Electronic Monitoring - MOPAC GPS Pilot

Data Protection Impact Assessment

Ministry of JUSTICE

MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

May 2018

Document information

Master location	:	MOPAC/ MOJ SERVER
File name	:	PIA – MOPAC PILOT GPS
Distribution	:	
Author(s)	:	MOJ/ MOPAC

Version control

Version no.	Version date	Summary of change	Author
V1.1	November 2016	First draft	Toby Head
V2	January 2017	Second draft	Toby Head/ Ruth Bloomfield
V3.1	April 2018	First draft	Ruth Bloomfield/ Harry Sanders
V4	May 2018	Final draft	Ruth Bloomfield
V5	October 2018	Revision in light of new knife crime cohort	Tom Dodsworth
V6	May 2020	Review in light of extension of knife crime pilot	Laura Norton and Tom Dodsworth
V7	May 2021	Review in light of extension of knife crime pilot and inclusion of domestic abuse pilot	Laura Norton and Tom Dodsworth

1. INTRODUCTION

On 8th February 2016, the Prime Minister announced the intention to launch GPS tagging pilots. The Mayor's Office of Policing and Crime (MOPAC) launched the London GPS pilot in March 2017 that included the electronic monitoring of a small number (75) of prolific and priority adult offenders on community orders, suspended sentence orders and Court imposed bail. The pilot was then extended to March 2019 to increase the robustness of the evaluation.

From 15th October 2018 the same pilot has also started to include those convicted of knife crime offences and sentenced in the East London area to a community disposal.

The original pilot concluded in March 2019. A new GPS pilot was launched in February 2019 and was expanded to include high risk domestic abuse perpetrators in March 2021, this is covered by 'Annex C – GPS Tagging on licence pilots'. The MOPAC GPS on licence pilots will conclude in March 2022 with some tag wearers monitored until September 2022.

The pilot is testing a range of factors including:

- how a GPS tag might impact on the behaviour of offenders sentenced by the Courts;
- how Courts respond when given the option of a GPS tag; and
- what other benefits GPS tagging might bring.

This document is the Data Protection Impact Assessment (DPIA) conducted on the MOPAC GPS monitoring pilot.

A DPIA was deemed necessary because the project involves:

- The processing of special category data or criminal offence data
- The use of new technologies
- The processing of personal data in a way which involves tracking individuals' online or offline location or behaviour

Findings

This DPIA concludes that a significant amount of personal and sensitive personal data will be processed and shared with stakeholders. However, safeguards - detailed in Section 2 - are in place to ensure compliance with Data Protection principles. Section 5, Risk Assessment outlines the identified data protection risks associated with the project and the proposed mitigation.

The data gathered for this programme will only be processed for the purpose for which it is obtained or for reasons that are not incompatible - this includes the evaluation of the pilot undertaken by MOPAC's Evidence and Insight Team.

Recommendation

Safeguards are in place as set out in Section 2: Data Processing, of this document. No further recommendations are proposed apart from the continued monitoring for changes to risk and the 6-monthly review of the DPIA.

Review Process

This document has been and will be reviewed at the following stages in the project:

Prior to the pilot commencement date	13th March 2017
Post commencement date	September 2017
At the end of pilot year 1	12th March 2018
Midway point of year 2 delivery/start of knife crime delivery	October 2018
Start of the second year of the knife crime pilot	May 2020
End of the second year of the knife crime pilot	May 2021

The pilot concluded in March 2019. A new GPS pilot was launched in February 2019 and was expanded to include domestic abuse perpetrators from March 2021, this is covered by 'Annex C – GPS Tagging on licence pilots'. The MOAPC GPS on licence pilots will conclude in March 2022 with some tag wearers monitored until September 2022.

2. DATA PROCESSING

2.1. THE NATURE OF THE PROCESSING

2.1.1. Collection of data

The data will be collected via a number of stakeholders involved in the delivery of the project. These include but are not limited to, Buddi Ltd, National Probation Service, Ministry of Justice, London Community Rehabilitation Company, Metropolitan Police Service and Her Majesty's Courts and Tribunal Service. The vast majority of the data will be collected as the individual progresses through the criminal justice system, from point of arrest, charge, court appearance, sentencing and management by London probation service (see Annex A).

Personal data will be stored on portable devices, namely laptops, specifically probation staff laptops.

2.1.2. Use of data

The data is required to enable the stakeholders to monitor effectively individuals subject to electronic monitoring. This involves monitoring compliance with Court Orders in the interest of upholding and administering the law and maintaining the wellbeing of society.

For the purposes of the pilot the data that will be gathered and processed will be that which is required to:

- identify and tag suspects and offenders who fall within scope for the pilot and who have been made the subject of an electronic monitoring requirement by way of a Court Order;

- whereabouts data to support the management and enforcement of Community Orders or Suspended Sentence Orders;
- monitor compliance with and enforce the requirements of such orders;
- minimise the risk to staff involved in the tagging process e.g. any threatening or violent behaviour by the subject or others at the premises;
- where justified and only in accordance with legislative provisions, the data captured may be shared with Criminal Justice Agencies and other Government Departments to assist with criminal enquiries or to seek advice/representation. The circumstances in which such data will be shared are set out in the body of this document;
- assist in the evaluation of the pilot and to inform future policy formation and implementation.

Some data is requested so that stakeholders can meet its obligations under equalities legislation.

Some extraneous location data will be captured by the system. This will not be accessed by the Monitoring team or shared with stakeholders unless there is a lawful reason to do so.

The data will be used for the management of subjects on relevant Electronic Monitoring orders, in accordance with the purposes outlined in section 16 above. The data will be used for audit purposes.

Aggregated, anonymised data will be used for statistical analysis to understand usage and trends etc. In certain cases, subject to justification, location and other data may be shared with Criminal Justice Agencies such as the Police to detect or prevent crime.

MOPAC will use personal data identifying individuals subject to EM orders in order to conduct a full evaluation. The MOPAC evaluation intends to map GPS requirements along with other enhancements under its GtO pilot. In order to complete this MOPAC will use names or other identifiers to match requirements. Data will be anonymised prior to publication of the evaluation.

2.1.3. Data storage

As part of the technical specification, the EM provider (Buddi) must adhere to BS10008 and ISO27001. MOPAC have been provided with evidence of ISO27001 certification from Buddi.

The system in use conforms to data security as defined by ISO27001 and BS10008. The data is held in a secure data hosting centre, accredited to ISO27001.

Communication from the tags to the software system is encrypted, utilising encryption key management solution that ensures data integrity from the point of generation on the device to the point of consumption in the data centre.

The monitoring team will adhere to the appropriate data security requirements from the Cabinet Office and from CESG.

All stakeholders must hold the data securely in accordance with relevant policies or detailed technical specifications within relevant contracts that must accord with the Data Protection Act.

