Management of Offenders Bill – Electronic Monitoring Provisions

Privacy Impact Assessment (PIA)

February 2018

Scottish Government
Riaghaltas na h-Alba
gov.scot

Management of Offenders Bill – Electronic Monitoring Provisions

Privacy Impact Assessment (PIA)

1. Introduction

The purpose of this document is to report on and assess against any potential Privacy Impacts as a result of the electronic monitoring provisions of the Management of Offenders Bill.

2. Document metadata

2.1 Privacy Impact Assessment for the Electronic Monitoring provisions of the Management of Offenders Bill.

2.2 Date of report: 08 February 2018

2.3 Author of report Jamie Begbie

2.4 Information Asset Owner (IAO) of relevant business unit: Linda Pollock, Deputy Director

2.5 Date for review of Privacy Impact Assessment (PIA): 01 June 2018

3. Description of the project

3.1 The Scottish Government is committed to strengthening the delivery of community justice, ensuring we continue to focus on public safety, and breaking the cycle of reoffending. We believe that electronic monitoring has a role to play in supporting our vision for a safer, fairer and more inclusive nation, in which those who have been victims of crime can feel safer and more reassured, and those with a history of offending can be supported to be active and responsible contributors to their communities.

3.1.1 Electronic monitoring was first piloted in Scotland in 1998, before being rolled out nationally in 2002 as a Restriction of Liberty Order (RLO), which is imposed only by courts. Since then, confidence has grown in the technology involved, and understanding has developed as to how electronic monitoring could be used more widely.

3.1.2 At present, legislation allows for electronic monitoring to be used in Scotland to monitor an individual's compliance with a curfew set by either the Scottish Courts and Tribunal Service, the Scottish Prison Service or the Parole Board for Scotland.

3.1.3 At present, a person can be curfewed to an address for up to 12 hours a day or - more rarely - 'away from' an address for up to 24 hours a day. Currently in Scotland there are approximately 1280 people being electronically monitored.

3.1.4 Following a Scottish Government consultation on the development of electronic monitoring in Scotland in 2013[1], an Electronic Monitoring Expert Group was established to consider how electronic monitoring could be better used within the criminal justice system in Scotland. The Group published a report in October 2016[2] which set out eight recommendations on how to take this forward.

3.1.5 On the back of the report of the Working Group we published a further consultation seeking views in relation to potential legislative changes to extend the use of electronic monitoring in Scotland[3]. That consultation closed on 13 May 2017 and 63 responses were received. Analysis of the responses received to the consultation was published on the Scottish Government website on 12 September 2017[4].

3.1.6 The expansion of electronic monitoring, including use of new technologies, will increase the options available to manage and monitor offenders in the community and further protect public safety.

3.1.7 We are currently working with partners to develop the new electronic monitoring legislation taking into account the recommendations of the Working Group and the responses to the consultation. The electronic monitoring provisions in the Management of Offenders bill will enable the wider use of electronic monitoring in community sentencing along with the introduction of new technologies.

3.1.8 This Privacy Impact Assessment relates only to the provisions as set out in Part 1 of the Management of Offenders (Scotland) Bill.

3.1.9 Detail of how the data for monitoring compliance with an electronic monitoring condition is collected, stored and disposed of will be set out in the Electronic Monitoring Contract, which will take effect from 1 April 2020. A Privacy Impact Assessment for the new electronic monitoring contract to be prepared during the procurement process.

3.2 Under the existing electronic monitoring schemes, Scottish Ministers are the data controllers. Scottish Ministers by contract have designated a Service Provider to manage the service on their behalf. This includes processing the data of those subject to electronic monitoring.

3.2.1 To ensure the effective operation of the electronic monitoring scheme, the collection and use of personal and sensitive, data will be necessary. Data such as the name, address and date of birth of an individual will be provided, along with, in some instances, details of the individual's offence and sentence. This allows the

---

[1] http://www.gov.scot/Publications/2014/10/7132
[2] http://www.gov.scot/Publications/2016/10/8620
[3] http://www.gov.scot/Publications/2017/03/6021
[4] http://www.gov.scot/Publications/2017/09/2305

provider to create and maintain a record of the individual. In addition to the data provided, the service provider will collect information related to the individual's compliance with their requirements.

3.2.2 The provisions of the Bill will not alter the current contract with the service provider but will enable the introduction of new technologies to carry out monitoring of compliance (i.e. Global Positioning System (GPS) and substance monitoring technologies).

