UK) Information Commissioner	The Commissioner responsible for enforcing the UK GDPR and the DPA 2018 throughout the UK, including Scotland. This is a different person from the *Scottish* Information Commissioner.
Personal data	Any information relating to a data subject by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject.
Processing	Defined very widely. It means any operation (or set of operations) performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure (including dissemination or transmission), alignment or combination, restriction, erasure or destruction. "Processing" personal data in response to an EIRs request entails disclosing personal data into the public domain.
SAR/Subject access request	A request made under Article 15(1) of the UK GDPR (or section 45(1)(b) of the DPA 2018) for a person's own personal data.
Special categories of data	Data relating to the data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, criminal convictions and offences or related security measures, and identifying genetic and biometric data. The processing of the special categories of personal data is subject to much tighter restrictions than other personal data.
SIC	The Scottish Information Commissioner, staff of SIC (depends on context)
The Commissioner	The Scottish Information Commissioner
The Section 60 Code	The Scottish Ministers' Code of Practice on the Discharge of Functions by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004 (December 2016 version)
UK GDPR	The version of the GDPR which now applies in the UK following Brexit, i.e. the GDPR as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

Regulation 11

The main points

1. Regulation 11 of the Environmental Information (Scotland) Regulations 2004 (the EIRs) sets outs when personal data can and cannot be disclosed under the EIRs. Regulation 10(3) makes it clear that, where a request for environmental information includes personal data, the personal data must not be made available (i.e. disclosed) otherwise than in accordance with regulation 11.

2. Personal data must not be disclosed if it is:

   (i) the personal data of the person requesting the information (regulation 11(1));

   (ii) the personal data of a third party – and other conditions apply (regulation 11(2)).

3. The exceptions in regulation 11 regulate the relationship between the EIRs, the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (the DPA 2018). (See **Appendix 1: Resources** for links to the UK GDPR and the DPA 2018.)

4. Remember that regulation 11 covers personal data which also falls within the definition of environmental information. There is a separate exemption in section 38 of the Freedom of Information (Scotland) Act 2002 (FOISA) for personal data which is not environmental information. (See **Appendix 1: Resources** for a link to the Commissioner's guidance on section 38 of FOISA.)

5. The GDPR and the DPA 2018 came into effect on 25 May 2018 and made a lot of changes to data protection laws in the UK (and the rest of Europe). Following Brexit, the UK is no longer subject to the GDPR, but is subject to the "UK GDPR". Anyone using this guidance should be aware that some of the cases and decisions referred to were decided under with the Data Protection Act 1998 (no longer in force). Although many of the key principles are the same under the new rules, care is required to ensure that the new regime is being complied with. This guidance is being updated as new decisions are issued (decisions issued under the new rules are highlighted in green in the Appendix) and as new guidance on data protection is published by the (UK) Information Commissioner (the ICO). (The ICO enforces and regulates data protection throughout the whole of the UK, including Scotland. Detailed guidance on data protection is available from the ICO.)

Brexit

6. The ICO's website has guidance on the effects exiting the EU might have on data protection laws in the UK after Brexit – see **Appendix 1: Resources** for a link.

Duration

7. Regulation 11 applies regardless of how old the information is. In practice, this will be limited because the provisions can only be applied if the information relates to *living* individuals. The exemptions do not apply to personal information of deceased people.

Regulation 11 and the public interest test

8. The exceptions in regulation 11 are generally absolute, which means that they are not subject to the public interest test. However, in two specific situations, the exception in

regulation 11(2) is subject to the public interest test. This means that, even if the exception applies, the personal data must be disclosed unless, in all the circumstances of the case, the public interest in making the personal data available is outweighed by the public interest in maintaining the exception. This is explained in more detail below.

Regulation 11 and neither confirm nor deny

9. Where any of the exceptions in regulation 11 applies, a public authority can refuse to reveal whether personal data exists or is held by it (regardless of whether it actually holds the personal data), provided it is satisfied that revealing whether the personal data exists or is held would, of itself, involve making personal data available contrary to regulation 11. (See regulation 11(6) and **Appendix 1: Resources** for a link to decisions issued by the Commissioner on this point.)

Background

The EIRs, the UK GDPR and the Data Protection Act 2018

Introduction

10. The UK GDPR and the DPA 2018 govern how the personal data of living people should be handled by organisations, while also providing individuals with a number of rights, including the right to access their own personal data and the right to object to organisations processing their personal data.

11. The EIRs, on the other hand, provide a general right to the information held by public authorities, providing that the information is not excepted from disclosure. Regulation 11 of the EIRs is where the UK GDPR, the DPA 2018 and the EIRs meet. It tells us when personal data can and can't be disclosed in response to an EIRs request.

12. Data protection laws changed on 25 May 2018 when the GDPR and DPA 2018 came into force. Following Brexit, the UK is no longer subject to the GDPR, but is subject to the UK GDPR. This briefing focusses on the interaction between data protection and FOI, so does not give guidance on the UK GDPR or the DPA 2018. Detailed guidance on this legislation is available from the ICO, who enforces data protection laws throughout the whole of the UK. Contact details for the ICO are provided below – see **Appendix 1: Resources.**

Processing for law enforcement purposes

13. While the UK GDPR and Part 2 of the DPA 2018 apply to most uses of personal data, Part 3 of the DPA 2018 contains specific rules for handling personal data for law enforcement purposes. Law enforcement purposes are defined in section 31 of the DPA 2018 as:

    the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

14. The rules in Part 3 of the DPA 2018 don't apply to all Scottish public authorities which are subject to FOISA: they only apply if the Scottish public authority is a "competent authority", which means it must be either:

    (i) listed in Schedule 7 to the DPA 2018 – the list includes the Scottish Ministers, Police Scotland, the Scottish Criminal Cases Review Commission, the Lord Advocate and the Scottish Information Commissioner – or

    (ii) has statutory functions for any of the law enforcement purposes.