Data in transit and in the data storage system is fully encrypted. The system provides a full audit trail around the access of data.

Staff that will access the data will have been vetted to the relevant levels required by their employer (the Metropolitan Police Service, National Probation Service or London Community Rehabilitation Company).

Buddi staff are also security cleared to various levels and Buddi are responsible for maintaining records of security clearances and renewals. If access to data is no longer required by an employee, then Buddi withdraw that access.

2.1.4. Data retention

All parties carrying out the functions set out in this DPIA 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 DPA compliant.

Once the pilot and the evaluation process has concluded the monitoring contractor and MOPAC will securely transfer all the data to the MoJ and ensure that all data is deleted in a way that prevents reconstitution of the personal data. This will include extraneous location data as the case management system cannot separate this from the other location data captured. Even if there were a way to remove the extraneous location data, doing so may compromise the integrity of other data held on the system.

All data transferred shall be retained securely by the MoJ for a period of at least six years post the end of an individual's order. Thereafter, subject to the data no longer being required, the MoJ will ensure that it is deleted, or, if that is not possible, placed beyond use. In certain circumstances the MoJ retains the right to hold the data for longer than 6 years post order. MOPAC will delete all project data after the secure transfer to the MoJ.

2.1.5. Data sharing

The following groups have access to some or all of the project's data:

- **The MoJ**, as Data Controller, will be given access to all records and reports as may be necessary;
- **MOPAC** as joint Data Controller will be given access to records and reports as may be necessary. MOPAC will not routinely access the electronic monitoring data on the whereabouts of individuals. However, as the contracting authority for the pilot will access records and reports to manage this contract and to enable the evaluation of the pilot.
- **NPS** will be given electronic monitoring data gathered on orders where they act as the Responsible Officer for that subject on that particular order (including those that are in the process of being allocated by NPS to a CRC), or if they are required to take enforcement action against a subject.
- **HMCTS** will be able to submit electronic monitoring notifications to the provider and may be given management information reports;
- **London CRC** will be given data gathered on orders where they act as the Responsible Officer for that subject on that particular order. This excludes

single requirement electronic monitoring orders as CRCs are not the Responsible Officers for those subjects.

- For subjects in BASS premises, the **BASS contractor** will be notified when Responsible Officers are informed of electronic monitoring breaches, if the subject consents to the data share. Their consent will be sought as part of their induction into the BASS premises.
- **The Police** will have routine access to the following data for the specified reasons;
    i) Data on Court ordered bail subjects, as they act as the Responsible Officers in such cases.
    ii) Data necessary to assist with managing compliance of other subjects such as on a suspended sentence order;
    iii) Any data necessary to assist in the apprehension of subjects who have breached their Court Order and are required to be returned to Court.

With regard to the internal departments listed above, information will be routinely shared as set out above in 2.1.5. for the purpose of evaluation, monitoring compliance and enforcing relevant orders.

Should stakeholders require access to data for other reasons or other data, including access to extraneous location data, they will need to submit an External Agency Request (EAR) to Buddi via secure email. In contentious cases, requests will be escalated to the MOJ for a final decision. The request must explain why access to the information is required and failure to provide sufficient justification will lead to it being rejected. Information will only be released in accordance with the provisions of the Data Protection Act unless otherwise directed by a Court. This will be the minimum amount of data necessary to comply with a valid EAR and where possible, it will be binary data (e.g. was X at y – yes/no).

MOPAC in conjunction with the MOJ has provided Buddi with guidance on EARs.

2.2. THE SCOPE OF THE PROCESSING

2.2.1. Whose data

All data processed will be that of offenders sentenced to a GPS electronic monitoring requirement as part of a community order, suspended sentence order or court-imposed bail. To be eligible for a GPS tag as a persistent offender the offender must:

i) Reside in one of the eight pilot boroughs (Hackney, Newham, Waltham Forest, Islington, Camden, Enfield, Haringey, Tower Hamlets)
ii) Have a current sentence
iii) Have an OGRS score of 75+ OR have an OGRS score of 50+ and committed a robbery or burglary offence in the last 12-months that they were in the community
iv) Be aged 18 or over
v) Pass the court threshold for custody

To be eligible for a GPS tag as part of the knife crime cohort (introduced from 15/10/18) the offender must:

i) Reside in one of the eight pilot boroughs (Hackney, Newham, Waltham Forest, Islington, Camden, Enfield, Haringey, Tower Hamlets)
ii) Have a current sentence
iii) Be sentenced for a knife crime offence (defined as either a knife possession offence or another offence which involved the use of a knife or other bladed object)
iv) Be aged 18 or over

Pass the court threshold for custody

2.2.2. Volume of those affected

Between March 2017 and March 2019, it is estimated that only a small number (approximately 200) persistent and knife crime offenders on community orders, suspended sentence orders and Court imposed bail will be monitored as part of this programme. An estimated 50 individuals will be monitored at any given time.

2.2.3. Type of data

Annex B sets out the data to be captured as part of the pilot. The data includes some that is required so that stakeholders can meet their obligations under the Equalities Act e.g. ethnic origin, sexual orientation. The data will also include some extraneous location data that is captured by the system (see **Annex B** for more detail) and photographic identification to ensure that the right person is being tagged.

Personal details, including demographic information about each individual are obtained from verified probation records.

2.2.4. The Use of Data

Data relating to individuals' movements will be collected through location monitoring on a constant basis. The location data will be used by probation providers to manage the subject's court order.

In the course of the management of the case, various information will be shared on an ad hoc basis to partners involved in the delivery of the pilot (see 2.1.5.). This is to ensure a case is managed effectively. The main personal data that will be held and passed between organisations will be: subjects' names, dates of birth, home addresses and, where applicable/available, offence, sentence details, gender, disability, ethnicity, telephone numbers, national insurance numbers, CRB/PNC/Court ref, security and welfare/safeguarding risks. Photographs of the subject may also be used to allow field officers to identify the individual.

Personal and sensitive personal data will be shared with stakeholders for the purposes of meeting the requirements of the Court Orders. Data will only be processed for the purposes for which it was obtained and for other purposes which are not incompatible.

Access to the data will be restricted on a need to know basis (i.e. to those requiring the data in order to achieve the intended objectives).

2.3. THE CONTEXT OF THE PROCESSING

2.3.1. Relationship with subjects

All data collected and processed as part of the project will be of those who have committed a criminal offence and have a current Community or Suspended Sentence Order. See section 4 for the lawful basis to collect the data.

All electronic monitoring subjects will, on induction, receive a Privacy Notice, which will explain how the data will be used. It will include the fact that some extraneous location data will be captured and retained, but not processed further unless there is a lawful reason to do so.

Individuals will not have an opportunity or right to decline to provide data. Initial mandatory information is required for monitoring the subject. As part of the Court Order personal information on the subject must be provided to be able to tag and monitor the subject through the EM service.

