



**The Data Protection Act 2018 and General Data Protection Regulation**

**The Freedom of Information Act 2000**

**Environmental Information Regulations 2004**

|  |   |  |
|--|---|--|
| <b>This instruction applies to:-</b>   |   | <b>Reference: -</b>  |
| HMPPS HQ<br>Prisons<br>National Probation Service  |   | <b>PSI - 03/2018</b><br><b>PI - 03/2018</b><br><b>AI - 02/2018</b> |
| <b>Issue Date</b>  | <b>Effective Date</b>   | <b>Expiry Date</b>   |
| 24 May 2018  | 25 May 2018   |  |
| <b>Issued on the authority of</b>  | HMPPS Agency Board  |  |
| <b>For action by</b>   | <p>All staff responsible for the development and publication of policy and instructions:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> HMPPS HQ</li> <li><input checked="" type="checkbox"/> Public Sector Prisons</li> <li><input checked="" type="checkbox"/> Contracted Prisons*</li> <li><input checked="" type="checkbox"/> National Probation Service (NPS)</li> <li><input type="checkbox"/> Community Rehabilitation Companies (CRCs)</li> <li><input type="checkbox"/> Other Providers of Probation and Community Services</li> <li><input checked="" type="checkbox"/> Governors</li> <li><input checked="" type="checkbox"/> Heads of Groups</li> <li><input checked="" type="checkbox"/> HMPPS Rehabilitation Contract Services Team</li> <li><input type="checkbox"/> Other Providers of Probation and Community Services</li> </ul> <p><i>* If this box is marked, then in this document the term Governor also applies to Directors of Contracted Prisons</i></p> |  |
| <b>Instruction type</b>  | <b>Service improvement/ Legal compliance</b>  |  |
| <b>For information</b>   | Community Rehabilitation Companies  |  |
| <b>Provide a summary of the policy aim and the reason for its development / revision</b> | <p>This Instruction is issued to update and replace Prison Service Instruction (PSI) 44/2014, AI 28/2014 and Probation Instruction 61/2014. It updates Her Majesty's Prison and Probation Service (HMPPS) policy on how to comply with information legislation and how to respond to requests for information under the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIRs) and under the data protection laws (the Data Protection Act (2018) and General Data Protection Regulation (GDPR)). It informs staff of the process for the handling of FOIA and EIR requests for information through the Knowledge and Information Liaison Officers (KILOs) network throughout HMPPS and of the handling process for subject access requests under the data protection laws. It aims to further embed FOI, EIR, and the UK's new data protection laws in the organisation and to ensure compliance with our statutory obligations under these statutes.</p>                     |  |

|  |  |
|--|--|
|  | Local Community Rehabilitation Companies (CRCs) which were established under Section 3 of the Offender Management Act 2007 are Private Limited Companies formed in accordance with the Companies Act 2006 and therefore are responsible for their own Information Access regimes. Because of this, the instruction does not apply. |
| <b>Contact</b>   | Kate Burns<br>Communication and Information Directorate<br>Ministry of Justice<br>Post point 10.38<br>102 Petty France<br>London, SW1H 9AJ<br>Tel: 020 3334 3248 Email: <a href="mailto:kate.burns@justice.gov.uk">kate.burns@justice.gov.uk</a>   |
| <b>Associated documents</b>  | <a href="#">PSI 35/2014 – Records, Archiving, Retention and Disposal</a><br><a href="#">PSI 24/2014 AI 18/2014 PI 18/2014 - Information Assurance Policy</a><br><a href="#">PSI 16/2016 AI 12/2016 PI 15/2016 – Information Sharing</a><br><a href="#">PI 28/2014 – Archiving, Retention and Disposal Policy</a>                   |
| <b>Replaces the following documents which are hereby cancelled:</b> PSI 44/2014, AI 28/2014 and PI 61/2014. <i>All hard copies of this instructions must be destroyed.</i> |  |
| <b>Audit/monitoring:</b> Compliance with this policy will be monitored by the Deputy Director of Information Operations Division in Ministry of Justice.                   |  |
| <b>Introduces amendments to the following documents:</b> None  |  |
| <b>Notes:</b> <i>All Mandatory Actions throughout this instruction are in italics and must be strictly adhered to.</i>   |  |

## CONTENTS

| Section | Subject  | For Reference By |
|---------|--|------------------|
| 1.      | <a href="#">Executive Summary</a>  | All Staff        |
| 2.      | <a href="#">Operational Instructions</a>   |                  |
| 3.      | <a href="#">Requests for Information under FOIA 2000</a>                             |                  |
| 4.      | <a href="#">Requests for Information under Environmental Information Regulations</a> |                  |
| 5.      | <a href="#">Requests for Information under data protection laws</a>                  |                  |
| 6.      | <a href="#">Roles and Responsibilities</a>   |                  |
| Annex A | <a href="#">Contact Details</a>  |                  |
| Annex B | <a href="#">Subject Access Request Form: Offender</a>                                |                  |

## 1. Executive Summary

### Update/Background

- 1.1 This instruction outlines HMPPS policy in responding to requests made under the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) 2004, the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR). The DPA 2018 and GDPR together are referred to in this instruction as the data protection laws.
- 1.2 *The instruction also provides an overview of the procedures staff must follow in order to ensure compliance with the data protection laws, FOIA and the EIR.*
- 1.3 The PSI replaces PSI 44/2014, AI 28/2014 and PI 61/2014. Separate instructions have been issued on [PSI 24/2014 AI 18/2014 PI 18/2014 - Information Assurance Policy](#), [PSI 16/2016 AI 12/2016 PI 15/2016 – Information Sharing](#), [PSI 35/2014 – Records, Archiving, Retention and Disposal](#) and [PI 28/2014 – Archiving, Retention and Disposal Policy](#).
- 1.4 The Ministry of Justice (MOJ) has a statutory requirement to respond to valid requests made under the data protection laws, FOIA and EIR.
- 1.5 Building on experience in other areas of the organisation, we have established processes for how we deal with requests for information. Two networks, Knowledge and Information Liaison Officer (KILO) and Information Access Representative (IAR), have been established across the business. This places the primary responsibility for responding to requests on the area responsible for the subject matter of the request. The Disclosure Team – part of the Communication and Information Directorate in MOJ – actively supports KILOs and IARs in their duties by logging cases and providing expert advice, training, guidance and procedural management of requests made under information legislation.