15. Responding to requests for data processed for law enforcement purpose won't, of itself, involve the processing of data for law enforcement purposes. This means that it's the GDPR and Part 2 of the DPA 2018 (rather than Part 3) which will determine whether personal data can be disclosed under the EIRs.

What is personal data?

16. "Personal data" is defined in section 3 of the DPA 2018 (and Article 4 of the UK GDPR) as any information relating to an identified or identifiable living individual, who can be identified, directly or indirectly, in particular by reference to:

    (i) an identifier such as a name, an identification number, location data or an online identifier, or

    (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

17. In most cases, it will be easy to tell if information is personal data. The two main elements of personal data are that:

    (i) the information must "relate to" a living person (information will "relate to" a person if it is about them, linked to them, has biographical significance for them, is used to inform decisions affecting them or has them as its main focus) and

    (ii) the person must be identified – or identifiable – from the data or from the data and other information. Information requests about a living individual's salary, expenses or health will be their personal data: the individual can be identified from those data and the information relates to the individual.

18. However, in some cases, it can be more difficult to tell whether information is personal data. For example, is CCTV footage always the personal data of the individuals appearing in it? The ICO has published guidance, entitled "What is personal data", which can help public authorities decide whether the information they are considering is personal data (see **Appendix 1: Resources** for a link to that guidance and to decisions from the Commissioner on this point).

19. The right to ask for personal data applies to personal data held in any format and includes manual unstructured data held by authorities subject the EIRs (see section 24 of the DPA 2018).

Can numbers or statistics be personal data?

20. Often, requests made under the EIRs are for statistics. For example:

    (i) How many criminals were prosecuted last year for wildlife crime?

    (ii) How many neighbours objected to a planning application?

    (iii) How many children were injured as a result of the chemical spill at school?

21. It can be difficult to know whether disclosing numbers will lead to living people being identified. If it does, then the information will be their personal data.

22. The Court of Justice of the European Union looked at the question of identification in *Breyer v Bundesrepublik Deutschland* (see **Appendix 1: Resources** for a link to the judgment). The Court said that the correct test to consider is whether there is a realistic prospect of someone being identified. In deciding whether there is a realistic prospect of identification, account can be taken of information in the hands of a third party. However, there must be a realistic causal chain – if the risk of identification is "insignificant", the information won't be personal data.

23. Although this decision was made before the GDPR, UK GDPR and the DPA 2018 came into force, the Commissioner expects that the same rules will apply. Although no longer applicable in the UK, recital (26) of the GDPR bears this out – and confirms that data should be considered anonymous (and therefore no longer subject to the GDPR) when the data subject(s) is/are no longer identifiable.

24. Public authorities responding to requests for numbers will therefore have to determine whether members of the public would be able to identify individuals from the statistics if they are disclosed. It's important that the scope for anonymisation is considered when handling requests which capture personal data. Scotland is a geographically (and therefore demographically) diverse country, so authorities will need to take account of matters such as population size and population density when deciding if disclosure would lead to individuals being identified.

25. It's worth remembering that, just because information is personal data, it does not mean that it cannot be disclosed under the EIRs. Regulation 11 tells us when it is possible to disclose personal data without breaching the UK GDPR/DPA 2018.

The special categories of personal data

26. If information falls into one of the special categories of personal data, it's very unlikely that the information can be disclosed without breaching the UK GDPR/DPA 2018. This means it's important for public authorities to know what types of personal data fall within the "special categories".

27. Article 9 of the UK GDPR says that personal data falls within the special categories of personal data if it reveals information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership
- genetic or biometric data (if processed for the purpose of uniquely identifying an individual)
- health;
- sex life;
- sexual orientation.

28. Section 10 of the DPA 2018 makes it clear that information should be treated in a very similar way to the special categories if it is about:

- criminal convictions
- offences
- related security measures.

29. Paragraphs **71** to **73** look at how to respond to EIRs requests for third party special category data.

Regulation 11(1): the requester's own personal data

30. When someone makes a request under the EIRs for their own personal data, the data is excepted from disclosure under regulation 11(1) of the EIRs. This is an absolute provision: the public authority does not have to go on to consider whether the public interest in making the personal data available is outweighed by the public interest in not making it available.

31. The reason this EIRs exception exists is that Article 15 of the UK GDPR (and, in the case of law enforcement processing, section 45 of the DPA 2018) gives us the right to access our personal data.

32. These routes are more appropriate when we want to access our own personal data. If information is disclosed under the EIRs, it's disclosed into the public domain. Disclosing personal data under the UK GDPR or DPA 2018 ensures that it's only disclosed only to the data subject; their personal data is kept private.

What do I do if someone asks for their own personal data under the EIRs?

33. If someone asks for their own personal data under the EIRs, it will be excepted from disclosure under regulation 11(1).