Any non-mandatory information, such as information on religious belief will be optional (this information is intended to assist the Authority monitor equality issues).

2.3.2. Rights to request access

We will be processing the data for the original purposes for which it was collected, or a purpose that is not incompatible with that aim. Individuals do not have the right to consent to the use of the data. However, they have the right to request certain aspects of the data held on them. All personal data for an individual can be searched for using the probation case reference number (CRN). Once collated, individual subject information is not published, only aggregated group data. Some data with personal details is passed to agencies who manage the subjects or, where justified, to assist with the prevention and detection of crime.

Subject Access Requests. Subjects can gain access to their own data by asking for a copy of their records by writing to MOPAC, City Hall, Queen's Walk, London SE1 2AA or email enquiries@mopac.london.gov.uk. In practice MOPAC will pass requests to Buddi for processing, however these will be subject to checks from MOPAC prior to a formal response to the subject. Exemptions may apply; all decisions will be logged.

If the individual is not content with any aspect of their data or monitoring of their EM order, they have the right to raise a complaint with the monitoring team by writing to Buddi Ltd, 17 Church St, Rickmansworth WD3 1DE. Buddi is required to forward copies of all complaints to MOPAC along with responses.

2.3.3. Correcting erroneous data

If a subject advises that some of the data about them is incorrect, the monitoring team will contact the organisation responsible for issuing the original order and

confirm what information they hold. Individuals will be informed of this process on induction.

The monitoring team cannot change the information at the subject's request unless it is found to be an input error. Any dispute regarding the accuracy of the data will be noted on the monitoring team's system. Therefore, should the subject continue to refute the validity of the information this will be recorded.

Stakeholders are also under an obligation to ensure the integrity and accuracy of the data provided to the contractor. Should stakeholders become aware of erroneous data they should alert the monitoring team.

2.3.4. Technology and its security

Data transferred from GPS tags to the monitoring centre will be via mobile networks and will be encrypted. All data shared with stakeholders will be via secure email.

All communications with stakeholders must accord to the Government Security Classification tier for the data being shared which will usually be 'Official' including some that may be marked Official Sensitive. 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 handling data in a manner appropriate for the assigned security classification.

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.

MOPAC Data Protection Officer (DPO) or a MOPAC director must be informed of all information breaches asap and within 24 hours of the occurrence. The DPO will complete an assessment of the risk to determine the next steps. If a breach is considered 'notifiable', the Senior Information Risk Owner (SIRO) must be informed asap, and will notify the Information Commissioner's Office (ICO). The ICO must be notified within 72 hours of us becoming aware of the breach.

2.4. THE PURPOSE OF THE PROCESSING

2.4.1. Why the data is required

Primarily, all data set out in Annex B is to support the case management of individuals subject to a GPS requirement under a Community or Suspended Sentence Order.

Alongside supporting the case management, the pilot intends to test a range of factors including:

- how a GPS tag might impact on the behaviour of offenders sentenced by the Courts;
- how Courts respond when given the option of a GPS tag; and

- what other benefits GPS tagging might bring.

2.4.2. The intended effect on the individual

The data collected, particularly location information, is used in the management of the court order. The data should be used to ensure that the subject's risk of serious harm to the public or themselves is reduced. Location monitoring can also be used to inform probation practitioners in activity relating to reducing the likelihood of reoffending and more widely as the practitioner supports the subject improve their life.

Crime mapping will also take place. This is where location data from the GPS tag is matched against MPS crime records. Crime mapping will only affect those individuals on a Suspended Sentence Order. This is because, as part of a Suspended Sentence Order, the individual would be in breach of their order were they to reoffend. Additionally, crime mapping will only be applied to offenders who are assessed to pose a risk of reoffending of 50% or more over two years, meaning that according to this assessment individuals with their characteristics are more likely than not to reoffend during this period. This assessment is made using the Ministry of Justice approved Offender Group Reconviction Scale (OGRS) and is a recognised and validated evidence-based assessment commonly used through the criminal justice system.

2.4.3. Broader benefits of processing the data

2.4.1. outlines the aims of the pilot. If the pilot was to succeed it would show that GPS location data has the ability to reduce risk of reoffending and identify individuals that may have committed a crime. Both of these outcomes would potentially decrease the level of victims.

3. CONSULTATION AND STAKEHOLDER AND ENGAGEMENT

Due to the sensitive nature of the project only a select few stakeholders have been consulted with regarding this DPIA. They include:

1. MOPAC – MOPAC's Delivery Team and Data Protection Lead
2. MoJ – Electronic Monitoring Team
3. Buddi Ltd – Technology provider who supply and monitor the tags and have built the IT system used under this project

The provider to the technology is Buddi Ltd. MOPAC and the MoJ have engaged with Buddi since its successful tender. Buddi provided evidence of GDPR compliance prior to 25th May 2018.

MOPAC will continue to engage with the Information Commissioner's Office to ensure the project is compliant with current data protection acts.

Identification of eligible cases relies on discretion of probation practitioners meaning that it is not possible to consult individuals prior to referral to the pilot. Each individual impacted is provided with a data notice prior to being fitted with a GPS tag. At the time of

the fitting appointment, questionnaires are carried out which allow individuals to raise any concerns they have regarding the impact of the GPS tag. The survey results are used to inform the evaluation and ongoing development of the pilot.

4. COMPLIANCE AND PROPORTIONALITY MEASURES

4.1. LAWFUL BASIS

Under GDPR article 6(3) public task: "the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law" MOPAC has the lawful basis to deliver GPS tagging as part of the Persistent Offender Programme (POP).

The legal framework for electronic monitoring imposed on such orders is set out in the Offender Management Act 2007, the Bail Act 1976, the Criminal Justice Act 2003 and the Crime and Courts Act 2013.

The processing of the data referred to in Annex A is necessary for several of the conditions set out in paragraphs 5 and 6 of Schedule 2 and paragraph 7 of Schedule 3 of the DPA. Specifically:

Schedule 2 - paragraph 5(a) the administration of justice; paragraph 5(c) for the exercise of any function of the Crown, a Minister of the Crown or a government department; paragraph 5(d) for the exercise of any other functions of a public nature exercised in the public interest by any person; paragraph 6 where the processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason or prejudice to the rights and freedoms of legitimate interests of the data subject.

Schedule 3 – paragraph 7(1)(a) administration of justice; paragraph 7(1)(b) the exercise of any functions conferred on any person by or under an enactment, or paragraph 7(1)(c) for the exercise of any function of the Crown, a Minister of the Crown or a government department.

In addition, information may be shared with relevant Criminal Justice and Civil Law bodies in accordance with section 35 of the DPA and paragraph 6(a) of Schedule 3 (i.e. for the purpose of, or in connection with, any legal proceedings including prospective legal proceedings). Whether section 35 applies will be considered on a case by case basis.