3.2.3 Any future GPS scheme would provide specific location data, and substance monitoring would provide additional data in relation to an individual's consumption of alcohol or drugs. However, this data will only be collected to ensure an individual is complying with the requirements placed on them. Additionally, the introduction of any new technology will require additional secondary legislation which will be accompanied by further specific impact assessments.

3.3 All data held by the service provider is stored on their IT equipment, subject to the data security provisions set out in the contract with Scottish Ministers. Only staff employed by the service provider and Scottish Government staff employed to manage the contract will have access to it. All data is and will be owned by the Scottish Ministers, managed by the service provider under contract.

3.3.1 As part of the contractual assurance process, Scottish Government staff conduct regular audits to ensure the accuracy of data held. In addition, assurance of the accuracy of the technology is sought from the service provider. A Privacy Impact Assessment will be carried out separately prior to the award of any new contract..

3.4 Any data shared currently is set out in the electronic monitoring contract. This allows the service provider to provide updates to the authority (i.e. the Scottish Court and Tribunals Service) that made the electronic monitoring order. The Bill states the general purpose of electronic monitoring (both in the context of electronic monitoring imposed by the court and by Ministers) and the powers in the Bill to make subordinate-legislation will enable the Scottish Ministers specify the organisations with which the data may be shared. Data sharing agreements will be entered into between the Scottish Ministers and the relevant organisations.

3.4.1 Data obtained by virtue of electronic monitoring may not be shared with any person except in accordance with—

- the Bill and subordinate legislation made under the Bill;
- the Freedom Information (Scotland) Act (2002); and
- the Data Protection Act 1998 and any successive legislation introduced by the UK Government in order to implement the EU General Data Protection Regulations.

3.4.5 Any requests for information under the above legislation will be considered by the Scottish Government Contract Manager. The Service Provider will not release any requested information unless authorised by the Scottish Government Contract Manager.

4. Stakeholder analysis and consultation

4.1 Under the Bill, an electronic monitoring requirement can be imposed by the court in relation to criminal proceedings or by the Scottish Ministers in relation to the early or temporary release of a prisoner from imprisonment or detention. A copy of the electronic monitoring requirement will be sent to G4S, the current service provider, who are responsible for the installation and maintenance of the equipment used to monitor the compliance with the electronic monitoring requirement.

4.2 Whilst making this PIA the following organisations were consulted with through a stakeholder engagement event:

Scottish Prison Service
Scottish Womens Aid
Turning Point
Positive Prison
Scottish Courts and Tribunal Service
Victim Support Scotland
Scottish Children's Reporter Administration

4.3 The outputs from the stakeholder discussion were shared with the group to ensure that all of the key issues from the session were captured. They were informed that the outputs from the session would help inform the content of the final PIA. The stakeholder group will be informed once the PIA is published on the Scottish Government website.

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations: As above the administration of electronic monitoring will involve Scottish Government, G4S (the current service provider), the Scottish Court and Tribunals Service, Scottish Prison Service and Parole Board Scotland.

5.2 Anonymity: The data from electronic monitoring is not shared beyond the Data Controller, Service Provider, the organisation that makes the order for electronic monitoring and a supervising officer designated by the court to support an individual's compliance with an electronic monitoring condition i.e. Criminal Justice Social Work. It would not be possible for anyone beyond that to identify any individual. Certain statistical information may be made available such as the current number of orders made and number of orders completed.

5.3 Technology: New technologies are being considered, in particular the introduction of GPS to monitor an individual's actual movement. The introduction of technologies to monitor an individual's consumption of alcohol is also being considered.

5.4 Identification methods:

- The Service Provider will continue to use the current method for providing identifiers to monitored individuals.
-
- There will be no new or substantially changed identity authentication requirements.

- The unique identifiers used are the person's name along with a five digit identifier. This information is not made publicly available and therefore should not have the effect of enabling identification of persons who were previously anonymous. The contract with the current service provider contains a confidentiality clause, which prevents, subject to the provisions of the Data Protection Act, the release and/or publication of any data obtained by the service provider in carrying out its functions under the contract.

5.5 Personal data

- There is no intention to make new or significant changes to the handling of types of personal data which could be of particular concern to individuals. In some instances information could be shared with a supervising officer i.e. Criminal Justice Social Work who has been designated by the court to provide support to the individual. This information will be around potential breaches of the electronic monitoring condition. Any information shared will always be under an appropriate data sharing provision.