34. There's nothing in the EIRs which requires public authorities to treat this sort of request as a request under Article 15 of the UK GDPR/or section 45 of the DPA 2018. However, under regulation 9 of the EIRs (the duty to provide advice and assistance), it will be good practice to go on to consider any EIRs request for an individual's own personal data as subject access requests in the normal way. This will include, if necessary, confirming the identity of the requester.

35. Guidance on responding to subject access requests is available from the (UK) Information Commissioner's website. See **Appendix 1: Resources** for a link to the website.

36. Even where the authority treats an EIRs request as a subject access request, it must issue a formal refusal notice under regulation 13 of the EIRs. Failure to do this would be a breach of the EIRs.

What if a third party is acting on behalf of the data subject?

37. Regulation 11(1) will also apply if a request is made for a third party's personal data by an individual acting on behalf of that third party. (For example, where a parent makes a request on behalf of a young child or a solicitor makes a request on behalf of their client.) The rule in paragraph 36 about issuing a refusal notice will also apply to these types of requests.

38. Authorities should take appropriate steps to confirm that the requester is acting on behalf of the data subject. This might include asking to be provided with a mandate from the person on whose behalf the request is being made.

What if the information is a mixture of the requester's and third party data?

39. If the personal data is difficult to separate, the appropriate way forward is to consider the information under the provision in regulation 11(1). For example, if someone asks for a complaint made by a neighbour about the requester, the letter will contain the personal data of the neighbour and the person complained about. It will be difficult to separate the two.

Treating the request as a request under the UK GDPR/the DPA 2018 will allow the public authority to consider whether disclosing any of the third party's personal data would adversely affect their rights and freedoms in line with Article 15(4) of the UK GDPR/section 45(4)(e) of the DPA 2018.

40. Again, the authority should issue a refusal notice under regulation 13 of the EIRs.

41. However, if the personal data of the third party is clearly distinct from the other personal data (for example, if a document has been separated into distinct sections on the different parties), then the third party data should be separately dealt with under the provision in regulation 11(2) of FOISA.

42. See **Appendix 1: Resources** for a link to the guidance issued by the ICO on this and for examples of decisions issued by the Commissioner which consider regulation 11(1) and its FOISA equivalent, section 38(1)(a).

Third party data: regulation 11(2)

Introduction

43. Regulation 11 is contains three different exceptions (referred to in regulation 11(2) as the first, second and third conditions).

44. While regulation 11(1) focuses on the personal data of the person asking for the information, regulation 11(2) focuses on the personal data of third parties. Some people think that third party personal data can never be disclosed under the EIRs, but that's not the case.

45. There are three situations where third party personal data is exempt under regulation 11(2). These are where:

    (i) disclosing the personal data would contravene any of the data protection principles in Article 5(1) of the UK GDPR ("the first condition");

    (ii) disclosing the personal data would contravene Article 21 of the UK GDPR (right to object to processing) and the public interest favours withholding the data ("the second condition"); and

    (iii) the data subject would not be entitled to be given the personal data if they made a subject access request for it under Article 15(1) of the UK GDPR or section 45(1)(b) of the DPA 2018 and the public interest favours withholding the data "(the third condition").

46. All three are all considered in more detail below.

Third party data: data protection principles (the first condition)

47. Personal data is exempt from disclosure if disclosure would contravene any of the data protection principles in Article 5(1) of the UK GDPR and in section 34(1) of the DPA 2018.

48. The exemption is absolute, so is not subject to the public interest test.

49. There are six data protection principles. Generally, the only principle which is likely to be relevant when considering whether to disclose personal data in response to an EIRs request is the "lawfulness, fairness and transparency" principle.[1]

50. Article 5(1)(a) states that

    personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

51. The reference to "transparency" in Article 5(1)(a) recognises the importance of letting data subjects know how, and determine the purposes for which, their personal data will be used.

Lawful processing

52. Article 6 of the GDPR says that processing shall be lawful only if:

    (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

    (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

    (c) processing is necessary for compliance with a legal obligation to which the controller is subject;

    (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

    (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

    (f) **processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.**

53. In practice, given the very narrow definition of "consent", when considering whether personal data can be disclosed under the EIRs, condition (f) (in bold) is the only condition which is likely to apply.[2]

---

[1] Principle (b), the purpose limitation principle, requires personal data to be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. This is similar to second data protection principle in the Data Protection Act 1998, which was repealed by the DPA 2018. Public authorities sometimes argued that disclosing personal data in response to an EIRs request would breach the second data protection principle. However, the ICO took the view that the second data protection principle did not prevent a public authority disclosing information under FOI provided the disclosure of the personal data was lawful, fair and transparent and provided the information was not exempt under any other FOI exemption. The Commissioner expects that the ICO will take the same view as regards principle b. in Article 5.

Condition (f). – the legitimate interests gateway

60. Condition (f) allows personal data to be processed where:

> *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*

> Although Article 6 does not usually allow public authorities to rely on condition f. when processing personal data, authorities can rely on condition f. when responding to EIRs requests.
>
> Regulation 11(7) of the EIRs specifically says:
>
> *In determining, for the purposes of this regulation, whether the lawfulness principle in Article 5(1)(a) of the UK GDPR would be contravened by the disclosure of information, Article 6(1) of the UK GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted.*

61. In the context of the EIRs, condition (f) can be split into three separate questions (see **Appendix 1: Resources** for a link to a Supreme Court judgment on this):

- Does the person making the information request have a legitimate interest in obtaining the personal data?
- If yes, is the disclosure of the personal data necessary to achieve that legitimate interest?
- Even if the processing is necessary to achieve that legitimate interest, is that overridden by the interests or fundamental rights and freedoms of the data subject(s)?