### Desired outcomes

- 1.6 The aim of this policy is to further embed Freedom of Information, Environmental Information Regulations and the new data protection laws in and across HMPPS including the National Probation Service (NPS), and to ensure compliance with our statutory obligations under this legislation.

### Application

- 1.7 This policy should be read by all staff, particularly those who update, note, add to or amend offender records; all staff who deal with requests made under these regimes; existing IARs, KILOs and their deputies and line managers; Local Information Managers (LIM).

### Mandatory actions

- 1.8 *All mandatory actions are shown in italics. Governors, Directors and Deputy Directors of Probation and Heads of Group must ensure that all staff responsible for the updating offender records and the management of records are familiar with the content of this instruction and understand the mandatory actions set out in Sections 2 to 6.*

### Resource Impact

- 1.9 This is a revision of existing instructions for which local systems should already be in place in prisons. *Within the HMPPS staff must be identified to fulfil the required roles of Information Access Representatives and Knowledge and Information Liaison Officer to support their teams in handling all requests in accordance with the relevant legislation.*

#### Explanation of Terms

- 1.10 The following terms are used within this instruction:

|                      |   |
|----------------------|---|
| DG                   | Director General                                |
| DPA                  | Data Protection Act 2018                        |
| GDPR                 | General Data Protection Regulation              |
| Data protection laws | DPA 2018 and GDPR                               |
| EIR                  | Environmental Information Regulations 2004      |
| FOI/FOIA             | Freedom of Information Act 2000                 |
| IAR                  | Information Access Representative               |
| ICO                  | Information Commissioner's Office               |
| IGDP                 | Information Governance and Data Protection team |
| KILO                 | Knowledge and Information Liaison Officer       |
| MC                   | Ministerial Correspondence                      |
| MOJ                  | Ministry of Justice                             |
| HMPPS                | Her Majesty's Prisons and Probation service     |
| NPS                  | National Probation Service                      |
| PQ                   | Parliamentary Question                          |
| RFI                  | Request for Information                         |
| SAR                  | Subject Access Request                          |
| TO                   | Treat Official Correspondence                   |

(Approved for Publication)

**Director of Prison Estate Transformation Programme**

## **2. Operational Instructions**

### **REQUESTS FOR INFORMATION - Identifying and Managing Requests**

2.1 It is very important to draw a distinction between FOIA, EIR, data protection requests and routine correspondence. It is also important that requests received by Establishments, Probation Offices, Groups, Units or Hubs which should be treated as requests for information under FOIA, EIR or data protection laws are identified and forwarded to Disclosure or the Branston Data Protection Team as quickly as possible. This is because timescales for response under these Acts are set by legislation and the countdown for reply starts the day that MOJ (at whatever point; i.e. an Establishment, Group, Probation Office, Unit or Hub) receives a request.

### **Parliamentary Questions/Ministerial and Director General/Treat Official Correspondence**

2.2 It is important that answers to Parliamentary Questions and replies to requests are consistent. *Each area must consider related PQs, MCs and DG Correspondence when responding to requests for information.*

### **Introduction to Information Access**

2.3 The three regimes this instruction is concerned with under which requests for information might be handled are:

- Freedom of Information Act 2000.
- Environmental Information Regulations 2004.
- Data protection laws; the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR).

2.4 A summary of the Acts and Regulations, follows at sections 3, 4 and 5.

### **Freedom of Information Act 2000 – General Background**

2.5 The Freedom of Information Act (FOIA) came into force on 1 January 2005. The essential principle of the Act is that there should be a general right of access to information held by public authorities consistent with the public interest, the right to privacy and effective public administration. The Act is designed to allow greater public access to information.

2.6 Any recorded information held by MOJ is **potentially** disclosable under the FOI regime. Any person making a request is entitled, subject to certain exemptions and cost limitations set out in the Act, to:

- Be informed in writing by MOJ whether we hold the information described in the request;
- Receive the information requested, if we hold it, subject to the application of exemptions (some of which are subject to a public interest test);
- Receive a reply within 20 working days.

2.7 *As a public authority, MOJ must have in place a system to ensure the efficient processing of requests for information submitted under FOI and to make sure that we are all aware of the requirements of the legislation and the role we have to play in*

*meeting those requirements.* The Act requires us to identify and locate records and respond within prescribed timescales.

### **Environmental Information Regulations 2004 – General Background**

- 2.8 The Environmental Information Regulations (EIRs) 2004 are based on the European Union Directive 2003/4/EC. They give the public access rights to environmental information held by a public authority in response to requests. The Regulations came into force on 1 January 2005 along with the Freedom of Information Act and cover any information that is considered to be 'environmental information' within the terms of the Regulations.
- 2.9 There are many similarities between the EIR and FOIA regimes, so the points above at 2.6 apply, including the timeframe. However, there are some key differences. EIRs requests do not have to be in writing. This means that telephone requests on environmental matters may also be valid (although in practice it is advisable to make a written record of any verbal requests received or to ask that the request is made in writing).
- 2.10 The Regulations promote the release of as much environmental information as possible to enable increased public participation in environmental decision making so there is an express presumption of disclosure in the EIRs. Furthermore, the exceptions contained in the EIRs are all subject to a public interest test, unlike with the exemptions contained in the FOIA, where some are "absolute" exemptions.

