HM Prison & Probation Service

Code of Practice

Electronic Monitoring Data

October 2020

Code of Practice

Electronic Monitoring Data

Electronic Monitoring Directorate

October 2020

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

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

Electronic Monitoring Directorate

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 the Criminal Justice Act 2003 [1] (as amended by the Crime and Courts Act 2013), the Secretary of State is required to issue a Code of Practice relating to the processing of personal data gathered in the course of electronic monitoring of persons serving a community order or suspended sentence with an electronic monitoring requirement.

2. In addition, the provisions of the Criminal Justice and Courts Services Act 2000[2], require the Secretary of State to issue a Code of Practice relating to the processing of data gathered in the course of electronic monitoring of persons with an electronic monitoring condition as part of a licence on release from prison or youth detention accommodation.

3. The issuing of this Code of Practice fulfils both requirements (as set out in paragraphs 1 and 2 above) 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. It has been drafted in consultation with MoJ colleagues and stakeholders including:

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

4. In accordance with the legislative requirements for this Code, its contents are not legally binding on any party. It 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.

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 the Criminal Justice and Courts Services Act 2000, the Criminal Justice Act 2003, the Offender Management Act 2007, the Crime and Courts Act 2013 and the Criminal Justice and Courts Act 2015.

[1] Section 215A

[2] Section 62B (as inserted by the Criminal Justice and Courts Act 2015)

6. Electronic monitoring data 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 for other law enforcement purposes such as, investigation, detection or prosecution of criminal offences. 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 the legislation referred to above. 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, and processing shall be in compliance with the provisions of data protection legislation for law enforcement purposes.

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 be imposed on a 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 Services Release and Resettlement Team. Licence conditions will be set in consultation with probation providers, or in the case of a youth the Youth Offending Team (YOT). In accordance with Her 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 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 National Probation Service (NPS) or Public Protection Casework Section (PPCS).

13. For determinate sentenced offenders under the age of 18, youth offending teams may recommend licence variations which are then submitted to the governor of a young offender institution or, for those released from secure training centres or secure children's homes, the Youth Custody Services Release and Resettlement Team for approval.

THE DATA AND MONITORING THE REQUIREMENT / CONDITION

14. The MoJ has contracted for electronic monitoring services i.e. the field services to fit and remove the necessary equipment, induct subjects on the requirements, the monitoring of their compliance with those requirements and the reporting of breaches to the appropriate supervising/enforcement agency. Not all contractors will perform all of those functions and some will not have access to subject's personal data.

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

- Ensure the right subject is tagged;
- 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.
- Lawfully respond to enquiries from Criminal Justice Agencies.

16. 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 15. 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

17. 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 24 hours a day in 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 Fair Processing Notice (see paragraph 21).

18. If the subject has been given a standalone electronic location monitoring requirement (i.e. one imposed otherwise 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.

19. 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.

20. If the subject has an electronic alcohol monitoring requirement imposed they will be fitted with a tag that measures the alcohol content in their bodies' perspiration.

SHARING INFORMATION

21. All electronic monitoring subjects will, on induction, receive a Fair Processing Notice, in compliance with data protection legislation, which explains the legal basis for the processing of their personal data and will explain the data subject's 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.

22. 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 basis for the sharing of data.

23. 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).

24. 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.

25. 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.

26. 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 and/or an electronic Portal, captured on those orders for the purposes for which it was obtained. So, for example:

- The MoJ have access to all records and reports for the purposes of monitoring compliance with the contract. Access will be in accordance with the GDPR.
- Probation providers will have access to 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.
- Prisons will be able to submit electronic monitoring notifications via email or onto the Portal;
- PPCS will have access to 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 have access to 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;
- Her Majesty's Courts and Tribunals Service (HMCTS) will be able to submit electronic monitoring notifications to EMS and alert EMS to any necessary amendments or variations to orders;
- Where it is proportionate and necessary, data will be disclosed to Police Forces to assist with the investigation, prevention and detection of crime. They may also be given data to assist with assessing risk and managing compliance of subjects such as those subject to 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.

27. 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.

28. 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.

29. 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).

30. Electronic monitoring contractors will not have direct access to information held on stakeholder systems, but relevant information will be shared via telephone, secure email or the Portal. 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

31. 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 should they wish to submit a SAR as part of their electronic monitoring induction.

Freedom of Information Requests

32. 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 Department 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

33. Data transferred from electronic monitoring tags 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 an electronic monitoring portal. Data transmitted to the 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 the portal.
34. 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 regards to processing data in a manner appropriate for the assigned security classification.
35. 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

36. 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.

37. '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.

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

39. 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.

40. 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;

41. 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.

42. 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

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

44. 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.

45. 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

46. 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.

47. 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.

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

Retaining Data

49. All data controllers carrying out the functions set out in this Code of Practice 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.

50. 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

51. 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.

52. 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.

53. The MoJ is the Data Controller of electronic monitoring information as 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 NPS).

54. 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.

55. 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.

56. 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 MoJ in accordance with the purposes identified in paragraph 15 above.

57. All parties above 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).

HOME DETENTION CURFEW

Adult Offenders

58. Offenders serving sentences of imprisonment of less than four years who are released early on HDC not only have an electronically monitored curfew but general licence conditions intended to protect the public, to prevent re-offending and to secure the successful re-integration of the offender into the community. The curfew conditions expire at the half way point of the sentence, but general conditions remain in force until the end of the sentence.

59. The appointed electronic monitoring contractor for HDC cases will monitor the curfew conditions and are permitted by reference to terms of the licence to authorise an absence from a curfew address in clearly defined circumstances and issue warning letters for minor curfew breaches. All other non-compliance must be reported to PPCS to consider whether a recall to prison custody is necessary.

60. Supervising Officers (probation practitioners) are responsible for supervising the general licence conditions and for reporting any breaches of those conditions to PPCS.

Under 18s

61. Children (under 18s) serving a sentence of detention under section 91 of the Powers of Criminal Courts (Sentencing) Act 2000 may be released on HDC. The curfew condition is monitored by the appointed electronic monitoring contractor and all non-compliance events are reported to the YOT to consider whether the matter should be taken to Court for enforcement action.

ELECTRONIC MONITORING CURFEW ONLY COMMUNITY SENTENCES

62. The appointed electronic monitoring contractor act as the Responsible Officer for electronically monitored curfew only community sentences. Serious violations of those orders are reported to the appropriate probation body to take enforcement action.

PILOT ACTIVITY

63. 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. A Data Protection Impact Assessment would be considered as part of any Pilot.

Barcode goes here:

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