Does the person making the information request have a legitimate interest in obtaining the personal data?

62. When assessing whether a requester has a "legitimate interest", it is good practice for public authorities to ask the requester why they want the information (unless it is already clear from the information request or from previous correspondence with the requester). Authorities should remember, however, that requesters aren't required to explain why they want the information if they don't wish to do so.

63. In some cases, the legitimate interest might be personal to the requester, e.g. they might want the information in order to bring legal proceedings. For most requests, however, there are likely to be wider legitimate interests, such as scrutiny of the actions of public bodies or public safety. See **Appendix 1: Resources** for some decisions issued by the Commissioner which consider whether the requesters had legitimate interests. (Note that

---

[2] Previous guidance issued by the Commissioner also suggested that condition (a) – consent – might also be relevant. However, in practice, given that consent must be freely given, specific, informed and unambiguous; that the authority must be able to demonstrate that consent has been given; and that consent must be capable of being withdrawn, it is unlikely that an authority will be able to rely on condition (a). The views of the data subject (or data subjects) will, however, be relevant when considering condition (f).

some of these decisions were issued before the GDPR, the DPA 2018 and UK GDPR came into effect.)

Is the disclosure of the personal data necessary to achieve that legitimate interest?

64. "Necessary" means "reasonably" rather than absolutely or strictly necessary. When considering whether disclosure would be necessary, public authorities should consider whether the disclosure is proportionate as a means and fairly balanced as to the aims to be achieved, or whether the requester's legitimate interests can be met by means which interfere less with the privacy of the data subject(s).

65. Authorities will need to consider whether it is necessary to disclose the personal data in full in order to fulfil the requester's legitimate interest, or whether there is any other information available to the requester which would meet these aims while interfering less with the interests or fundamental rights and freedom of the data subjects. See **Appendix 1: Resources** for examples of decisions looking at whether disclosure is necessary to satisfy the requester's legitimate interest. (Again, note that some of these decisions were issued before the GDPR, the DPA 2018 and UK GDPR came into force.)

Even if the processing is necessary to achieve that legitimate interest, is that overridden by the interests or fundamental rights and freedoms of the data subject(s)?

66. Even if the processing is necessary for the legitimate interest of the requester, do the interests or fundamental rights and freedoms of the data subject(s) override this interest?

67. This involves a balancing exercise between the interest of the requester and the interests of the data subject(s). Only if the legitimate interest of the requester outweighs the interests of the data subjects can the personal data be disclosed. Disclosure will always involve some intrusion of privacy. However, that intrusion will not always be unwarranted and public authorities must consider each request on a case by case basis.

68. Although no longer applicable in the UK, recital (47) of the GDPR makes it clear that much will depend on the reasonable expectations of the data subject(s).

69. These are some of the factors which public authorities should consider:

- Does the information relate to an individual's public life (their work as a public official or employee) or to their private life (their home, family, social life or finances)? Information about an individual's private life deserves more protection than information about their public life. The seniority of their position and whether they have a public facing role will also be relevant. The more senior a person is, the less likely it is that disclosing information about their public duties will override the interests of the person who made the request. Information about a senior official's public life should also generally be disclosed unless it also reveals details of the private lives of other people, such as their family.

- Would the disclosure cause harm or distress? Disclosing information about an individual's private information or family life may cause distress (and it's worth remembering that the exemption must be interpreted in line with Article 8 of the European Convention on Human Rights, which states that everyone has the right to respect for his private and family life, his home and his correspondence – see **Appendix 1: Resources** for a link to the ECHR). Some disclosures could also risk the fraudulent use of the disclosed information (e.g. details of bank accounts) or pose a security risk (e.g. addresses, work locations or travel plans where there is a risk of harassment or other credible threat to the individual). In these cases, the interests of

the data subject(s) are likely to override the interests of the requester. However, the focus should be on the harm or distress in a personal, as opposed to professional, capacity. (Authorities concerned about the risk of harm may also wish to consider the exception in regulation 10(5)(a) of the EIRs which, amongst other things, covers public safety) – see **Appendix 1: Resources** for a link to the Commissioner's guidance on that exception.)

- Whether the individual has objected to the disclosure. Even where the data subject has objected to the disclosure, this isn't necessarily the end of the matter. It is a factor to take into account, but it doesn't automatically mean that the interests of the data subject will override the interests of the requester.

Children

70. Particular care needs to be taken when responding to a request for a child's personal data. Article 6 and recital 38 (still relevant, if no longer applicable in the UK) of the GDPR make it clear that particular care must be taken to protect the rights of children: children may be less aware of the risks, consequences and safeguards involved in processing. See **Appendix 1: Resources** for a decision relating to the personal data of children.

Conditions for disclosing special category personal data

71. Article 9 of the UK GDPR only allows special category personal data to be processed in very limited circumstances. (This is unsurprising, given the nature of data falling within this definition – see **Appendix 1: Resources** for a link to the ICO's guidance on special category data.)