### **Data Protection Act 2018 and General Data Protection Regulation – General Background**

- 2.11 These data protection laws came into force in May 2018. Their essential purpose is to safeguard personal data; balancing the legitimate needs of organisations to obtain and use personal data with the rights of individuals to privacy.
- 2.12 The laws set out the requirements that organisations, such as MOJ including HMPPS Headquarters Groups/HMPS/NPS, need to adhere to when processing personal information. It also stipulates a number of rights for individuals in relation to how their personal data is processed and managed.
- 2.13 One right, under the data protection laws, is for individuals to have access to the information about them that is being processed by organisations. These requests are known as Subject Access Requests (SARs) and are usually used by individuals who want a copy of the information held on them.
- 2.14 Organisations can request proof of identification.
- 2.15 As well as providing individuals with the right to a copy of data held on them SARs also entitle those making a request to be informed of:
- The purposes of the processing;
  - The categories of personal data processed;
  - The recipients or categories of recipient to whom the personal data have been or will be disclosed, including in third countries or international organisations;
  - The envisaged retention period, or, if this is not possible, the criteria used to determine this period;
  - The individual's rights of rectification, erasure, to restrict processing or to object to processing
  - Their right to lodge a complaint with the ICO;

- Information regarding the source of the data (if not collected from the data subject)
- The existence of automated decision-making including profiling, information about the logic involved and the significance and envisaged consequences of the processing for the data subject.

2.16 Under the data protection laws, SARs have to be answered in full within **one month** of receiving the request. If the SAR is from a member of staff or ex-member of staff and the request is complex the time to respond can be extended by up to two months. The data subject must be informed of any extension within one month of receipt of their request and told the reasons for the delay. This extension does not apply to SARs made by offenders.



### **3. Requests for Information under FOIA 2000**

#### **How to recognise a Freedom of Information Act request when you get one**

- 3.1 Any request for recorded information received by a public authority has to be answered in accordance with the Freedom of Information Act 2000 or the Environmental Information Regulations 2004. *The only exception will be an individual's request for their own personal data (Subject Access Request) which must be handled under the terms of the data protection laws (see section 5).*
- 3.2 Recorded information means the information which the Department has recorded in permanent form and includes, but is not limited to information held electronically, e-mails, hard copy documents, images and recordings.
- 3.3 *A FOIA request must be made in writing, either in hard copy via letter or digitally via email, or potentially social media. Anyone, anywhere within HMPPS can receive a request, but it should be promptly brought to the attention of the Disclosure Team via [data.access@justice.gov.uk](mailto:data.access@justice.gov.uk) by the area that received it. As soon as the request is received the timescales start so it is important these are dealt with quickly.*
- 3.4 *A contact name and address (an email address is sufficient) must be provided.*
- 3.5 Anyone, anywhere in the world can make a request – it doesn't matter who they are. Guidance from the Information Commissioner's Office stipulates that we should be both applicant (and motive) blind. This means we cannot let who the individual is or why they would request particular information influence responding to a request in line with the FOIA.
- 3.6 The request does not have to specify it is made under the terms of the FOIA. It is up to us, as a public authority, to identify a FOIA request and deal with it correctly.

#### **How to determine whether a request is business as usual correspondence/ general enquiry or a FOIA Request**

- 3.7 It is very important to draw a distinction between FOIA requests and routine correspondence. FOIA deals only with requests for recorded information ('information' under the FOIA means information *recorded* in any form). So, for example, a request for a general explanation as to why we made a particular decision or for an opinion on a particular issue should be treated as routine correspondence. Whereas, a request for copies of the recorded information we considered or wrote down in making a particular decision or policy would be an FOIA request.
- 3.8 As an example, if an enquiry asked an opinion as to why HMPPS decided to introduce a training course at a particular prison – that is not a request under FOIA. If the request asked for the information that was considered in making the decision to introduce the training course, or records of information relating to that decision (including an opinion if already recorded), that is a request that should be handled under the FOIA.

#### **What to do when you identify that you have received a Freedom of Information Act request**

- 3.9 It is important that you identify then action FOIA requests quickly because the Department has a 20-working day statutory deadline to respond to the request from the date it is received anywhere in the Department.

- 3.10 *Therefore once you have identified you have a FOIA request, you must send it **ASAP (within 24 hours) to the Disclosure Team for logging and action.*** This should be done by email: [data.access@justice.gov.uk](mailto:data.access@justice.gov.uk) If the FOIA request has been received in hard copy it must be scanned and emailed to the Disclosure Team.
- 3.11 The Disclosure Team will then take this forward under the Department's agreed processes for FOIA requests. This will be via the KILO network, who are trained FOIA experts within business areas. Therefore, once you have forwarded the FOIA request you don't need to do anything else unless you hear again from the Disclosure Team or your KILO.

### **What to do when you are contacted for information by the Disclosure Team or a KILO**

- 3.12 As above, there is an agreed process for handling FOI requests in the MOJ via the Disclosure Team and the KILO network. They will action the response in line with the Department's timelines and compliance responsibilities under the Act. You may, on occasion, be asked by a KILO or by Disclosure Team for the purpose of a request:
- Whether information (all or part) in scope of a request is held or not.
  - Whether the cost limit is engaged (see 3.16 to 3.20).
  - To provide a copy of the information in scope of the request. You only need to start compiling the information when specifically asked to do so.
- 3.13 If you are aware of a particular consideration, sensitivity or exemption that might be relevant to the information you are providing or that it is of public interest, please also ensure that you highlight this to the KILO and/or to the Disclosure Team. Alternatively, please make sure you alert the KILO and/or the Disclosure Team to other relevant officials (such as subject matter experts), as this helps ensure all wider considerations are taken into account. For example, a security concern might arise following the disclosure of particular information. Any redaction will be done by the Disclosure team.
- 3.14 Please note that any information that you create when responding to a request, for example, an email to a colleague about the content of the proposed response, could itself be considered for disclosure in response to a future FOI request on the subject.

### **Community Rehabilitation Companies (CRCs) and other contracted service providers**

- 3.15 CRCs are private limited companies formed in accordance with the Companies Act 2006 and are therefore, responsible for their own Information Access regimes. The same applies to other contracted third-party suppliers, for example private prisons. However, CRCs are under a contractual duty to provide the information required to enable the Department to respond to an FOI request.

### **Cost of replying – 'appropriate limit'**

- 3.16 Under section 12 of the Freedom of Information Act, MOJ is not obliged to comply with any information request where the prescribed costs of doing so exceed £600. The £600 limit applies to all central government departments and is based on work being carried out at a rate of £25 per hour, which equates to 3½ days work per request. Prescribed costs include those which cover establishing whether information is held and then the cost of locating, extracting, retrieving and collating the information. They do not include, for example, considering whether any information is exempt from disclosure, overheads such as heating or lighting, or disbursements such as photocopying or postage.