Furthermore, section 29 of the DPA, provides an exemption from a sub set of the DPA requirements in processing of personal data, if it is for prevention or detection of crime purposes. This is not a blanket exemption and so whether this exemption applies or not, will be considered on a case by case basis. In any event, a Schedule 2 condition and for sensitive personal data, a Schedule 3 condition, will still need to be satisfied.

In addition, information may need to be shared with relevant Criminal Justice and Civil law bodies in accordance with paragraph 6(a) of Schedule 3 i.e. for the purpose of, or in connection with, any legal proceedings including prospective legal proceedings.

It is also recognised that the processing of personal and personal sensitive information engages Article 8 of the European Convention of Human Rights i.e. the right to respect

for private and family life. The Ministry of Justice considers that it is both lawful and proportionate to process the data referred to in Annex B, location data and photographic identification, in order to comply with relevant electronic monitoring orders and, where justified, to assist the Police with criminal enquiries.

We are satisfied that the data collected will be only that which is necessary to meet the requirements set out above. Data will only be processed for the purposes for which it was obtained and for other purposes which are not incompatible, such as (and only where justified) the prevention or detection of crime.

4.2. DATA PROTECTION BILL 2018

The GPS programme falls under Part 3 of the Data Protection Bill 2018. Part 3 relates to:

- a person (organisation) specified in Schedule 7 – which lists government departments, chief constables (including the Met Commissioner), various other bodies which would not include MOPAC, and "A person who is, under or by virtue of any enactment, responsible for securing the electronic monitoring of any individual", or
- "any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes". The "law enforcement purposes" are then defined as "the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

Paragraph 6 of Schedule 1 (1) of the Data Protection Bill (when brought into force) is relevant to the programme.

This condition of Paragraph 6 of Schedule 1 (1) is met if the processing - (a) is necessary for a purpose listed in sub-paragraph (2), and (b) is necessary for reasons of substantial public interest. (2) Those purposes are - (a) the exercise of a function conferred on a person by an enactment or rule of law…) and paragraph 1 of Schedule 8 (This condition is met if the processing— (a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) is necessary for reasons of substantial public interest).

4.3. ROLES AND RESPONSIBILITIES

4.3.1. The Monitoring Body

For the purpose of this pilot, the monitoring body (i.e. the person responsible for the monitoring) will be Buddi Ltd (Company Number 05308826). This contractor will have access to all the data captured and will process any data in line with data protection obligations. They will ensure that such information is not shared unless justified in accordance with the law, the provisions of this document and the contract between the contractor and MOPAC.

4.3.2. Data Controller and Data Processing Roles

The Data Protection Act (DPA) draws a distinction between a 'Data Controller' and a 'Data Processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. It is the Data

Controller that must exercise control over the processing and carry data protection responsibility for it.

A **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be processed.

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:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available; or
- alignment, combination, blocking, erasure or destruction of the information or data.

In accordance with the provisions of the DPA, the Data Controllers of electronic monitoring information for the purposes of this Pilot will be as follows:

- The MoJ is the Data Controller for offender information provided to MOPAC and its contractors for the purposes of this pilot. It determines the purposes for which the data is to be processed for electronic monitoring of subjects on Court bail, offenders on community orders and suspended sentence orders. The MoJ is the parent Department of HMCTS and NOMS (which includes NPS). Briefly, the role of each of those bodies is set out below:

  HMCTS

  HMCTS will be responsible for issuing notifications of electronic monitoring requirements on Court Orders.

  NOMS HQ

  The Electronic Monitoring Team in NOMS HQ has a vested interest in the outcomes of this pilot and others to help inform the future development and formation of policy decisions.

  NPS

  Save for single requirement electronic monitoring orders (see paragraph 20), NPS is responsible for supervising high risk of serious harm offenders who have an electronic monitoring requirement attached to their community order /suspended sentence order. Should a subject breach the electronic monitoring requirement, NPS will consider:

i) issuing a warning letter if the breach is considered unacceptable
ii) taking breach action by referring the case back to Court for it to, amongst other options, consider amending or cancelling the requirements of a community order /suspended sentence order. NPS also do this on cases referred to it by CRCs (see below).

NPS also has a duty imposed by section 4 of the Offender Management Act 2007 which relates to the giving of assistance to any court in determining the appropriate sentence to pass, or making any other decision, in respect of a person charged with or convicted of an offence.

- MOPAC is a Joint Data Controller with the MoJ as it determines the manner in which the data will be processed as party to the contract with the monitoring service provider and for the evaluation. MOPAC are the contracting authority for the pilot and responsible for, and has control over, the activities and performance of contractor.

- All Police Forces have a remit to manage subjects on Court Bail and are responsible for the apprehension of subjects who have breached their orders and are required to be returned to the Court. In some cases, the Police also assist in managing compliance with relevant orders and will have access to some data on those subjects for that purpose e.g. pilot subjects on suspended sentence orders. In specific circumstances, the Police may also request to use and interpret electronic monitoring data for reasons other than monitoring compliance, including for the purposes of prevention and detection of crime. The process by which the Police may request data for the purposes of prevention and detection of crime unrelated to managing compliance with an order, is set out in paragraphs 37-38 below. Once data has been passed to the Police Forces, they will become Data Controllers of it.

- CRCs are Data Controllers in accordance with the contracts that are in place between the MoJ and the CRCs. Save for single requirement electronic monitoring orders, CRCs are responsible for supervising medium and low risk of serious harm offenders who have an electronic monitoring requirement attached to their community order /suspended sentence order. Should a subject breach the electronic monitoring requirement (see paragraph 20 for caveat) CRCs will consider:
  i) issuing a warning letter if the breach is considered unacceptable;
  ii) taking breach action by referring the case to the NPS Enforcement Officer to consider and where appropriate, cause an information to be laid before a justice of the peace in respect of the offender's failure to comply with the requirement;

Each Data Controller has full responsibility to process the shared personal data lawfully, safeguard any personal information or data to which they have access and to ensure, where appropriate, confidentiality.

The Data Processors of electronic monitoring information will be:

- The third-party contractor appointed to provide the tags and monitoring service;

Single Requirement Electronic Monitoring Orders

For cases that form part of the pilot the contracted monitoring service will act as the Responsible Officer for single electronic monitoring requirements imposed as part of a community order or suspended sentence order. The monitoring team will be responsible for issuing warning letters and determining whether breach proceedings are necessary. If the latter scenario occurs the monitoring team will submit a breach report to the Enforcement Officer in the National Probation Service so that a breach application may be lodged at Court.