72. Schedule 1 to the DPA 2018 contains a very wide range of conditions which allow authorities to process special category data (including data relating to criminal convictions, offences or related security measures) in relation to matters such as employment, social security and social protection; health or social care; public health; research.

73. However, despite the wide range of conditions in Schedule 1 to the DPA 2018, it is likely that, for the purposes of FOI, the only situations where it is likely to be lawful to disclose third party special category data in response to an information request are where, in line with Article 9 of the UK GDPR, the personal data has manifestly been made public by the data subject (condition (e)).[3] Any public authority relying on this condition must be certain that the disclosure was made with the intention of making the special category data public.

Criminal offence data

74. Criminal convictions and offences data are given special status in the UK GDPR: Article 10 makes it clear that this type of personal data can only be processed under the control of official authority or when the processing is authorised by domestic (UK) law providing for appropriate safeguards for the rights and freedoms of data subjects.

75. Criminal offence data (see section 11(2) of the DPA 2018) includes personal data relating to:

- the alleged commission of offences;

[3] Condition (a) also allows special category data to be processed where the data subject has given explicit consent to the disclosure of the information. However, in practice, given that consent must be freely given, specific, informed and unambiguous; that the authority must be able to demonstrate that consent has been given; and that consent must be capable of being withdrawn, it is unlikely that an authority will be able to rely on condition (a) to disclose special category data in response to a FOISA request.

- proceedings for an offence committed or alleged to have been committed by the data subject; or
- the disposal of such proceedings, including sentencing.

76. Criminal offence data can only be processed if one of the stringent conditions in Parts 1 to 3 of Schedule 1 to the DPA 2018 can be met (section 10(5) of the DPA 2018). Parts 1 to 3 contain a wide range of conditions which allow personal data to be disclosed, but it is difficult to find any which would allow a public authority to disclose criminal offence data into the public domain in response to an EIRs request. Consequently, it is unlikely that it will ever be lawful to disclose criminal offence data under the EIRs.

77. See **Appendix 1: Resources** for a link to a decision from the Commissioner on this point.

Fairness

78. Processing of personal data must be fair as well as lawful, so fairness needs to be considered separately.

79. Guidance issued by the ICO in relation to the UK GDPR states that fairness means public authorities should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

80. Public authorities take the following into account (these are similar to the issues to be considered when looking at Article 6 – see above):

- Whether the individual expects their role to be subject to public scrutiny. Consideration should be given to the person's seniority, whether they have a public profile and whether their role requires a significant level of personal judgement and individual responsibility.
- Whether any distress or damage would be caused to the data subject as a result of the disclosure;
- Any express refusal by the data subject;
- Whether the information relates to the data subject's public or private life. A person's private life is likely to deserve more protection.

81. As noted above, if a condition in Article 6 to the UK GDPR (and Article 9 of the UK GDPR and Schedule 1 to the DPA 2018 if the request is for special category data) permits data to be processed, the disclosure will probably also be fair, although it is good practice for public authorities to consider this point separately.

Lawfulness

82. If there are no conditions which would allow the personal data to be processed, the disclosure of the data will be unlawful.

83. Where a condition permits the data to be processed, it is likely that the disclosure will be otherwise lawful. Disclosure might still be unlawful if it would, for example, breach a confidence. In these cases, other exceptions in the EIRs may apply.

Names of public authority employees

84. Information requested under the EIRs often includes the names of public authority employees, for example the author of a document, the senders or recipients of internal emails or the attendees at a meeting. Authorities should follow the general approach outlined in paragraphs **62** to **69** above to decide whether names can be released.

85. It's good practice for authorities to tell employees what their general policy is about releasing names. However, given that so much will depend on the seniority of the member of staff, their role and the context of the request, authorities shouldn't adopt a blanket policy.

86. A public authority may have a policy of disclosing information about senior members of staff above a certain grade, but if disclosing a name would, for example, cause the employee harm or distress, for example by exposing them to threats or reprisals, the information may have to be withheld. (Of course, the context might make disclosure less likely to be harmful – if all the information shows is that a member of staff forwarded an email to someone at the request of a third party, disclosure is unlikely to cause harm.)

87. On the other hand, it may be necessary to disclose information about a relatively junior member of staff, depending on the specific nature and responsibilities of their post. See **Appendix 1: Resources** for a link to a decision on this point.

Contact details

88. Similar considerations may apply to other details of individual staff, for example, direct line or mobile telephone numbers. As with other personal data, private (as opposed to work) numbers are more likely to merit protection.

89. Where staff details are being withheld, it's important to keep redactions to the minimum necessary to remove the risk of identification. This is particularly relevant where valuable context would be lost otherwise – consider, for example, whether the full email address needs to be redacted or just that part with the employee's name (the rest is still likely to help the requester understand where the communications in question originated and were sent to).

Third party data: Article 21 of the UK GDPR (the second condition)

90. Personal data is excepted from disclosure if disclosing the data to a member of the public would contravene Article 21 of the UK GDPR (regulation 11(2) read with regulation 11(3B)).

91. Article 21 of the UK GDPR gives data subjects the right to object to a data controller processing their data. Where a notice has been given, the controller can no longer process the data unless there are compelling grounds for doing so which override the interests, rights and freedoms of the data subject.

