HM Prison & Probation Service

Code of Practice

Electronic Monitoring Data

March 2024

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at:

Electronic Monitoring Team

102 Petty France,

London

SW1H 9AJ

Print ISBN [ ]
Web ISBN [ ]
ID [ ] [ ] / [ ]

Printed on paper containing 75% recycled fibre content minimum.

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty’s Stationery Office

Contents

Purpose

1. In accordance with the provisions of specific legislation (including but not limited to section 62B of the Criminal Justice and Courts Act 2000 and section 395(1) of the Sentencing Act 2020), the Secretary of State for Justice is required to issue a Code of Practice relating to the processing of personal data gathered in the course of electronic monitoring imposed as part of relevant court orders or a licence on release from prison or youth detention accommodation.

2. The issuing of this Code of Practice fulfils those requirements so far as the processing of electronic monitoring data concerns personal data. It clarifies the expectations, safeguards and broad responsibilities for the collection, retention, processing and sharing of electronic monitoring data where it is personal data. The original Code, which was published in February 2018 and updated in October 2020, was drafted in consultation with Ministry of Justice (MoJ) colleagues and stakeholders including:

   The Information Commissioner's Office;
   The Police;
   The Youth Justice Board; and
   The Parole Board

3. This version of the Code makes some minor amendments to reflect the current electronic monitoring landscape and to anticipate further legislation on its use. However, the vast majority of the Code and fundamental principles of data protection compliance remain unchanged.

4. The Code is provided to help Data Controllers and Data Processors involved in electronic monitoring of persons subject to relevant orders/licences to understand the data protection legal framework and adopt good practice. Its content does not seek to remove or replace any of the contractual provisions that are in place for service providers. Failure to observe the Code does not of itself make someone liable in either criminal or civil proceedings, however breach of data protection or other laws may incur liability.

The legal framework

5. The legal framework for the imposition of electronic monitoring as part of orders/licences in scope of this document is set out in a number of different statutes covering different types of order. These include the Criminal Justice and Courts Services Act 2000, the Criminal Justice Act 2003, the Crime and Courts Act 2013, the Criminal Justice and Courts Act 2015 and the Sentencing Act 2020.

6. Electronic monitoring data in scope of this Code is collected and processed for law enforcement purposes, specifically the prevention of crime, execution of criminal penalties and safeguarding against the prevention of threats to public security. Therefore Part 3 of the Data Protection Act 2018 applies. Where necessary and proportionate to do so, information may be shared with relevant

Agencies or public bodies for other purposes, including other law enforcement purposes such as, investigation, detection or prosecution of criminal offences. Personal data will only be shared if it is justified and proportionate, where it is lawfully permitted or where an exemption to the prohibition on sharing applies. Processing shall be in compliance with the provisions of data protection legislation. Further information on data sharing is set out in paragraphs 23 to 34.

7. Where the electronic monitoring data processed constitutes personal data as defined in data protection legislation, the processing of it must comply with the six data protection principles contained in Part 3 of the Data Protection Act 2018, which require that it must be:
   - Processed fairly and lawfully;
   - Processed for specified, explicit, and legitimate purposes and not processed in a manner that is incompatible with those purposes;
   - Adequate, relevant and not excessive;
   - Accurate, and where necessary kept up to date;
   - Not kept for longer than is necessary;
   - Processed in a manner that ensures appropriate security;

8. It is recognised that the processing of personal data engages Article 8 of the European Convention on Human Rights i.e. the right to respect for private and family life. However, Article 8 is not an absolute right and public authorities are permitted to interfere with it if it is lawful and proportionate to do so and necessary in the interests of national security, public safety or for the prevention of disorder or crime.

9. The MoJ considers that it is both lawful and proportionate to process personal data for the purposes of complying with relevant electronic monitoring orders/licences issued under relevant legislation.

Imposing an electronic monitoring requirement or condition

10. It is a decision for the Courts whether to impose an electronic monitoring requirement as part of a Court Order and it is incumbent upon them to consider any statutory safeguards and issues of fairness and proportionality.