4.4. LEGISLATION AND POLICIES

Privacy & Electronic Communications Regulations 2003 Technology Does the project involve new or inherently privacy-invasive electronic communications technologies? For the avoidance of any doubt, 'communication' means any information exchanged or conveyed between finite parties by means of a public electronic communications service but does not include information conveyed as part of a programme service, except to the extent that such information can be related to the identifiable subscriber or user receiving the information.'	GPS tags will be used to communicate subject's location back to the monitoring team.
Privacy & Electronic Communications Regulations 2003 Communication providers Does the project involve new or existing communication providers? For the avoidance of doubt, 'communication providers' means a person or organisation that provides an electronic communications network or an electronic communications service.	Existing
[Privacy & Electronic Communications Regulations 2003 Communication subscribers / users Does the project involve new or existing communication subscribers / users? For the avoidance of doubt, 'communication subscriber' means a person who is a party to a contract with a provider of public electronic communication services for the supply of such services. 'User' means an individual using a public electronic communications service.]	No

[Human Rights Act 1998 Article 2: Right to Life Does the project involve new or existing data processing that adversely impacts an individual's right to life, subject to any limitations as may be defined in Article 2(2)? For the avoidance of any doubt, the limited circumstances are that in peacetime, a public authority may not cause death unless the death results from force used as follows: • Self-defence or defence of another person from unlawful violence; • Arresting of someone or the prevention of escape from lawful detention; and • A lawful act to quell a riot or insurrection.	No
[Human Rights Act 1998 Article 3: Prohibition of Torture Does the project involve new or existing data processing that adversely impacts an individual's right to be not subjected to torture or inhuman or degrading treatment? For the avoidance of doubt, this is an absolute right.	No
[Human Rights Act 1998 Article 4: Prohibition of Slavery or Forced Labour Does the project involve new or existing data processing that adversely impacts an individual's right to be not held in servitude or forced to perform compulsory labour? For the avoidance of doubt, this is an absolute right; the following are excluded from being defined as forced or compulsory labour: • Work done in ordinary course of a prison or community sentence; • Military service; • Community service in a public emergency; and Normal civic obligations.	No

[Human Rights Act 1998 Article 5: Right to Liberty and Security Does the project involve new or existing data processing that adversely impacts an individual's right to be not deprived of their liberty subject to certain limitations? For the avoidance of doubt, the following limitations apply when a person is: • Held in lawful detention after conviction by a competent court; • Lawfully arrested or detained for non-compliance with a lawful court order or the fulfilment of any lawful obligation; • Lawfully arrested or detained to affect the appearance of the person before a competent legal authority; • Lawfully detained to prevent the spreading of infectious diseases; • Lawfully detained for personal safety (applies to persons of unsound mind, drug addicts etc.); and • Lawfully detained to prevent unlawful entry into the country or lawful deportation from the country.	No, it does not.
[Human Rights Act 1998 Article 6: Right to a Fair Trial Does the project involve new or existing data processing that adversely impacts an individual's right to have a public hearing within a reasonable time by an independent and impartial tribunal established by law? For the avoidance of doubt, the hearings included are both civil and criminal proceedings that are not specifically classified as hearings that must be heard 'in camera', i.e. closed to the public.	No, it does not.

[Human Rights Act 1998 Article 7: Right to no Punishment without Law Does the project involve new or existing data processing that adversely impacts an individual's right to not be prosecuted for a crime that was not, at the alleged time of commission, constitute a criminal offence under national or international law? For the avoidance of doubt, this is an absolute right.	No, it does not.

[Human Rights Act 1998 Article 8: Right to Respect for Private and Family Life Does the project involve new or existing data processing that adversely impacts an individual's right to respect for privacy in terms of their private and family life subject to certain qualifications? For the avoidance of doubt, the qualifications are: • Legal compliance; • National security; • Public safety; • National economy; • Prevention of crime and disorder; • Protection of public health and morals; • Protection of rights and freedom of others.]	*The GPS Pilot engages article 8, that is to say, it will involve a prima facie interference with the right under article 8(1). The pilot involves the collection, use and storage of information about the day to day movements of around 100 people for the purpose of monitoring their compliance with a court order and, in certain cases, investigating crimes. The interference can, however, be justified under article 8(2). The ultimate purpose for which the information is being processed is the prevention and detection of crime. Article 8(2) states that the prevention of disorder or crime is one of the permissible bases for interference with the right in article 8(1). Public safety and the protection of the rights and freedoms of others may also be relevant.* *For the interference to be justified, it will need to be "in accordance with the law" and "necessary in a democratic society" within the meaning of article 8(2). The pilot is being conducted within the parameters of a legal framework which includes the Crime and Justice Act 2003 and orders made pursuant to it, the Code of Practice specifically relating to the pilot that the Secretary of State is required to issue pursuant to s 215A of that Act, as well as the DPA. In order for the interference to be "necessary in a democratic society" it will have to meet a pressing social need and be proportionate to that need. In general terms, there is a pressing social need to reduce crime in London and within the UK generally. The processing of data from electronic tags is likely to assist with meeting that need because the information will be used to monitor compliance with court orders and in certain cases, in the investigation of crime. Although some location data will be extraneous to the purpose of monitoring the terms of the court order, measures are to be put in place to ensure that such data is only accessed if there is a lawful reason to do so. In such cases, a specific request will need to be made to access the data (an External Agency Request) and it must set out why the information is required. Such information will only be released if it is in accordance with the provisions of the DPA (for example, sections 29 and 35) and only the minimum amount of data necessary to comply with the request will be disclosed including only binary data, for example, 'yes/no'. This*

	suggests that any interference will be proportionate.
[Human Rights Act 1998 Article 9: Right to Freedom of Thought, Conscience & Religion Does the project involve new or existing data processing that adversely impacts an individual's right to freedom of thought, conscience and religion subject to certain qualifications? For the avoidance of doubt, the qualifications are: • Unless prescribed by law; • In interest of public safety; • Protection of public order, rights or morals; • Protection of rights and freedoms of others.	No, it does not.
[Human Rights Act 1998 Article 10: Right to Free Expression Does the project involve new or existing data processing that adversely impacts an individual's right to hold opinions and express their views singly or in dialogue subject to certain qualifications? For the avoidance of doubt, the qualifications are as set out in Article 9 above.	No, it does not.
[Human Rights Act 1998 Article 11: Right to Freedom of Assembly & Association Does the project involve new or existing data processing that adversely impacts an individual's right to freedom of peaceful assembly and association with others subject to certain qualifications? For the avoidance of doubt, the qualifications are as set out in Article 9 above.	No, it does not.