- There is no intention to introduce a new database or to change the handling arrangements for the data.

- There will be no new or significant changes to the handling of personal data about a large number of individuals.

- There will be no new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources.

- The project will not involve the linkage of personal data with data in other collections.

5.6 Changes to data handling procedures

- Data is collected to ensure compliance with the electronic monitoring requirement (i.e. to wear and refrain from tampering with an electronic tag) and the underlying measures which are being monitored (i.e. court order or licence conditions). The introduction of new technologies may provide large quantities of data. Currently the data collected is reviewed and, where no longer necessary, disposed of in compliance with the requirements set out in the electronic monitoring contract. The requirements set out in the current contract follow the data protection principles. Also consideration will be given to Part 3 of the Data Protection Bill which applies to all processing for law enforcement purposes.

- We do not intend to make any changes to the data quality assurance processes or standards for any new technology introduced.

- We have no intention of changing data security access or disclosure arrangements. The introduction of new technologies will be handled in line with the current requirements. Information will not be disclosed beyond the current organisations (see Para5.2). The current contract sets out the security access requirements for any systems that hold personal data.

- Any new or changed data retention arrangements set out in the contract will follow the data protection principles.

- There is already clear data retention rules stated within the current contract. These will be reviewed to ensure that they comply with data protection legislation.

- There will be no changes made to the medium of disclosure for publicly available information. Electronic Monitoring does not have routine disclosure. The only information that is disclosed is statistical information (i.e. the number of completed orders).

5.7 Statutory exemptions/protection

- No exemptions will apply other than those set out in the regulations of the incoming Law Enforcement Directive. Also consideration will be given to Part 3 of the Data Protection Bill which applies to all processing for law enforcement purposes.

- The bill does not involve systematic disclosure of personal data to, or access to personal data by, third parties that are not subject to comparable privacy regulation.

5.8 Justification

- The Electronic Monitoring in Scotland consultation was launched on 2 March 2017 and closed on 19 May 2017. The analysis of the consultation responses was published on the Scottish Government website in 12 September 2017.

- The expansion, and more detailed regulation, of electronic monitoring via the Bill which will increase the options available to courts when dealing with offenders and will increase the options available to Ministers and the Parole Board when releasing a prisoner from prison. The introduction of new electronic monitoring technologies, such as GPS, will enable the use of exclusion or inclusion zones thereby ensuring more closer scrutiny of offenders and offering victims significant reassurance.

- The expansion of electronic monitoring will also enable more targeted measures to be imposed on an offender taking into account their individual circumstances

and thereby increasing the effectiveness of those measures in reducing re-offending.

- The collection, use, retention and destruction of personal data in relation to an offender represents an interference with the ECHR Article 8 rights of the offender. The regulation-making powers in the Bill enable Ministers to regulate and thereby mitigate this interference by restricting when certain data can be collected and used.

5.9 Other risks

- No other risks have been identified through either the consultation or stakeholder engagement processes.

6. The Data Protection Act Principles

Principle 1
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

6.1.1 The processing of data for the purposes of electronic monitoring will be fair and lawful. The purpose of electronic monitoring is stated in section 1(4) and 5(4) of the Bill and this purpose must be explained to the offender by the court or Ministers as appropriate.

6.1.2 Individuals will sign a declaration which informs them about the use of their personal data. This is signed when the service provider fits their tag and monitoring unit. This will be reviewed in light of the EU Law Enforcement Directive and Part 3 of the Data Protection Bill.

6.1.3 There is a need to amend both privacy and data notices due to the introduction of the EU Law Enforcement Directive and Part 3 of the Data Protection Bill which applies to all processing for law enforcement purposes in May 2018.

6.1.4 Under current legislation the processing of data for the purposes of electronic monitoring is necessary for (1) in the case of personal data, compliance with a legal obligation to which the data controller is subject; (2) the administration of justice; (3) the exercise of any functions conferred on any person by or under an enactment; or (4) the exercise of any functions of the Crown, a Minister of the Crown or a government department.

6.1.5 Consideration must also be given to the Convention Rights of offenders who are subject to electronic monitoring. Electronic monitoring would constitute an interference with the Article 8 rights of the offender (right to respect for private and family life). This interference is justified as it is backed up with robust legislative measures, is for the purpose of public safety and preventing crime or disorder, and is a proportionate means of achieving that purpose.