11. An electronic monitoring condition may also be imposed on a release licence, by the Parole Board or by the Secretary of State through the governor/director of a prison/ young offender institution or the Youth Custody Service's (YCS) Release and Resettlement Team. For adults, licence conditions will be set in consultation with probation providers. For children and young people, licence conditions or notice of supervision (NoS) requirements are set in consultation with the relevant Youth Offending Team (YOT). In accordance with His Majesty's Prison and Probation Service (HMPPS) policy, the aims of the licence period are to protect the public, to prevent re-offending and to secure the successful re-integration of the offender into the community. Licence conditions should be preventative as opposed to punitive and must be proportionate, reasonable and necessary.

However, the mandatory curfew imposed under the Home Detention Curfew (HDC) is also punitive in that it reflects the fact that the prisoner is still serving the custodial element of the sentence.

12. For adult offenders, the body with authority to add, remove and amend licence conditions after release will depend on a number of factors including the type of sentence and who has authority to direct release of the offender. However broadly this will be one of the Parole Board or, on behalf of the Secretary of State, the Probation Service or HMPPS Public Protection Casework Section (PPCS).

13. For determinate sentenced offenders under the age of 18, YOTs may request additional licence conditions or NoS requirements. All requests for additional conditions/requirements are approved by the Secretary of State for Justice. This responsibility has been delegated to Governors for children placed in Young Offenders Institutions (YOIs) and to the YCS's Sentence and Release Team for children placed in Secure Training Centres (STCs) and Secure Children's Homes (SCHs).

The data and monitoring the requirement / condition

14. The MoJ has contracted for electronic monitoring services including the provision of equipment, field service and monitoring service. The field service is responsible for fitting / removing the necessary equipment and inducting subjects on the electronic monitoring requirements. The monitoring service monitors subjects' compliance with the requirements imposed by relevant orders/licences and reports violations to the appropriate supervising/enforcement agency.

15. The personal data processed by electronic monitoring contractors will be that which is necessary to:

- Ensure the right subject is electronically monitored;
- Monitor subjects' compliance with the relevant orders/licences.
- Monitor subjects' location in accordance with a court order or licence requirement;
- Ensure the contractor is able to discharge its contractual obligations and to allow for the monitoring of its performance against contractual requirements;
- Safeguard the public and staff e.g. recording details of any behaviour by the subject or others at the premises that is relevant to the risk assessment of safety and sharing this information where appropriate;
- Assist the MoJ in meeting its obligations under the Equality Act 2010;
- Inform the MoJ about the use of electronic monitoring across the legislative landscape and to evaluate activity/ effectiveness.
- Lawfully respond to enquiries from, for example, public bodies and Criminal Justice Agencies.

16. Contractors who provide equipment are not required to interrogate the personal data held in systems. However, they may need to access the systems for the purposes of maintenance and assurance. Contractual requirements are in place to ensure any personal data accessed by contractors for these purposes is dealt with in accordance with data protection law.

17. The data will only be processed in accordance with data protection legislation. Unless an exemption within the Data Protection Act 2018 applies, or there is another lawful basis permitting the processing, the data will only be processed for the purposes set out in paragraph 16 and 17. Security and access to data are restricted in accordance with legislation and guidance produced in association with this. Only the necessary amount of personal data will be shared for the purposes of meeting the requirements set out above.

Location and Curfew Monitoring

18. Where the relevant order/licence includes an electronic location monitoring requirement/condition, the subject will be fitted with a location monitoring enabled tag. The location monitoring hardware and associated software will capture the subject's location throughout the day in order to monitor compliance with the order/licence. However, where location monitoring is only imposed to monitor a specific requirement/condition, such as an exclusion zone, active monitoring (i.e. reviewing the data rather than the data simply sitting in the system) of the location information will only take place if there is a lawful reason to do so e.g. following a breach of the requirement/condition and only where it is proportionate and necessary. It will not be actively monitored at other times. This will be explained to the subject as part of a privacy notice that will be issued on induction (see paragraph 22).

19. If the subject has been given a whereabouts monitoring requirement (i.e. a location monitoring requirement imposed other than for the purpose of monitoring the subject's compliance with any other requirement and referred to by the MoJ as trail monitoring) all the location data captured may be evaluated by the agency responsible for supervising the order or licence.