- 3.17 You may therefore be asked by a KILO and/or the Disclosure Team for information about whether there are cost considerations in relation to a request for which you may be supplying the information.
- 3.18 For example, requests for information on 'all prisons' or 'all approved premises' may come into this category unless the information requested is held centrally or readily available in each establishment or region.
- 3.19 The cost limit does not take into account the time needed to redact information, consider the use of exemptions (as indicated above) or carry out the public interest test when considering whether or not to release the information. However, if there is extensive redaction needed on a large number of documents you can consider refusal under section 14 of the FOIA (vexatious). If this is considered you must contact the Disclosure Team as this cannot be applied without their permission.
- 3.20 FOIA requires the Department to offer advice to a requester as to how they might amend their request to meet the cost limit (under the section 16 duty to give advice and assistance). You may therefore be asked by a KILO and/or the Disclosure team if you have a recommendation as to how to narrow a request to bring it within the cost limit for inclusion in the response to the requestor.

### Exemptions under FOIA

- 3.21 The FOIA recognises that there will be valid reasons for protecting certain information from disclosure and, as such, includes some exemptions to disclosure. Some of these exemptions are 'absolute exemptions'. Others, known as 'qualified exemptions' require that before taking a decision on disclosure, we consider whether or not it is in the public interest to release the information into the public domain or not. Please note that exemptions should not be applied, in blanket fashion, to whole documents. There will need to be a consideration of which exemptions apply to which parts of the document. Any information that doesn't fall under an exemption can be released, with the released information either extracted out of the document or the withheld material being redacted. For further information, please speak to your KILO or the Disclosure Team.
- 3.22 As above, if you think an exemption may be engaged for information you are providing the Disclosure Team or a KILO, or perhaps as the information expert you have specific insight into what the public interest arguments are in favour of disclosure or non-disclosure, please highlight this to your KILO.
- 3.23 Further information about FOIA exemptions and the FOIA in general can be found on the GOV.UK website or via the Information Commissioner's Office: [www.ico.org.uk](http://www.ico.org.uk)

### Publication Scheme

- 3.24 *Under the FOIA, the Department must have a publication scheme that sets out categories of information to be made available to the public as a matter of course.* For example, planned statistical publications. This information can be found on the Ministry of Justice pages of the GOV.UK website <https://www.gov.uk>.
- 3.25 If you think your business area should routinely be publishing information please contact the Disclosure Team for advice. As a general rule, the ICO advise that public authorities should publish the following on a routine basis:
- minutes and agendas of public meetings;
  - documents it is required to make public by other legislation such as the Local Government Act 1972;
  - minutes of senior-level policy and strategy meetings e.g. board meetings; and

- any background documents which are referred to in the agenda or minutes, or were circulated in preparation for the meeting. These are considered part of the agenda.

### **Disclosure Log**

3.26 Replies to requests where information has been disclosed may be published on the department's Disclosure Log. This allows further requests for the same information to be directed to it and to reduce the number of information requests which need full consideration. This log is managed by the Disclosure Team and can be found on the Ministry of Justice pages on the GOV.UK website: <https://www.gov.uk/>

### **Emails between staff and staff notebooks**

3.27 All recorded information, including emails between staff and their notebooks, are potentially releasable under FOIA and the data protection laws. When drafting emails and making notes, always consider the FOIA and data protection implications and the potential for criticism of the Department or embarrassment for individuals if they were released. Both emails and notes should, without exception, meet the same professional Departmental standards as all written correspondence.

### **Timescale for response**

3.28 The timetable for responding to a request for information under FOIA is 20 working days from receipt anywhere in the MOJ to final reply. This deadline is statutory. However, it should be noted that in trigger cases a response must be sent to the Disclosure Team within 10 working days.

## **4. REQUESTS FOR INFORMATION UNDER ENVIRONMENTAL INFORMATION REGULATIONS**

### **Environmental Information Regulations 2004**

4.1 There are many similarities between the FOIA and EIR regimes. As with FOIA, EIR gives access rights to recorded information, primarily about the environment. Our experience is that HMPPS receives substantially more EIRs than other areas of the Department and it is important that we are aware of it and know how to identify requests which fall under it. However, these are treated under the same Departmental process as FOIA requests. So, if you are not sure if a request is EIR or FOIA just send it to the Disclosure Team and they will assess it for you.

4.2 Some points to note on the EIR:

- EIR requests do not have to be made in writing. It is helpful to ask for the request to be made in writing but it is not necessary for an individual to do so.
- *There are a number of exceptions contained in EIR which **must** be considered before information is released in response to a request, but **all** EIR exceptions are subject to a public interest test.*
- A requestor does not have to mention EIR. Some requests may specifically mention a piece of legislation, for example, FOIA, but this does not prevent you from treating them under the EIR where the subject matter makes it appropriate to do so.

4.3 Examples of requests for “environmental information” are:

- Requests which relate to emissions, noise or waste likely to affect elements of the environment;
- Policies, legislation, plans, programmes, environmental agreements and activities likely to affect or protect the elements of the environment;
- Cost-benefit and other economic analyses and assumptions used within the framework of environmental measures and activities;
- The state of human health and safety, including contamination of the food chain, conditions of human life and built structures in as much as they are or may be affected by the state of the elements of the environment;
- Information on new buildings (for example prison establishments), including local planning considerations.

### **What to do when you identify that you have received an EIR request**

4.4 Please follow the same process as outlined above for FOIA (see 3.9 to 3.11).

### **Timescale for response**

4.5 The timetable for responding to a request for information under EIR is 20 working days from receipt anywhere in the MOJ to final reply. This deadline is statutory.