Principle 2
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

6.2.1 The purpose of electronic monitoring is stated in section 1(4) and 5(4) of the Bill and this purpose must be explained to the offender by the court or Ministers as appropriate. The Scottish Ministers are therefore restricted in how the data can be processed and further regulation of the processing of personal data for the purposes of electronic monitoring can be achieved through subordinate legislation. Any subordinate legislation to further regulate the processing of data is therefore restricted by this over-arching purpose.

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

6.3.1 The extent of the information collected by virtue of electronic monitoring will be determined by the nature of the device used. GPS monitoring will clearly result in the acquisition of more personal data than RF monitoring. All personal data collected must relate to the monitoring of an individual's compliance with an electronic monitoring requirement and the underlying court disposal or licence conditions. Subordinate legislation made under the Bill will be able to restrict the use of GPS monitoring so that it is not used in circumstances where the collection of specific information about an offender's whereabouts would be inappropriate.

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

6.4.1 The terms of the contract with the service provider and the approval of appropriate devices will ensure that the personal data obtained from individuals is accurate. In instances where accuracy of the data is contested the Service Provider will attend to ensure that the equipment is working correctly and that there are no technical issues.

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

6.5.1 It is clear that data which shows a breach should be kept for longer as it has evidential purposes. Personal data showing the offender's compliance with the relevant requirements placed on them should be kept until the end of the sentence/period of assessing compliance. Personal data showing the offender's non-compliance with the relevant requirements placed on them should be retained until any criminal proceedings which may arise from the data are complete.

6.5.2 Data is held, retained & disposed of in line with the requirements of the EM contract.

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.

6.6.1 There will be no change to the systems in place to allow response to subject access requests. Any requests for access to data will be considered under the Data Protection Act, the Law Enforcement Directive as well as the Data Protection Bill which is currently proceeding through the UK Parliament.

6.6.2 The legislation does not introduce or involve marketing.

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

6.7.1 The legislation does not introduce new systems to provide protection: this will be set as part of the electronic monitoring contract between Scottish Ministers, as the Data Controller, and the Service Provider. A Privacy Impact Assessment will be produced as part of any new contract.

6.7.2 The contract supplier is responsible for the training of all staff regarding handling data.

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

6.8.1 It is not expected that the new legislation will require us to transfer data outside of the EEA.

6.8.2 If such a transfer is required the provisions of the Data Protection Act, the Law Enforcement Directive and, ultimately, the Data Protection Bill will apply.

7. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result	Residual Risk Rating
Breach of Article 8 – Human Rights – Is the data that we collect proportionate? Are we clear on the purpose of collecting this data?		Electronic monitoring constitutes an interference with Article 8 rights which must be justified in terms of legal certainty, purpose and proportionality. The Bill creates a robust statutory basis for electronic monitoring and provides a statutory statement of the purpose of electronic monitoring. The rules on the imposition of electronic monitoring ensure that courts and Ministers can impose electronic monitoring in circumstances which strike the necessary balance between the rights of the offenders and the need to monitor compliance and ensure public safety.	Reduced	
Data Protection Act – The data collected may be considered excessive.		We only collect and retain the information that we absolutely need. We have subordinate-legislation making powers to make provision restricting the collection of data to ensure, for example, that the intrusive data collected by GPS monitoring is only used in appropriate circumstances.	Reduced	

Data Security Access levels to data not set to ensure that only those with permissions are allowed access to data		Structured contractual arrangements to ensure safeguards of data collected – Systems/training/security arrangements	Reduced	

8. Incorporating Privacy Risks into planning

Explain how the risks and solutions or mitigation actions will be incorporated into the project/business plan, and how they will be monitored. There must be a named official responsible for addressing and monitoring each risk.

Risk	Ref	How risk will be incorporated into planning	Owner
Breach of Article 8 – Human Rights		Build into the legislative planner	Jamie Begbie
Data Protection Act		1) Build into the legislative planner 2) Build into the contractual agreement	Jamie Begbie Stuart Morrison
Loss of Data		Build into the contractual agreement	Stuart Morrison

9. Authorisation and publication

The PIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the PIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the PIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "Privacy Impact Assessment (PIA) report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a PIA has been conducted.

I confirm that the impact of (undertaking the project/applying the policy – add appropriate wording) has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a Deputy Director	**Date each version authorised**
Linda Pollock , Deputy Director, Community Justice	8 February 2018

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78851-636-5 (web only)

Published by The Scottish Government, February 2018

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS370766 (02/18)