92. If a data subject has exercised their rights under Article 21, their personal data will be exempt from disclosure under the EIRs, unless the public interest favours disclosure – see below.

93. It should be noted that Article 21 of the UK GDPR permits allows data subjects to object to processing at any point. This means that a data subject can object *after* an information request has been made. If public authorities receive an information request for third party data, they will need to consider whether, as data controllers, they are required to alert the data subject that the request has been made and to give him/her an opportunity to object to the disclosure of the information.

94. Additional guidance on seeking comments from third parties (including data subjects) can be found in the Scottish Ministers' Section 60 Code of Practice. See **Appendix 1: Resources** for a link to the Code.

The public interest test

95. This is one of the few cases where regulation 11 is subject to the public interest test.

96. This means that, even where disclosing the personal data would be contrary to Article 21 of the UK GDPR, the authority must go on to consider the public interest in relation to the personal data. The public interest test assesses whether, in all the circumstances of the case, the public interest is better served by disclosing or withholding the personal data.

97. The EIRs do not define the term "public interest", but it has been described as "something which is of serious concern and benefit to the public". It has also been said that the public interest does not mean what is of interest **to** the public, but what is in the interest **of** the public.

98. The Commissioner has produced separate guidance to assist with the consideration of the public interest test. See **Appendix 1: Resources**.

Third party data: subject access request (the third condition)

99. Article 15(1) of the UK GDPR gives data subjects the right to access their personal data, subject to a number of exemptions (see sections 15, 16 and 26 of, and Schedules 2, 3 and 4 to, the DPA 2018).

100. Where personal data is being processed by competent authorities for law enforcement purposes under Part 3 of the DPA 2018, section 45(1)(b) of the DPA 2018 gives data subjects the same right, subject to the exemptions in section 45(4) of the DPA 2018.

101. The exemptions in the UK GDPR and the DPA 2018 cover matters like national security; crime; health, education and social work records; and the exercise of some regulatory functions.

102. Regulation 11(2), read in conjunction with regulation 11(4A), exempts personal data from disclosure if, as a result of an exemption, the data subject would not be given the data if they made a request for it. This is, however, subject to the public interest test.

The public interest test

103. This is the other situation where regulation 11 is subject to the public interest test. So, even if the data subject would not be entitled to get the information under Article 15(1) of the UK GDPR or under section 45(1)(b) of the DPA 2018, the authority must disclose the personal data unless the public interest in maintaining the exemption outweighs the public interest in disclose it.

104. See paragraphs **95** to **98** above for more information on the public interest test.

Appendices

Appendix 1: Resources

SIC Decisions

Note: Some of these decisions were issued before the GDPR, DPA 2018 and UK GDPR came into force. The decisions published under the new legislation are highlighted in green.

Reference	Decision number	Authority	Summary
Neither confirm nor deny Paragraph 9	039/2011	Scottish Ministers	The Ministers were asked about representations made to them by Prince Charles on certain planning developments and on red squirrels. The Ministers refused to confirm or deny whether they held any information falling within the scope of the request, but we ordered them to tell the requester whether they held the information.
Neither confirm nor deny Paragraph 9	277/2013	Scottish Environment Protection Agency	SEPA were asked to confirm that a named individual was a SEPA employee. In the circumstances, we were satisfied that revealing whether it held the information would breach the first data protection principle.
Identifiability Paragraph 18	016/2020	Moray Council	This was a request for the names of the two separate degrees held by candidates shortlisted for interview for a particular post. The Council argued that the information was the personal data of the candidates. We didn't agree that there was a significant risk of identification, given that the degree names on their own wouldn't relate to an individual and the candidates could come from anywhere.
Statistics Paragraph 24	005/2009	Aberdeenshire Council	The Council was asked about the number of weapons seized from local schools, including the names of the schools, the types of weapons seized, the age and sex of the pupils involved, what sanction they had received and whether the police had been called. The requester made it clear that he was

Reference	Decision number	Authority	Summary
			not interested in identifying the children. The Council answered all of the requester's questions, but refused to disclose the names of the schools involved on the basis that disclosing this final piece of the jigsaw would lead to the children being identified. The requester disagreed, arguing that a secondary school would typically have hundreds of pupils in one year, and a primary school dozens. When we looked at the actual school rolls, and took into account the information the Council had already disclosed, the actual number of children who could be one of the pupils a weapon had been seized from was much lower. We concluded that disclosure would lead to identification and that the names of the schools had to be treated as personal data.
Statistics Paragraph 24	014/2009	Chief Constable of Strathclyde Police	The Police were asked for the numbers of registered sex offenders (RSOs) in specified postcode areas. We initially agreed with the Police that disclosing the numbers would lead to individual RSOs being identified. The requesters appealed to the Court of Session and, on review, and in the light of guidance from the Court of Session, we came to the conclusion that there was insufficient evidence to conclude that individuals could be identified by the disclosure of the statistics. We accepted that, where a person already knows that an individual is an RSO, disclosure of the statistics would permit that person to identify the individual RSO as one of a statistical cohort. However, this in itself would not make the statistical information personal data; it is not the disclosure of the statistics which would identify the individual.
Statistics	156/2011	University of Glasgow	Here, we considered whether statistical information about students who had