Human Rights Act 1998 Article 12: Right to Marry Does the project involve new or existing data processing that adversely impacts an individual's right to marry and found a family subject to certain restrictions? For the avoidance of doubt, the restrictions are regulated by law so long as they do not effectively take away the right, e.g. age restrictions apply.	No, it does not.
Human Rights Act 1998 Article 14: Right to Freedom from Discrimination Does the project involve new or existing data processing that adversely impacts an individual's right to be treated in a manner that does not discriminate the individual from others subject to certain restrictions? For the avoidance of doubt, this right is restricted to the conventions as set out in the European Convention of Human Rights 1950; the grounds for discrimination can be based on: • Sex • Race • Colour • Language • Religion • Political persuasion • Nationality or social origin • Birth • Other status.	No, it does not.
Regulation of Investigatory Powers Act (RIPA) 2000 Does the project involve new or inherently privacy invasive electronic technologies to intercept communications? For the avoidance of doubt, 'communications' is defined in RIPA Part V, section 81(1).	No

Regulation of Investigatory Powers Act (RIPA) 2000 Does the project involve new or inherently privacy invasive electronic technologies pertaining to the acquisition and disclosure of data relating to communications?	No
Regulation of Investigatory Powers Act (RIPA) 2000 Does the project involve new or inherently privacy invasive electronic technologies pertaining to the carrying out of surveillance?	No. The use of GPS will allow the monitoring of subject's location in a real time or passive state. Subjects will be informed that the tag has this capability. As subjects will be aware of this capability RIPA does not apply.
Regulation of Investigatory Powers Act (RIPA) 2000 Does the project involve new or inherently privacy invasive electronic technologies pertaining to the provision of the means by which electronic data protected by encryption or passwords may be decrypted or accessed?	No
Regulation of Investigatory Powers Act (RIPA) 2000 Does the project undertake any of the functions of the Security Service, the Secret Intelligence Service or the Government Communications Headquarters?	No

4.5. PROPORTIONALITY

4.5.1. Crime Mapping

For Suspended Sentence Orders, the probation management of an offender is the same as with a Community Order.

In addition, as an offender is deemed to be in breach of the SSO if he/she commits a further offence during the operational period, the location data on an offender's whereabouts can be used to routinely match against reported crimes. Data is then used to ensure that the offender is complying with the requirement not to commit further offences.

Persistent offenders are only eligible for GPS under this programme if they are deemed to pose a high likelihood of reconviction within two years (based on an Offender Group Reconviction Score (OGRS) of 75%+ or 50-74% with a burglary or robbery committed in the preceding two years). The proportionality of the Crime Mapping function is underpinned by this eligibility criteria.

For knife crime offenders, crime mapping will only be applied to those on a Suspended Sentence Order who additionally have an OGRS score of 50% or more. This ensures that crime mapping is only used in cases in which it is proportionate to individual's the risk of reoffending.

A single point of contact within the MPS will upload offences onto the monitoring platform; restrictions will be in place to limit the time period and geographical area being matched (for a wider search, an External Agency Request would need to be made.

4.5.2. Exclusion Zones

A Court Order will include a provision for the subject's location to be monitored as a stand-alone requirement or for the purposes of monitoring compliance with another requirement such as an exclusion/inclusion zone. Where such a provision is made, the subject's whereabouts will be monitored using GPS. Inevitably, in order to monitor whether the subject enters or exits an exclusion/inclusion zone, some extraneous data will be captured, specifically the location of the individual at other times. For mitigation please see Section 5, Risk Management.

4.5.3. GPS Order Scenarios – Whereabouts Data Use

Community Orders

24 Hour Monitoring – All data is retained to monitor the order. No crime mapping can take place but EARs could be made under certain circumstances.

Compliance Monitoring (Exclusion Zone) – All data is retained but only exclusion location data is shared with partners unless an acceptable EAR is made.

Suspended Sentence Orders

24 Hour Monitoring – All data is retained to monitor the order. Crime mapping will take place and EARs could be made under certain circumstances.

Compliance Monitoring (Exclusion Zone) – All data is retained but only exclusion location data is shared with partners unless an acceptable EAR is made or for the purposes of crime mapping.

5. RISK ASSESSMENT

Principles	Identified Risk	Potential impact on the monitored individual	Level of Risk (impact)	Mitigation
Data minimisation	GPS technology provider collects a greater level of data than necessary	High	Medium	For those individuals with an exclusion zone, GPS data will also be collected when outside of the zone. There is a legal basis for this data to be used in crime mapping for individuals subject to Suspended Sentence Orders (Individuals must legally not reoffend when subject to a Suspended Sentence Order). Probation Responsible Officers, who can access relevant data for 24-hour whereabouts, do not have direct system access to the Buddi system and hence would have no way to access data for exclusion zone cases. Responsible Officers (ROs) only have access to GPS information for inside exclusion zones and Points of Interest Zones – whereby an offender allows their RO to see their movements in certain areas. The GPS Toolkit, which acts as the operating model for all stakeholders, makes it clear that no Responsible Officer or other external party can request location data, except via the External Agency Request process. For Community Orders, this data will not be shared with any delivery partner, unless an

				External Agency Request (EARs) is made and signed off by the MoJ. A clear record of all EARs is kept by Buddi, who have been provided with clear guidelines on how to deal with these and the escalation process to the MoJ for borderline cases. The log of EAR requests is sent to the MoJ on a regular basis. MoJ have provided guidance to Buddi Ltd outlining when and how to respond to an EAR. In circumstances whereby the request is Justified, Authorised, Proportionate, Auditable, Necessary, then the requested data should be shared. EARs must explain why access to the specific information requested is required and how the data will assist with the aim. If this is, unclear or tenuous, the request must be rejected. The request for data must be limited to the minimum necessary to fulfil the aim. If the request is too broad in scope it must be rejected. The request must explain the nature of any urgency and the time for a response. The request must be dated and signed and the monitoring team must confirm the authenticity of the requestor before any data is released. The MOJ should be consulted if Buddi do not feel that the EAR meets the requirements for information sharing but further requests are received. A log of all EARs is maintained, and subject to quality monitoring by the MOJ. Allocated staff at

				the technology company, Buddi, will have access to this data but will only have reason to view it if an External Agency Request is successful. The subject will be notified on induction of the use of all whereabouts data. Data will be retained for a period no greater than 6 years from the expiry of the requirement of the court order. Where possible, data will be stripped of personal identifiers and saved by MOPAC for evaluation purposes prior to the 6-year period. Data may be held by the Ministry of Justice for the full 6-year period in line with their data retention policy. Where data transfers take place, this will be completed via secure email.
Storage limitation	Partner agencies do not follow MOPAC/ MoJ data retention policies and do not delete data at the end of the project	Medium (individuals are informed of data retention policies)	Low	All parties carrying out the functions set out in this DPIA 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 DPA compliant. Once the pilot and the evaluation process has concluded the monitoring contractor/MOPAC will securely transfer all the data to the MoJ. This will include extraneous location data as the case management system cannot separate this from the other location data captured. Even if there were a way to remove the extraneous location