## **5. REQUESTS FOR INFORMATION UNDER DATA PROTECTION LAWS**

### **Data Protection Laws**

- 5.1 The UK's data protection laws regulate the processing of information in relation to living individuals. This includes the obtaining, holding, using or disclosing of information. In particular, personal data is that which relates to a living individual who can be identified either from the data or other information which is in our possession or is likely to come into our possession. It includes any expression of opinion about the individual and any indication of the intentions of us as data controller or any other person in respect of the individual. Personal data also includes data on an individual's location, their genetic and biometric data and online identifiers such as IP addresses if they can be linked to an individual.
- 5.2 A data controller must implement appropriate technical and organisational measures to ensure that, by design and default, only personal data which is necessary for each specific purpose of the processing is processed.  
The MOJ is a single data controller covering its headquarters and Executive Agencies including HMPPS and HMPPS headquarters and National Probation Service (NPS). Community Rehabilitation Companies are each separate data controller and are each responsible for meeting the obligations of the data protection laws.
- 5.3 The data protection laws give individuals the right to know what information MOJ holds about them and sets out rules to make sure this information is handled properly. The laws require anyone who handles personal information to comply with a number of important principles.
- 5.4 The laws do not cover information held on the deceased. Requests for such information would be handled under FOIA.

### **Summary of Principles**

- 5.5 The principles of the data protection laws are that:
- Personal data shall be processed fairly, lawfully and in a transparent manner;
  - Personal data shall be obtained only for specified, explicit and legitimate purpose(s) and not be processed in any manner incompatible with those purposes. Further processing for archiving in the public interest, scientific or historical research or statistical purposes shall not be considered incompatible with the initial purposes;
  - Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed;
  - Personal data shall be accurate and where necessary, kept up to date; every reasonable step must be taken to ensure personal data that is inaccurate, having regard to the purposes for which it is processed is erased or rectified without delay.
  - When processed for criminal law enforcement purposes, including the execution of criminal penalties:
    - personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments;

- a clear distinction must, where relevant and as far as possible be made between personal data relating to persons suspected of having committed or being about to commit a criminal offence; persons convicted of a criminal offence; persons who are or may be victims of a criminal offence and witness or other persons with information about offences;
- all reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for criminal law enforcement purposes. If after it has been transmitted it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

- Personal data must not be kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which it is processed. Personal data may be stored for longer if it will be processed solely for archiving in the public interest, scientific, historical or statistical research purposes.
- Personal data shall be processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.6 All MOJ personnel who process or use personal data should familiarise themselves with and ensure they follow these principles at all times. The term 'process' has wide ranging meaning under data protection law and covers any action taken in respect of personal data from obtaining and recording information through to handling, using, sharing, storing and destruction of information.

5.7 The MOJ, including HMPPS, has a duty (under the first principle) to inform individuals of the purposes for which we intend to process their personal data when we begin our contact with them. This principle also means that we must have a legitimate need for the information we gather and use; be able to explain how we use personal data and make sure we do not do anything unlawful with it. For example, when an offender is first received at a prison establishment or a visitor attends an establishment, HMPPS provides to them a Privacy Notice. For offenders and visitors this information must be given to them when they arrive in the establishment and for offenders being supervised by the NPS at their first probation meeting. The information must be provided in a concise, intelligible and easily accessible format, using clear and plain language.

5.8 The data protection laws also require us to restrict the personal data we have about individuals to the minimum we require for the purposes we need it. In other words, we should ensure that we do not gather information for which we do not have a legitimate need.

5.9 The laws require us to ensure that we are clear about how long we need to keep and store information. We do this through our records retention and destruction policies and schedules which explain how and when we should retain or securely destroy personal information. More information on retention and destruction can be found in [PSI 35/2014 – Records, Archiving, Retention and Disposal](#) and PI 28/2014 - Archiving, Retention and Disposal Policy.

#### **Other obligations under the data protection laws**

5.10 The data protection laws also oblige us to keep all personal data accurate and up to date. Individuals whose personal data we are processing can contest its accuracy and require us stop processing it while its accuracy is verified. If the information is

inaccurate or incomplete the law requires us to correct and or complete it within one month. If it cannot be clearly proven that the data is inaccurate the ICO advises to note on the record that the information in question is in dispute.

- 5.11 Requests for information that involve the release of personal information, whether about the applicant or another person, are subject to the data protection laws. In practice, the legislation provides strict rules around what, if any, sensitive personal data, pertaining to, for example health, racial or ethnic origin, sexual life or private personal data, such as home address, telephone number or information about personal life, would be disclosable to a third party. Limited details about individuals which identify their official role, for example, job title, responsibilities, work contact details, prison officer number and name may be disclosable. For example, if the information is already known to the requestor or it is reasonable in all the circumstances to release it.
- 5.12 Where we process individuals' personal data, the data protection laws also provide them with a number of rights which support the Principles. These are the right:
- Of subject access;
  - To have incorrect personal data corrected and incomplete data completed (rectification, as noted at 5.10);
  - To have their data erased or to restrict its processing;
  - Not to be subject to decision-making solely by automated means including profiling;
  - To have a copy of their data provided in a machine-readable format (referred to as data portability);
  - To object to processing based on legitimate interests or the performance of a task in the public interest;
  - To prevent processing for the purposes of direct marketing;
  - To compensation for damage suffered as a result of an infringement of the data protection laws by the data controller.
  - To make a complaint to the Information Commissioner's Office.

### **Requests for processing of personal data to stop**

- 5.13 There may be circumstances when we are approached by individuals and requested to delete (erase) or stop (restrict) or they are otherwise objecting to the processing their personal data. If this is the case you should refer in the first instance to [PSI 35/2014 – Records, Archiving, Retention and Disposal](#) to ensure that the data is being kept in line with the HMPPS records retention and destruction policy. If you receive such a request you should consider it on a case by case basis and against the following points:
- Is the data being retained in line with the records retention and destruction policy or has it already been destroyed? If the retention period has expired and there is no other clear justification to retain the information, i.e. it has been



retained in error, the information should be destroyed and this destruction recorded on the destruction log or stored and not processed further if this is what the request was for.