Reference	Decision number	Authority	Summary
Paragraph 24			graduated from the University was personal data. The University provided examples of how individual graduates could be identified by the triangulation of the data sought, information published in the media about graduations and other publicly available information. We accepted that it was possible to identify individual graduates through a combination of these information sources (even though the route to identification was complex) and that the statistical information was personal data.
Statistics Paragraph 24	012/2019	Dumfries and Galloway Health Board	The requester wanted to know how many psychologists had undertaken data protection training. Given the small numbers of psychiatrists, we were satisfied that individual could be identified and that the numbers were personal data.
Statistics Paragraph 24	019/2019	Lothian Health Board	The Board was asked for the number of operations cancelled for non- clinical reasons, broken down by reason. The authority withheld data where the figures were “five or less” on the basis that it disclose could lead to individuals being identified. We disagreed: the request was for figures broken down by year, the population of the health board area was around 800,000 and the reasons given for cancellation were generic. This meant that the figures were unlikely to lead to individuals being identified.
Statistics Paragraph 29	151/2019	Police Scotland	This related to a request for the number of homophobic hate crimes against police officers, reported to the Procurator Fiscal in Wick in 2017 and 2018. Police Scotland refused to say how many, claiming that it would lead to individuals being identified: they noted the small geographical area (and population), the number of police officers who could be involved and the

Reference	Decision number	Authority	Summary
			fact that many police officers would be known to the community in such a location. While noting all of these factors, we didn't accept that disclosing the number of relevant offences (alone) would make a meaningful contribution to identifying the individuals in question – bearing in mind that the commission of a hate crime wouldn't necessarily bear any relation to particular characteristics of the victim.
Necessary Paragraph 65 Legitimate interests Paragraph 63	029/2016	Glasgow City Council	The Council was asked about a complaint which had been made about the removal of a tree. We concluded that the requester had legitimate interests in the personal data contained in the complaint, but that disclosure was not "necessary" for the purposes of her legitimate interests.
Legitimate interests Paragraph 63 Necessary Paragraph 65 Unwarranted prejudice Paragraph 69	128/2015	City of Edinburgh Council	The requester asked the Council for copies of complaints received by the Council about the chimes at a church. Some of the information named individual Council employees. We agreed that the requester had a legitimate interest in obtaining this information and that disclosure was necessary to achieve those interests. However, we concluded that disclosing details about the names of the employees would cause them unwarranted prejudice: they were not senior members of staff and did not have public-facing roles. Complaints about the clock had attracted attention in the national media: disclosing names would lead to unwarranted focus on them.
Legitimate interests Paragraph 63 Necessary Paragraph 65	016/2019	Glasgow City Council	The Council was asked about its correspondence with the owners of a building which he understood to be subject to a dangerous buildings notice. The Council disclosed the correspondence but withheld names and contact details. We found that,

Reference	Decision number	Authority	Summary
			while the requester had a legitimate interest in the names and contact details, disclosure was not necessary for his purposes.
Criminal offence data	046/2019	Police Scotland	We agreed that the names and dates of birth of offenders who had breached home detention curfews was criminal offence data and that there were no conditions in the DPA 2018 which would allow the data to be disclosed.
Employee names Paragraph 87	055/2007	Highland Council	This concerned a request for the qualifications of an employee. The employee's post was not particularly senior, but the specific nature and responsibilities of their post, which involved providing advice to the Council on matters of public safety, gave rise to expectations of transparency and accountability. We concluded that their qualifications should be disclosed.
Section 38(1)(b) Paragraph 70	098/2019	Stirling Council	The Council was asked for details of exam grades of a named school, broken down by subject and grade. The Council disclosed some information, but refused to disclose a more detailed breakdown as it believed disclosure would breach the data protection principles. We upheld the Council's position in relation to the more detailed information (which we accepted was personal data), focusing in this case on the particular care that must be taken when looking at a child's personal data (Article 6 and recital 38 of the GDPR).

All of the Commissioner's decisions are available on the Commissioner's website. To view a decision, go to www.itspublicknowledge.info/decisions and enter the relevant decision number (e.g. 032/2020).

If you don't have access to the internet, contact our office to request a copy of any of the Commissioner's briefings or decisions. Our contact details are on the final page.

Other resources

Paragraph	Resource	Link
The main points	ICO website: Data protection and Brexit	https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/
3	United Kingdom General Data Protection Regulation Keeling Schedule	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf
4	(SIC) FOISA Exemption Guidance Section 38: Personal information	http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section38/section38briefing2018.aspx
3	Data Protection Act 2018	http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
12 35	(UK) Information Commissioner contact details	The Information Commissioner Wycliffe House Water Lane Wilmslow SK9 5AF Tel. 0303 123 1113 Email: casework@ico.org.uk The Information Commissioner's Office – Scotland 45 Melville Street Edinburgh EH3 7HL Tel: 0131 244 9001 Email: scotland@ico.org.uk
18	(ICO) Guidance: What is personal data?	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
22	Breyer v Bundesrepublik Deutschland C-582/14	http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5a43ad9a18e97498382489c6c7fea9de9.e34KaxiLc3qMb40Rch0SaxyKbhf0?text=&docid=184668&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1077604