20. Curfew requirements will be monitored through radio frequency (RF) technology. In cases where the subject has both a location monitoring requirement and an electronically monitored curfew requirement, they will be fitted with a location monitoring enabled tag which will also allow for the curfew to be monitored using RF technology. In cases where subjects are given a curfew but not a location monitoring requirement, they will be fitted with an RF only enabled tag. The tag in each case will communicate with a unit installed in the subject's place of residence and the system will capture each time they enter or exit the property. In addition, the movements of a subject may be captured if and when the individual passes a location where another unit has been installed, as it will read the presence of any RF tags within the immediate vicinity. Data captured outside of curfew hours will not be processed further unless there is a lawful reason and only where it is necessary and proportionate to do so.

Alcohol Monitoring

21. If a subject has an electronic alcohol monitoring requirement imposed, they will be fitted with a tag that measures the alcohol content in their body via their perspiration. The information gathered will be shared with the relevant supervising or enforcement agency.

Sharing information

22. All electronic monitoring subjects will, on induction, receive a Privacy Notice, in compliance with data protection legislation, which explains the legal basis for the processing of their personal data and their data protection rights. The notice will explain the types of data that may be collected and, where necessary and proportionate to do so, this data may be shared with Criminal Justice Agencies for specific purposes.

23. Personal data must only be shared where it is permitted by law and is justified, necessary and proportionate to do so. It is the responsibility of the Data Controllers identified later in this document, to ensure that there is a lawful gateway and basis for the sharing of data.

24. For example, for the purposes of convicted individuals, there are express powers within the Offender Management Act 2007 that allow for the sharing of offender information by specific parties for specific purposes. Section 14(4) of the Offender Management Act 2007 provides that the sharing of information is permitted where it is necessary or expedient for the following purposes:

- probation purposes;
- the performance of functions relating to prisons and prisoners;
- any other purposes connected with the management of offenders (including the development or assessment of policies relating to matters connected with the management of offenders).

25. Also, section 36(3) of the Data Protection Act 2018 permits personal data collected for a law enforcement purpose to be processed for another law enforcement purpose (whether by the controller that collected the data or by another controller) provided that the controller is authorised by law to process the data for that purpose and the processing is necessary and proportionate to that other purpose.

26. As a government department headed by a Minister of the Crown, the MoJ may in some instances be able to rely on common law powers to share data.

27. Notifying organisations including HMCTS, prisons, young offender institutions and the Probation Service, will be able to send orders through to the EM contractor by secure means.

28. Agencies with the responsibility to supervise/enforce the orders/licences will be given or have access to electronic monitoring data via the telephone, secure email or secure web based systems for the purposes for which it was obtained. So, for example:

- The MoJ have access to all records and reports for the purposes set out in paragraph 16, including monitoring compliance with the contractual provision and discharging its duty as a Data Controller. Access will be limited on a need to know basis and in accordance with data protection legislation.
- Probation providers will be given electronic monitoring data gathered on Orders/licences where they act as the Responsible Officer, supervising officer or enforcement agency for that subject on that particular Order/licence.
- PPCS will be given data on offenders released on licence from prison custody and will pass information onto supervising officers for purposes of managing the offender or to the Parole Board as evidence for recall to custody or to inform release decisions, where relevant;
- The MoJ HDC Appeals Team will be given data on offenders recalled to prison from release on HDC, and will occasionally pass data onto contracted forensic experts in order to determine the cause of damage to the EM equipment;
- The Police will be given data on the cases where they act as the responsible agency e.g. court bail and some civil orders. Where it is proportionate and necessary, data will also be disclosed to Police Forces to assist with investigations or to help prevent or detect crime. In addition, data may be provided to assist with assessing risk, managing resources and compliance of subjects such as those subject to Integrated Offender Management processes or Multi Agency Public Protection Arrangements. Data may also be shared to assist in the apprehension of a subject following a breach of their electronic monitoring condition, or where there is another reason to arrest, or to locate an individual for the purposes of safeguarding life or property.

29. When requested, where lawful, necessary and proportionate, subject's personal data may be shared with those organisations and other public authorities without the subject's consent.