- Are there any reasons (such as security, intelligence or litigation) why the data in question needs to be retained in line with the retention schedules and could not be destroyed early or not be processed further?
- Is the processing necessary in relation to a contract that the individual has entered into or because the individual has asked for something to be done so they can enter into a contract?
- Is the processing necessary because of a legal obligation that applies to MOJ/HMPPS (other than a contractual obligation)?
- Is the processing necessary to protect the individual's "vital interests"?
- Is the data still required for operational or business reasons?
- Is the information likely to be relevant to defend a civil claim if one is made against the Department?
- What reason has the individual given for the request? Are they contesting the accuracy or completeness of the information?
- Is the data being processed unlawfully?
- Is the processing based on consent and has the data subject withdrawn their consent?
- How long is it until the retention period is due to expire? If the data is approaching the end of the established retention period, there may be occasions when it might be acceptable to destroy the data, depending on the original reasons for retention.

5.16 A record should be kept of the request and the decision made including the reasons for the decision. A response must be given to the requestor within one month. If the request was received in electronic form the response should be provided if possible, in electronic form unless otherwise requested by the data subject.

5.17 Further guidance on such cases should be sought from the MOJ Departmental Records Officer (DRO) or the HMPPS Agency Records Officer. See [Annex A](#) for contact details.

### **Routine disclosure of personal information to individual offenders**

5.18 The processes set out in this Instruction are not intended to replace or interfere with existing arrangements for the local disclosure of information to offenders, for example the reasons for categorisation decisions, disclosure of parole dossiers, requests to see money accounts, correspondence sheets or property cards(s) etc. Similarly, information that the offender would be expected to see as part of the day-to-day running of the prison, such as adjudication records or other information the offender has already been party to.

5.19 *Where there are existing arrangements set out in other Instructions/Orders for disclosing information to individual offenders, these must continue to be followed.*

5.20 *Care must be taken with requests for personal information from third parties to ensure they are acting on behalf of the individual. It is common to receive enquiries either directly or via third parties. However, personal information in relation to living juveniles, young adults and adult offenders must not be disclosed even to close relatives without the offender's consent.*

### Requests for information from third parties

5.21 HMPPS, in headquarters, prisons and probation, receive a significant number of requests for information on offenders, ex-offenders and deceased offenders from third parties. These requests usually fall into three broad categories. These are:

- Requests for information on offenders and ex-offenders from third parties, including police forces and local authorities;
- Requests for information about ongoing litigation between an offender or ex-offender and HMPPS; and
- Requests for information on a deceased offender from their next of kin via legal representatives ahead of a forthcoming coroner's inquest.

5.22 IGDP and the Disclosure Team will provide advice on how to respond to requests for personal information from third parties, including requests from police forces or those involved in litigation against offenders and ex-offenders and the legal representatives of a deceased offender's next of kin where HMPPS is not involved in that case, if necessary. There is also guidance available in the Information Access Representative Manual and KILO Manual.

5.23 If there is an ongoing litigation claim against HMPPS or MOJ, Gallagher Bassett (MOJ Claims Handlers) or The Government Legal Department (GLD) Solicitors will provide advice on the information required for disclosure. If the information holder has any concerns they may liaise with the HMPPS National Litigation Unit (NLU) who may in turn seek advice from IGDP. NLU's contact details are at [Annex A](#).

5.24 If the coroner's inquest into the death of an offender is yet to be held Equalities, Interventions and Operational Practice (EIOPG) or (GLD) Solicitors will provide advice on the information required for disclosure who may in turn also seek advice from IGDP.

5.25 ERD group handles any litigation concerning a death in custody. Any requests for the disclosure of a deceased offender's records following the inquest into their death should be forwarded to the GLD Solicitors case holder or ERD contact for consideration as part of the civil litigation process.

5.26 Non-business as usual requests from third parties for information about staff should be forwarded to: [datamanagement@hmpps.gsi.gov.uk](mailto:datamanagement@hmpps.gsi.gov.uk)

### What to do when you identify that you have received a request from an individual for their own personal information:

5.27 Requests made by any individual (including offenders, ex-offenders, current and former members of staff, victims and members of the public) for personal information about them are called **Subject Access Requests (SARs) under the data protection laws.**

5.28 It is important that you identify then action SARs quickly as the Department has a **one month (30 calendar days) statutory deadline** to respond to the request from the

date a request is received anywhere in the Department. Send SARs to the appropriate area of the business, detailed below.

- 5.29 **Offender and ex-offender SARs:** If you receive a request from an offender, ex-offender or their representatives you should immediately determine if the request is a SAR or a request for routine information, which can be given directly to the offender. *If you are satisfied that the request is a SAR, you must send it immediately on to the data protection team based in Branston.* You should also ensure that you send to the team signed authority from the offender if the request is being made by their representative.
- 5.30 **All other SARs:** *If you receive a SAR from anyone else – including from a current or former member of staff - you must send it ASAP (at least within 24 hours) to the Disclosure Team for logging and action via email: [data.access@justice.gsi.gov.uk](mailto:data.access@justice.gsi.gov.uk).* If it received in hard copy it should be scanned and sent electronically.

**What to do if you are asked to provide information by Disclosure, the Branston based data protection team, a KILO or the Shared Service Centre HR SAR team in relation to a SAR request**

- 5.31 In order to comply with a SAR those who handle these requests on behalf of the Department may ask you to carry out a search for, and supply them with, the requestor's personal data, for consideration under the data protection laws. They may also ask for other information from you in order to comply with the laws.
- 5.32 You should ensure you are satisfied with the identity of the person commissioning the information and then follow the instructions they have outlined to you, including meeting the relevant timeframes set.
- 5.33 You should carry out the appropriate searches, as instructed, to identify the personal data of the data subject.
- 5.34 Personal data is information where an individual is **identifiable** from it and it also has to **relate** to the individual. If you are not sure if the information you have identified is personal data then the following guide will help: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/>. Alternatively, please consult the relevant expert who has commissioned the data from you.
- 5.35 Please be mindful of how you handle any personal data to ensure this is in line with the data protection obligations we each have, outlined above. You also need to ensure that any personal information is sent and received securely in line with the Departmental process for handling personal data.
- 5.36 If you think an exemption under the data protection laws may be engaged for information you are providing to the Disclosure Team, IGDP, a KILO or the Shared Service Centre SAR team – or perhaps as the information expert you have specific information to which the team should be alerted (for example security information or other sensitivities), please ensure you highlight this. Any redaction will be done by the Disclosure team.
- 5.37 The relevant team will then respond to the SAR directly in line with the data protection laws' requirements.