				data, doing so may compromise the integrity of other data held on the system. All data transferred shall be retained securely by the MoJ for a period of at least six years post pilot evaluation, only being retained if there is a lawful reason to do so. Thereafter, subject to the data no longer being required, the MoJ will ensure that it is deleted, or, if that is not possible, placed beyond use.
Purpose limitation	Use of data for evaluation is unlawful	Medium	Medium	MOPAC's Evidence and Insight Team have been commissioned to undertake the evaluation. MOPAC's Evidence and Insight Team have Metropolitan Police Service accounts and therefore all data is transferred via secure email and is stored on a secure server. All Evidence and Insight employees are Counter Terrorism Clearance security checked. The evaluation of the programme is an extension of the lawful basis as it is required to understand whether the programme works. MOPAC's Evidence and Insight Team will abide by MOPAC's Information Governance Policy.
Storage Limitation	Loss or compromise of data	High	Medium	All stakeholders (HMCTS, NPS, CRC, MPS, MOJ) must follow their local policies on reporting a compromise or loss of data. In addition, where this relates to shared MoJ data, the stakeholder must inform the MoJ as soon as possible, or no later than 24 hours after the compromise / loss is identified. On being notified of the possible incident, the stakeholder organisation 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 MOPAC/HMPPS/Ministry of Justice's operations or reputation; • the necessary actions to be taken to mitigate the risk, both immediately and for the future. MOPAC Data Protection Officer (DPO) or a MOPAC director must be informed of all information breaches asap and within 24 hours of the occurrence. The DPO will complete an assessment of the risk to determine the next steps. If a breach is considered 'notifiable', the Senior Information Risk Owner (SIRO) must be informed asap, and will notify the Information Commissioner's Office (ICO). The ICO must be notified within 72 hours of us becoming aware of the breach.

				If the incident is considered serious or impacting, the lead manager must immediately inform the appropriate HMPPS Senior Official. All contracted providers should report the incident through the contractual line (designated contract manager). An investigation should take place into the circumstances of the loss to ensure that lessons are learned and shared where necessary.
Lawfulness, fairness and transparency	Subject has a lack of understanding around the use of data	Medium	Medium	All electronic monitoring subjects will, on induction by the person fitting the tag, receive a Privacy Notice, which will explain how the data will be used. It will include the fact that some extraneous location data will be captured and retained, but not processed further unless there is a lawful reason to do so.
Accuracy	GPS technology takes inaccurate readings	High	Low	Buddi technology accounts for inaccuracy and reports on it for each reading taken. The reading will include the distance the subject could have been from the coordinate that is reported. The reading also includes the strength of signal. The potential for locations to be reported incorrectly will also be taken into account during crime mapping. The crime mapping analyst will provide local police teams with an assessment of the accuracy level of the GPS signal, compared to the crime co-ordinates submitted by police.

				In certain circumstances location data and it accuracy may be put under extra scrutiny, for example if this relates to a breach of an enforceable exclusion zone. In such cases there is a process in place to prompt confirmation and, if necessary, discussion between the Responsible Officer and the Buddi customer service team, who can double check location information and provide expert advice on accuracy. Buddi also provide extra analysis and Court admissible reports when information is provided to link a wearer to the location of a new offence. Buddi also have experience of expert witness testimony in cases where location data accuracy is part of a Court trial.
Integrity and confidentiality	Agencies without permission view GPS location data	High	High	Data will only be shared when necessary, justified and proportionate to do so. Stakeholders will only routinely have access to information to monitor compliance with and the enforcement of relevant orders. The location data is stored on the secure Buddi Eagle database, which only Buddi staff have full access to. Probation Responsible Officers are provided with log in for this system, through which they can access basic information about their own cases only; this does not include access to any location information or data that they would not already have provided to Buddi. If Responsible Officers want to access any location data, this must be done via a recordable request to Buddi, either to set up a monitoring zone or point of interest of to request a specific piece of data for a specific reason, i.e.

				record of attendance at a drug treatment centre over a month period. No other agencies or professionals have access to location information except through the EAR process. If information is required for reasons other than those specified above, the requestor will need to submit an External Agency Request. These will be scrutinised by the monitoring team and, in some cases, by the MoJ and information will only be released in accordance with the Data Protection Act. All stakeholders must hold the data securely in accordance with relevant policies or detailed technical specifications within relevant contracts, which must align to the Data Protection Act. 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 and security cleared. Stakeholders must make themselves aware of, and adhere to, their organisation's information security policies and procedures in regard to handling data in a manner appropriate for the assigned Government Protective Marking, which will usually be Official or Official Sensitive. MOPAC Data Protection Officer (DPO) or a MOPAC director must be informed of all information breaches asap and within 24 hours of the occurrence. The DPO will complete an assessment of the risk to determine the next steps. If a breach is considered 'notifiable', the

				Senior Information Risk Owner (SIRO) must be informed asap, and will notify the Information Commissioner's Office (ICO). The ICO must be notified within 72 hours of us becoming aware of the breach. If the incident is considered serious, the lead manager must immediately inform the appropriate HMPPS Senior Official. All contracted providers should report the incident through the contractual line (designated contract manager). An investigation should take place into the circumstances of the loss to ensure that lessons are learned and shared where necessary.
Lawfulness, fairness and transparency	Crime mapping is mistakenly carried out for cases who does not meet the criteria	High	High	With the addition of knife crime offenders, the difference between offenders who are and who are not eligible for crime mapping becomes less clear, as this is no longer solely reliant on Order type. The forms completed at the time of sentencing and sent to Buddi have been revised to explicitly record the OGRS score, to make sure this clear. In addition, new process maps in the Buddi control centre and for the tag fitting operatives have been written to ensure this distinction is double checked to avoid confusion. An escalation process in place to check cases where any ambiguity remains, with a clear presumption that cases should not be crime

				mapped until the OGRS score is confirmed to be at least 50%.

6. SIGN OFF

6.1. MOPAC DATA PROTECTION OFFICER

7. Item	Name/date	Notes
Measures approved by:		
Residual risks approved by:		
DPO advice provided:		
Summary of DPO advice:		
DPO advice accepted or overruled by:		
Comments:		
Consultation responses reviewed by:	N/A	
Comments: N/A		
This DPIA will be kept under review by:	Project Manager	

6.2. Final Sign off

For and on behalf of **MOPAC**

Signed:

Position:

Date:

For and on behalf of **MOJ**

Signed:

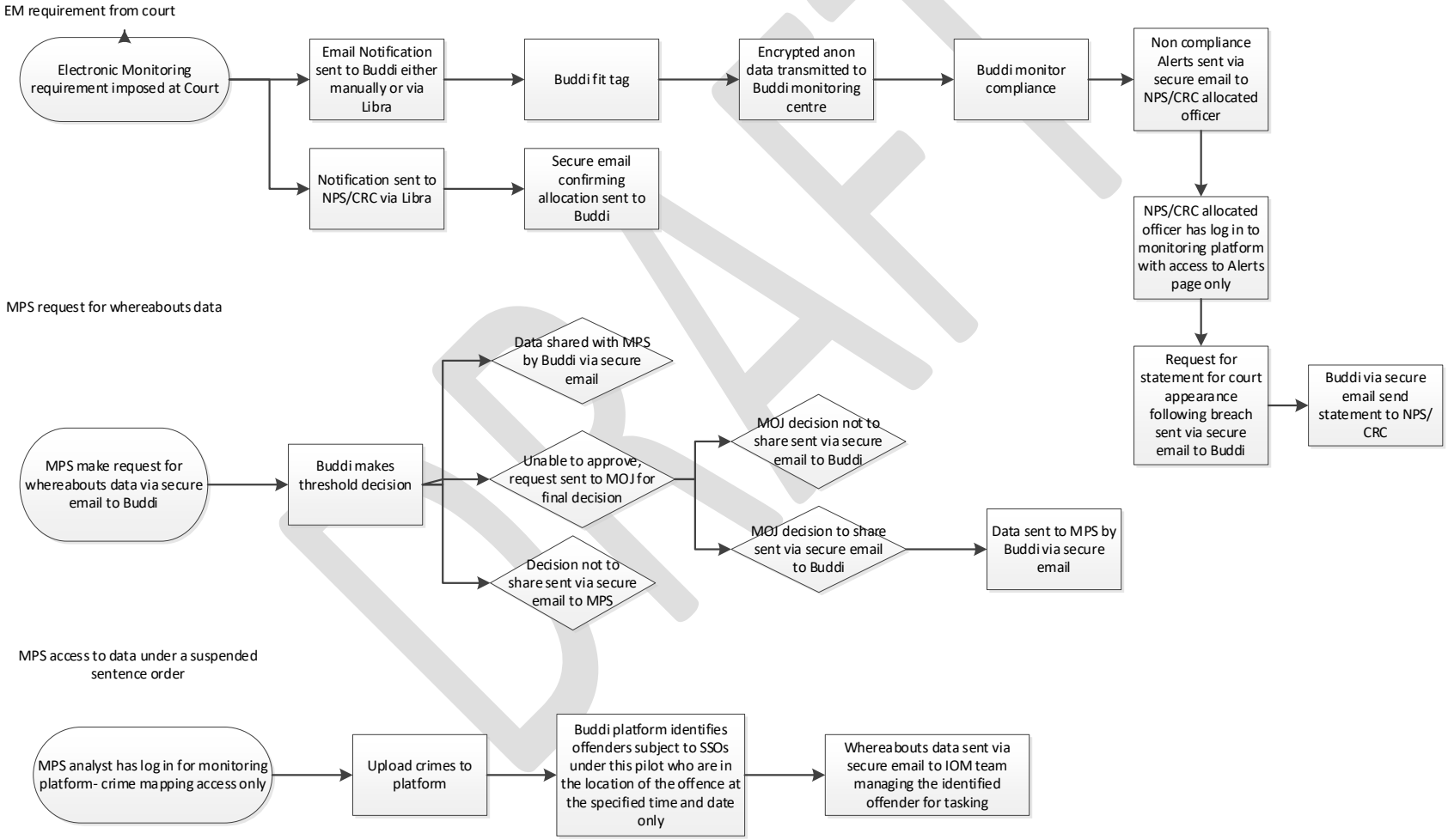
Position:

Date:

7. ANNEXES

Annex A – Data Flow Diagrams

Subject Journey



Annex B – Data Requirements

Offender details
Forename
Middle name(s)
Surname
Subject postcode
Subject address
Subject telephone number (if available)
Subject date of birth
Subject gender
Subject age
Subject ethnic origin
Subject religion
Subject sexual orientation
Subject Marital/partnership status
Subject pregnancy status
Subject disability status
Please note anything that falls under Disability Act pertinent to wearing of a tag (leave clear if nothing)
Nationality
Language spoken
PNC ID
CRN
Number of previous offences
HO offence code for offence / charge leading to EM requirement
Date of Index offence or charge leading to EM requirement
Order details
Responsible officer name
Name of probation provider or court that made the decision to tag
Please note if there is a different court for breach purposes than the above
Start of order date
End of order date
Date of decision to tag (i.e. date of sentence.)
Expected end of monitoring period
Type of requirement
Other requirement(s) of the order
Sentence length in days (if indeterminate or life, tariff length) if not court bail case
Responsible officer email address
Responsible officer phone number
Police contact
CPS contact
Court contact
NPS contact
CRC contact
BASS contact
Victim liaison officer contact
Safeguarding concerns have been noted
Is the subject a MAPPA nominal?
Variations

Date application to vary EM requirements, if any (note: all changes must be added to Change spreadsheet)
Date application made
Decision-maker
Outcome of application
Nature of change (if several, please note in comments)
Comments on change
Dates of authorised absences
Alerts, Violations and breaches
Date of violation, or alert
Type of violation or alert
Is violation in connection with a re-arrest / new offence, type of (alleged) offence
Outcome of violation, or alert
Was the violation, or alert termed a formal breach of EM requirements? (Please follow up with Responsible Officer to clarify)
Breach court hearing date
Outcome of breach
If other enforcement action – date enforcement action carried out
If enforcement action - outcome
If monitoring continues with additional action – what was the action?
Authorised absences
Date of authorised absence
Date application made
Reason given for authorised absence
Decision-maker
Outcome of application
Nature of change (if several, please note in comments)
Comments on change
External agency requests
External Agency Request date
Request received from
Whether the data request is routine (usually a request from the stakeholder who manages the wearer) or non-routine (a request from an authority who does not directly manage the wearer, such as the police
For police requests only -the type of offence that the police are investigating (e.g. burglary, robbery, assault etc.)
Decision made by Monitoring centre?
Monitoring centre staff name dealing with request.
If the request requires MoJ approval, the date that the request was forwarded
Confirmation of whether the request was approved or rejected
A brief outline of the reasoning for the decision (either approvals or rejections)
The name of the person who made the final decision
The outcome for the request should be included here, whether all data, partial data, or no data was released
The date that the requester was informed of the decision
GPS Tag and fitter details
Fitter identification details
Tag identification number

Tag strap identification number
Home beacon identification number
Tag on (i.e. date of installation)
Tag off (i.e. date of deinstallation)
Reason for deinstallation
Failed installations (date)
Failed installation reason
Exclusion address / zone
Inclusion address/ Zone
Points of interest/ Interest zones
Details of EM schedule
Tag broken / lost
Base station broken / lost
Individual entry survey- at installation, deinstallation
Fitter identification details
Tag identification number
Date tag fitted
Subject gender
Subject age
Subject ethnic origin
Subject religion
Subject sexual orientation
Subject Marital/partnership status
Subject pregnancy status
Subject disability status
Consent gained for additional information on subject's views on use and impact of tag
Fair processing and offender leaflet provided
Crime mapping under SSOs and for offenders with an Offender Group Reconviction Scale (OGRS) score of 50%+ on the knife crime on licence pilot
Number of offences searched
Offence type, and date of offence with match
Tag identification if a match
Outcome