30. Information may also be disclosed to a wider range of requestors under Part 3 of the DPA or under GDPR e.g. a solicitor acting on behalf of the subject, if the subject provides their consent.

31. Information will only be released if lawful and in accordance with data protection legislation unless otherwise directed by a Court. Any information disclosed must only be used for the purpose(s) for which it was disclosed and it must not be further processed in a manner that would be incompatible with that purpose(s).

32. Electronic monitoring contractors will not have direct access to information held on stakeholder systems, but relevant information will be shared via telephone, or secure means. This includes sharing information relating to the risk the subject

may pose to others where it is necessary and relevant for the protection and safeguarding of staff and the public. Information may also be shared for statutory safeguarding purposes or to report potential criminal behaviour.

Subject Access Requests

33. Individuals who are subject to electronic monitoring conditions or requirements are entitled under the data protection laws, 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. Subjects will be provided with the relevant contact details as part of their electronic monitoring induction.

Freedom of Information Requests

34. All Data Controllers that are public authorities in this process, are subject to the provisions of Freedom of Information Act 2000 and shall assist and co-operate to enable each other to comply with their respective statutory duties in relation to requests for Information. Electronic monitoring contractors are under a contractual duty to provide the information required to enable the MoJ to respond to an FOI request. Any requests for information in relation to the electronic monitoring service should be submitted to the following email address:

data.access@justice.gov.uk

Transmitting data

35. Data transferred from electronic monitoring equipment to the monitoring centre will be encrypted during transit and will remain so whilst retained. All data shared by electronic monitoring contractors with stakeholders will be via, telephone, secure email or secure portal. Data transmitted to any portal will be encrypted during transit and will remain so whilst retained. In addition, supervising/enforcing organisations may receive an alert via SMS from contractors to look at their email or relevant portal.
36. All communications with stakeholders must accord to the Government Security Classification tier for the data being shared which will usually be ‘Official’. Parties carrying out the functions outlined in this Code should make themselves aware of, and adhere to, their organisation’s information security policies and procedures in regard to processing data in a manner appropriate for the assigned security classification.
37. All staff have a duty of confidentiality and a personal responsibility to safeguard any information with which they are entrusted. This includes ensuring that they comply with the legal and regulatory requirements and standards, for example the encryption of personal data on removable media.

Data compromise or loss

38. Data protection laws require stakeholders who are Data Controllers and processers to appropriately handle and protect data. Those same demands also require stakeholders to report, manage, and in some cases report, breach events to the Information Commissioner where data requiring protection is either lost or compromised, damaged, destroyed or processed unlawfully. Every staff member, irrespective of role, grade, or location, is required to report an event involving loss or compromise of data. All stakeholders should ensure that their staff understand what constitutes a data breach, and that this is more than a loss of personal data. Stakeholders should also ensure that they have an internal breach reporting procedure in place to help decision-making about whether a breach should be notified to the Information Commissioner.

39. 'Lost' is defined as information where the location is unknown (this can be both internally and externally) or where its suspected location is out of the stakeholder's control.

40. 'Compromise' is defined as information that has been subject to unauthorised access, use, modification or corruption.

41. All stakeholders must follow their local policies on reporting a compromise or loss of data. In addition, where this concerns shared MoJ data, the stakeholder must inform the MoJ Electronic Monitoring Directorate as soon as possible, or no later than 24 hours after the compromise / loss is identified.

42. On being notified of the possible incident, the controller (see section on data protection roles) reporting the incident must establish whether it is a potential significant incident. Some of the factors to consider include:

    - the nature of the information (is it personal information or sensitive corporate information?)
    - the number of individual records involved (if personal information)
    - the possible impact of the incident, including the apparent risk to the individuals, their families (for instance, children), staff, victims, offenders under supervision, members of the public and MoJ's operations or reputation;

43. If a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the Data Controller responsible for the data must notify the breach to the Information Commissioner, without undue delay, and where feasible, not later than 72 hours after becoming aware of it. If, by exception, a decision is taken not to notify the Information Commissioner, the reasons should be recorded and made available to the Information Commissioner on request.