### Timescale for response to Subject Access Requests

- 5.38 The timescale for complying with SARs under the data protection laws is **one month** from the date the request is received anywhere in the Department – including personal identification (if required) and information to enable the Department to locate the information which that person seeks. If the SAR is from a staff or ex-staff member and is complex the timescale can be extended by up to two months. The individual making the request must be notified of the delay within one month and the reasons for the delay.
- 5.39 For more information on SARs that relate to current and former employees of the Department both managers and staff should refer to the relevant My Services pages, SAR request forms and SAR guidance.

### Information which did not originate within MOJ

- 5.40 Requests for personal data that relate to information held by the Department are not limited to information originated by us. *HMPs must only hold documents originated by third parties, for example, police and probation service, where there is a business need to do so.*

### Exemptions

- 5.41 The Act recognises that there will be some circumstances where organisations should protect personal information from disclosure. This can be due to the subject of the information or a third party. For example, the laws allow for an exemption if the personal information is being used for the purposes of prevention or detection of crime, and disclosure would be likely to harm these activities.
- 5.42 The data protection team in Branston will consider all the information and apply any appropriate exemptions before releasing it for SARs received from offenders and ex-offenders. Similarly, KILOs are responsible for consideration of exemptions in relation to all other SARs received by the Department. For staff SARs please contact the Shared Service Centre staff SAR team.

## **6. ROLES AND RESPONSIBILITIES**

### **Areas of Responsibility**

- 6.1 MOJ policy is that requests for information and SARs should be responded to by the business area with the lead for the information requested via the MOJ's KILO and IAR networks. This places responsibility for meeting the statutory deadline with the appropriate area of the business, and allows:
- For those with the best understanding of the subject matter of the request to collate and consider the application of exemptions to any information held;
  - MOJ to provide better quality advice to requesters on how broad or vague requests might be modified to allow us to answer them;
  - MOJ to monitor and improve our overall performance where necessary.
- 6.2 The only exception to this rule is requests from offenders and ex-offenders for their own personal data under a SAR. Because of the volume of requests made, prison establishments and NPS hubs are supported by a separate dedicated MOJ team who handle offender and ex-offender SARs on behalf of HMPPS. This team is part of MOJ and is based in Branston, Staffordshire.
- 6.3 *Requests for the disclosure of routine current information such as parole dossiers and other reports must be dealt with as day to day business (see paragraph 5.18 to 5.20).*

### **All Staff**

- 6.4 All staff are responsible for identifying when they have received a FOIA, data protection or EIR request and ensuring that these requests are forwarded to the appropriate part of the business for logging and action, **on the day they are received**. If a hard copy request is received it should be scanned and sent electronically to the following:
- requests under FOIA or EIR should be directed to the Disclosure Team for logging and action at [data.access@justice.gov.uk](mailto:data.access@justice.gov.uk)
  - requests for their personal data (SARs) under the data protection laws from employees or ex-employees should also be directed to the Disclosure Team at [data.access@justice.gov.uk](mailto:data.access@justice.gov.uk)
  - requests for their personal data (SARs) under the data protection laws from offenders or ex-offenders should be directed to the Branston based data protection team at [data.access@hmpps.gsi.gov.uk](mailto:data.access@hmpps.gsi.gov.uk)

### **Heads of Group, NPS Deputy Directors, Governors/Directors of Contracted Prisons**

- 6.5 *Heads of Groups/NPS Deputy Directors/Heads of Units must nominate a KILO and, for establishments (including contracted prisons), and NPS divisions, an IAR and a Deputy for their business area, and ensure that procedures are in place to facilitate the prompt handling of requests and that we comply with the appropriate legislative time limit.*
- 6.6 Managers and the Senior Civil Service have overall responsibility for ensuring timeliness and compliance within their business areas for FOIA and data protection requests.

### **The Disclosure and Branston Data Protection Teams' Role**

- 6.7 The Disclosure Team and Branston data protection team support the Department in handling requests for information, including running the KILO and IAR networks and providing the dedicated service for managing offender and ex-offender SARs.

6.9 The Disclosure Team's role includes:

- To support KILOs and enable them to fulfil their responsibilities under the information legislation;
- To provide training, general guidance and disclosure advice to equip KILOs and IARs to answer and manage requests for information;
- Logging and allocating all MOJ FOIA/EIR and staff and ex-staff subject access requests;
- Monitoring the MOJ's overall performance in answering requests for information, including timeliness and compliance with the FOIA and EIR;
- Setting the internal processes to be followed by the Department for FOIA and EIR requests.

6.10 The Branston data protection team's role includes:

- Logging and application of exemptions to information requested by offenders under the right of access.
- To support IARs and enable them to fulfil their responsibilities under the information legislation;
- To provide training, general guidance and disclosure advice to equip IARs to answer and manage requests for information;

**The MOJ Information Governance and Data Protection (IGDP) team's role.**

6.10 The IGDP team's role is to provide strategic oversight on the application and interpretation of the data protection laws across MOJ, to support the MOJ's Data Protection Officer (DPO) and provide a central point of expertise on data protection. The team is responsible for responding to complaints and queries from the ICO on data protection law compliance.

6.11 The team also manage the MOJ's governance arrangements on information assurance and data protection including liaison with the MOJ risk team, supporting the MOJ Senior Information Risk Owner and Information Asset Owners and acting as the secretariat to the MOJ Information Risk and Security Board, the Arms' Length Body Senior Information Risk Owner Board and the Information Assurance Leads Committee.

6.12 The team provide a programme of training and maintain a suite of guidance on a number of data protection related topics including data protection impact assessments, data sharing and data incident management.

6.13 The team manage a group of senior stakeholders (Information Assurance leads) across the department.

**Knowledge and Information Liaison Officer (KILO) Role:**

- 6.14 KILOs are responsible for processing and responding to FOIA and data protection requests in line with the Freedom of Information (FOI) Act, data protection laws and Environmental Information Regulations (EIR), alongside providing advice and guidance on these Acts to their immediate teams. This is done in line with the Roles and Responsibilities Service Level Agreement.