Paragraph	Resource	Link
42	(ICO) Right of access detailed guidance	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/
61	South Lanarkshire Council v Scottish Information Commissioner	https://www.supremecourt.uk/cases/docs/uksc-2012-0126-judgment.pdf
69	European Convention on Human Rights	http://www.echr.coe.int/Documents/Convention_ENG.pdf
69	(SIC) EIRs exceptions guidance: Regulation 10(5)(a) of the EIRs	http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/EIRsexceptionbriefings/Regulation10(5)(a)/Regulation10(5)(a)InternationalRelationsNationalSecurity.aspx
71	(ICO) Guidance on special category data	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/
95	Section 60 Code (December 2016 version)	https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiuy8rr_9_bAhXkAMAKHUlIA8UQFggsMAE&url=https%3A%2F%2Fbeta.gov.scot%2Fpublications%2Ffoi-eir-section-60-code-of-practice%2FFOI%2520-%2520section%252060%2520code%2520of%2520practice.pdf&usg=AOvVaw1rlIGJxmp-xj08JBg9rJna
98	(SIC) EIRs Public Interest Test Guidance	http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/ThePublicInterestTest/ThePublicInterestTestEIRs.aspx

Appendix 2: Regulations 2 and 11

2 Interpretation

(1) In these Regulations –

…

“the data protection principles" means the principles set out in –

(a) Article 5(1) of the UK GDPR, and

(b) section 34(1) of the Data Protection Act 2018;

“data subject” has the same meaning as in the Data Protection Act 2018 (see section 3 of that Act);

…

"personal data" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2) and (14) of that Act);

…

“the UK GDPR” has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(10) and (14) of that Act); and

…

(3A) In these Regulations, references to the UK GDPR and the Data Protection Act 2018 have effect as if in Article 2 of the UK GDPR and Chapter 3 of Part 2 of that Act (exemptions for manual unstructured processing and for national security and defence purposes) –

(a) the references to an FOI public authority were references to a Scottish public authority as defined in these Regulations, and

(b) the references to personal data held by such an authority were to be interpreted in accordance with paragraph (2) of this regulation.

…

11 Personal data

(1) To the extent that environmental information requested includes personal data of which the applicant is the data subject then the duty under regulation 5(1) to make it available shall not apply to those personal data.

(2) To the extent that environmental information requested includes personal data of which the applicant is not the data subject, a Scottish public authority must not make the personal data available if –

(a) the first condition set out in paragraph (3A) is satisfied, or

(b) the second or third condition set out in paragraph (3B) or (4A) is satisfied and, in all the circumstances of the case, the public interest in making the information available is outweighed by that in not doing so.

(3A) The first condition is that the disclosure of the information to a member of the public otherwise than under these Regulations –

(a) would contravene any of the data protection principles, or

(b) would do so if the exemptions in section 24(1) of the Data Protection Act 2018 (manual unstructured data held by public authorities) were disregarded.

(3B) The second condition is that the disclosure of the information to a member of the public otherwise than under these Regulations would contravene Article 21 of the UK GDPR (general processing: right to object to processing).

(4A) The third condition is that any of the following applies to the information –

(a) it is exempt from the obligation under Article 15(1) of the UK GDPR (general processing: right of access by the data subject) to provide access to, and information about, personal data by virtue of provision made by or under section 15, 16 or 26 of, or Schedule 2, 3 or 4 to, the Data Protection Act 2018, or

(b) on a request under section 45(1)(b) of that Act (law enforcement processing: right of access by the data subject), the information would be withheld on reliance on subsection (4) of that section.

(5) [Deleted]

(6) For the purposes of this regulation, a Scottish public authority may respond to a request by not revealing whether information exists or is held by it, whether or not it holds such information, if to do so would involve making information available in contravention of this regulation.

(7) In determining, for the purposes of this regulation, whether the lawfulness principle in Article 5(1)(a) of the UK GDPR would be contravened by the disclosure of information, Article 6(1) of the UK GDPR (lawfulness) is to be read as if the second sub-paragraph (disapplying the legitimate interests gateway in relation to public authorities) were omitted.

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and Status. *E.g. C5 Key Documents Handbook v01 CURRENT ISSUE*	C2 EIRs Guidance Regulation 11: Personal data v03 CURRENT ISSUE
VC File Id	131225
Type	Briefing
Approver	SMT
Responsible Manager	HOE
Date of next planned review	July 2021
Approval & Publication	
Approval Date (major version)	19/02/2020
For publication *(Y/N)*	Y
Date published	11/03/2021
Name of document in website file library	EIRsGuidanceRegulation11Personaldata
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	10 March 2021

Summary of changes to document

Date	**Action by** *(initials)*	**Version updated** *(e.g. v01.25-36)*	**New version number** *(e.g. v01.27, or 02.03)*	**Brief description** (*e.g. updated paras 1-8, updated HOPI to HOOM, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding*)
19/02/2020	BOW	03.00	03.01	New document created following approval of draft
19/02/2020	BOW	03.01	03.02	DCS updated, published on website
03/03/2020	MK	03.02	03.03	Contents page updated (had wrongly incorporated flowchart)
12/03/2020	BOW	03.03	03.04	DCS updated, published on website
28/01/2021	MK	03.04	03.05	Changes made to reflect Brexit; flowchart temporarily removed
28/01/2021	MK	03.05	03.06	Changes reviewed; other minor changes made
28/01/2021	BOW	03.06	03.07	DCS updated, published on website
10/03/2021	MK	03.07	03.08	Cross reference in para 29 sorted
11/03/2021	BOW	03.08	03.09	DCS updated, published on website

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info