44. If the incident is considered serious or impacting, the lead manager must immediately inform the appropriate Senior Official through the management line. All contracted providers should report the incident through the contractual line

(designated contract manager). An investigation should take place into the circumstances of the breach to ensure that lessons are learned and shared where necessary. Where appropriate action should be taken to mitigate the effect on the data subject, including by informing them what has happened and assisting them in mitigating actions they wish to undertake themselves.

Data rectification and erasure

45. Should stakeholders become aware that a subject's personal data is inaccurate or incomplete, they must take reasonable steps to rectify the situation.

46. If stakeholders identify that the processing of data infringes the principles set out in paragraph 7 above, then unless the data is required as evidence, the Data Controller should be asked to consider its erasure.

47. If the subject requests rectification or erasure of their personal data, then the relevant party must respond to the subject informing them of the outcome of their request. Should the request be refused the subject must be informed of their right to take the matter up with the Information Commissioner and/or the Court.

Holding and retaining data

Holding Data

48. All stakeholders must hold the data securely in accordance with relevant policies or detailed technical specifications within relevant contracts. These provisions must accord with Cabinet Office security standards and the Data Protection Act 2018.

49. All stakeholders must ensure the integrity and confidentiality of the information they hold. All staff that have access to the information must be suitably trained, be security cleared at the appropriate level for the information that they handle and comply with the Official Secrets Act 1989. Access to the data must only be by those who have a legitimate need to review the data. Inappropriately accessing or processing the data without the Data Controller's knowledge may constitute a criminal offence.

50. In accordance with Data Protection legislation, personal data must not be held outside of the European Economic Area.

Retaining Data

51. All Data Controllers carrying out the functions set out in this Code must adhere to their organisation's record management policies and procedures specifically in relation to retention and destruction of data. Such policies and procedures must be compliant with data protection legislation. Personal data must not be held for longer than is necessary for the purposes it was collected for.

52. Subject's personal electronic monitoring data will be held by the relevant contractor for up to 6 years post order end unless there is a lawful reason to hold it for longer, such as an ongoing investigation. Thereafter, it will be securely destroyed.

Data protection and processing roles

53. A **Data Controller** is a competent authority (as defined by the Data Protection Act) that**,** either alone or jointly, determines the purposes for which, and the means by which, any personal data are, or are to be processed. It is the Data Controller that must exercise control over the processing and carry data protection responsibility for it.

54. A **Data Processor** in relation to personal data, is any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller. **Processing**, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- collection, recording, organisation, structuring or storage,
- adaptation or alteration,
- retrieval, consultation or use,
- disclosure by transmission, dissemination or otherwise making available,
- alignment or combination, or
- restriction, erasure or destruction.

55. The MoJ is a Data Controller of electronic monitoring information where it determines the purposes for which data are processed for electronic monitoring of subjects on orders and licences. The MoJ is the parent Department of HMCTS and HMPPS (which includes public sector Prisons and the Probation Service).

56. The Home Office may also be a Data Controller for civil orders where it determines the purpose for which and the manner in which the data is processed.

57. Where electronic monitoring data is passed to an organisation outside of the MoJ for specific, lawful purposes, that organisation will be the Data Controller of the information in its possession for those purposes.

58. Each Data Controller has full data protection responsibility to safeguard any personal information or data to which they have access and to ensure confidentiality. They will be responsible for maintaining control and security of the information within their organisation's systems.

59. The Data Processors of the electronic monitoring information will be the appointed electronic monitoring contractors responsible for collating and disseminating subject's personal information on behalf of the Data Controller in accordance with the purposes identified in paragraphs 16 and 17 above.

60. All parties must ensure that significant decisions affecting subjects are not based solely on automated processing. If such decisions are made solely by automated processing, then the subject should be informed and has the right to request that the decision is reconsidered or taken again not based on solely automated processing (see sections 49 and 50 of the DPA 2018 for further information).

Pilot activity

61. The MoJ and others may pilot the use of electronic monitoring to test its effectiveness and inform future policy. The pilots will accord with the provisions of the data protection laws and contractual and/or technical safeguards will be in place to ensure that personal data is only accessed and shared where there is lawful reason to do so.

Barcode goes here:

2.93cm (h)
3.74cm (w)
16.2cm to the right of page
25.1 below page