### Information Access Representatives (IAR)

- 6.15 IARs provide the link between the Disclosure Team, the Branston based data protection team and prison establishments and NPS divisions. *All establishments, including contracted prisons and NPS divisions must appoint an IAR and a Deputy or Supervisor to coordinate the information required to respond to SARs from offenders and ex-offenders, and to third-party requests (see paragraph 5.21).* The appointed IAR can also fulfil the role of KILO.
- 6.16 *Establishments/NPS divisions must appoint a new IAR when the existing one moves to another role or leaves HMPPS.*
- 6.17 The full range of IAR responsibilities are set out in detail in the IAR Manual. In summary:

*On receipt of a SAR from the Branston based data protection team the IAR must:*

- *Obtain all the information requested in the SAR;*
  - *Check that all photocopies are legible, copied single sided and are **not** hole punched or stapled together;*
  - *Check only one copy of the information is forwarded (i.e. that all duplicates are removed);*
  - *Identify information already released to the offender and put in separate envelope;*
  - *Ensure security information is provided in a separate envelope and attached to the top of the remainder of the information being provided*
  - *Forward the information securely, as stipulated by [PSI 24/2014 AI 18/2014 PI 18/2014 - Information Assurance Policy](#), as quickly as possible to the Branston team but not later than **five days from receipt of request***
  - *Inform the Branston team on 01283 496066 of any difficulty in meeting the response target.*
- 6.17 Because every document held by HMPPS that relates to an offender has to be examined and where appropriate redacted, it can, in the most complex cases take a number of weeks for the Branston team to process one SAR. It is therefore important that all requested information is provided to the Branston team within the timescales stated.
- 6.18 Establishments or NPS offices should not hold information on an offender for longer than is necessary or where there is no business need to do so. *Files arriving at establishments or NPS offices from other agencies, for example, police, which are **not** required, must be returned to the agency concerned.*

**CONTACT DETAILS:****1. Information Governance and Data Protection Team**

Address: Ministry of Justice  
 IGDP team  
 10<sup>th</sup> Floor  
 102 Petty France  
 LONDON  
 SW1H 9AJ

email [data.compliance@justice.gov.uk](mailto:data.compliance@justice.gov.uk)

**2. Disclosure Team**

Freedom of Information Requests/Environmental Information Requests and  
 Subject Access Requests from employees, ex-employees and members of the public:

Address: Ministry of Justice  
 Disclosure Team  
 10<sup>th</sup> Floor  
 102 Petty France  
 LONDON  
 SW1H 9AJ

e-mail: [data.access@justice.gov.uk](mailto:data.access@justice.gov.uk)

Website <https://intranet.justice.gov.uk/guidance/knowledge-information/providing-information-to-the-public/personal-data-under-the-data-protection-act/>

**3. Subject Access Requests from offenders and ex-offenders**

Address: Ministry of Justice  
 Data Protection Team  
 Branston Registry, Building 16  
 Supply and Transport Store  
 Burton Road  
 Branston  
 BURTON UPON TRENT  
 Staffordshire DE14 3EG

Information Line 01283 496066

Fax 01283 496179

Website <https://intranet.justice.gov.uk/guidance/knowledge-information/providing-information-to-the-public/personal-data-under-the-data-protection-act/>

e-mail [data.access@hmps.gsi.gov.uk](mailto:data.access@hmps.gsi.gov.uk)



#### 4. HMPPS Regulation Team – Equality Rights and Decency Group

Address: HMPPS Regulation Team  
Equality, Rights and Decency Group  
Point 4.05  
4<sup>th</sup> Floor 102 Petty France | London | SW1H 9EX

e-mail [noms\\_equalities@noms.gsi.gov.uk](mailto:noms_equalities@noms.gsi.gov.uk)

#### 5. HMPPS Agency Records Officer

Address: Information Management & Security  
Post Point 4.42  
4<sup>th</sup> Floor  
102 Petty France  
LONDON  
SW1H 9EX

Information Line 0203 3340324

Website [Information Policy and Assurance Guidance](#)

e-mail [informationmgmtsecurity@noms.gsi.gov.uk](mailto:informationmgmtsecurity@noms.gsi.gov.uk)

#### 6. HMPPS Information Policy and Assurance Team

Address: Information Management & Security Team  
Post Point 4.42  
102 Petty France  
LONDON  
SW1H 9EX

Information Line 0203 3340324

Website [Information Policy and Assurance Guidance](#)

e-mail [InformationmgmtSecurity@noms.gsi.gov.uk](mailto:InformationmgmtSecurity@noms.gsi.gov.uk)

#### 7. HMPPS National Litigation Unit and NOMS Safer Custody Casework Team

Address: HMPPS National Litigation Unit  
Equality, Rights and Decency Group  
Post Point 4.15  
4<sup>th</sup> Floor  
102 Petty France  
SW1H 9EX

e-mail [nlt@noms.gsi.gov.uk](mailto:nlt@noms.gsi.gov.uk)

**SUBJECT ACCESS REQUEST FORM: OFFENDER**

You should complete this form if you want us to supply you with a copy of personal data, which we hold about you. You are entitled to receive this information under the Data Protection Act 2018.

You should send your request and proof of your identity to Ministry of Justice, Branston Registry, Building 16, S & T Store, Burton Road, Branston, Burton-on-Trent, Staffordshire, DE14 3EG.

We will endeavour to respond promptly and in any event within one month of the request being approved, i.e., if necessary confirmation of identity and any further information required to proceed with your request.

To proceed with your subject access request, we require your: -

**Full Name:**

**Establishment(s) and/or probation offices:**

**Your Date of Birth:**

**Your Prison Number(s):**

**Date of Sentence:**

**Description of the type of personal data, which you are seeking and the dates for which we should search.**

If we are not satisfied that you are who you say you are we reserve the right to refuse to grant your request.

If the information you request reveals details, directly or indirectly, about another person we will usually be required to remove them out.

I confirm that I have read and understood the terms of this subject access form.

**Signed.....**

**Dated.....**