Enforcement Notice issued by the Information Commissioner concerning contraventions of Article 5(2) and Article 35 UK GDPR by the Home Office

ENFORCEMENT NOTICE

HOME OFFICE

28 February 2024

DATA PROTECTION ACT 2018
ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE

To: The Secretary of State for the Home Department.

Of: The Home Office, Peel Building, 2 Marsham Street, London, SW1P 4DF.

PART I: INTRODUCTION AND SUMMARY

1. The Home Office is a "controller" as variously defined in sections 3(6), 5 and 6 of the Data Protection Act 2018 ("DPA") and Article 4(7) of the UK General Data Protection Regulation ("UK GDPR").

2. Unless otherwise stated, references to "Articles" are to articles of UK GDPR, and "Sections" to sections of the DPA.

3. The Home Office processes personal data for the purposes of its management of immigration, including individuals entering or leaving the UK, securing the border, leave, settlement, citizenship or other immigration services, claiming asylum or other forms of protection. The Home Office also processes personal data as part of its functions to enforce immigration laws, law enforcement for criminal matters and other lawful matters including those related to public health. The Home Office is the controller for this information, including when the information is collected or processed by third parties on its behalf.

4. The Information Commissioner (the "Commissioner") hereby issues the Home Office with an Enforcement Notice ("EN") under section 149 DPA, in the terms set out in this EN. This EN relates to contraventions by the Home Office of Articles 35 and 5(2) UK GDPR in relation to its processing of personal data for its satellite tracking services GPS expansion pilot (the "pilot").

5. This pilot extended the Home Office's use of electronic tagging as an immigration bail condition to a new cohort: data subjects who arrive in the UK via unnecessary and dangerous routes who have claims suitable for consideration under the detained asylum casework (DAC) process.

The infringements

6. The Commissioner has found that the Home Office has infringed Articles 35 and 5(2) UK GDPR (the "infringements") as follows:

   Article 35: The Home Office failed to carry out a DPIA in relation to the pilot which satisfies the requirements of Article 35.

   In summary, the DPIA (Draft DPIA V2.3) did not set out either at all, or in sufficient detail:

   - A systematic description of the envisaged processing operations and the purposes of the processing. The DPIA did not set out each processing operation, and the stated purposes are inconsistent and unclear.
   - An assessment of the necessity and proportionality of the processing operations in relation to those purposes.

- Continuous monitoring using GPS tracking by an electronic tag is intrusive. The Home Office did not demonstrate that less privacy intrusive methods could not meet its objectives.

- An objective assessment of the risks to the rights and freedoms of data subjects, and the measures envisaged to address those risks. Whilst some risks to the rights and freedoms of data subjects were identified, Draft DPIA V2.3 (including the section 7.2 risk table) failed to sufficiently assess all of the risks, and as a result did not sufficiently propose measures to address those risks.

Article 5(2): The Home Office, in breach of the accountability principle, has failed to demonstrate its compliance with Article 5(1), in particular:

- Article 5(1)(a) principle of lawfulness: the Home Office identified the lawful basis for the processing as Article 6(1)(e), and for special category data as Article 9(2)(g) and schedule 1 paragraph 6 DPA. However, the Home Office did not demonstrate that the processing was necessary and proportionate for these purposes. This was not demonstrated in its DPIA or its guidance for Home Office staff. The Home Office failed to demonstrate why less privacy-intrusive methods could not meet its objectives.

- Article 5(1)(a) principle of fairness and transparency: the Home Office's privacy notice(s) do not demonstrate compliance with minimum transparency requirements, as set out at Articles 12 and 13.

- Article 5(1)(c) principle of data minimisation: the Home Office's Draft DPIA V2.3 and guidance for Home Office staff does not demonstrate that data minimisation will be considered and actioned when requesting access to the personal data produced by the electronic tags (the "trail data").

7. Annex 1 of this EN sets out the actions that the Commissioner requires the Home Office to take to correct the infringements.

8. The findings set out in this EN and the requirements set out in Annex 1 relate to the assessments and documentation the Home Office has shared with the Commissioner which underpin the pilot. The Commissioner expresses no view in this EN as to whether processing of personal data by the Home Office in relation to the pilot is otherwise compliant with data protection legislation more generally.

PART II: LEGAL FRAMEWORK

9. Section 149(1) DPA provides that, if the Commissioner is satisfied that a person has failed, or is failing, as described in section 149(2) DPA, the Commissioner may, by written notice (an "enforcement notice"), require that person to take steps or refrain from taking steps specified in the enforcement notice.

10. The types of failure described in section 149(2) DPA include "where a controller or processor has failed, or is failing, to comply with …":

- at section 149(2)(a) "a provision of Chapter II of the UK GDPR … (principles of processing)"; and

- at section 149(2)(c) "a provision of articles 25 to 39 of the UK GDPR … (obligations of controllers and processors)".

11. Section 150 DPA provides that:

"(1) An enforcement notice must -

(a) "state what the person has failed or is failing to do", and

(b) "give the Commissioner's reasons for reaching that opinion.

12. Chapter II of the UK GDPR sets out the principles which controllers must comply with, and requirements which apply when controllers are processing special categories of data and criminal records data.

13. Article 5(2) UK GDPR sets out the principle of accountability and requires that controllers must "be able to demonstrate compliance with" Article 5(1) UK GDPR.

14. Article 5(1) sets out the other principles relating to processing of personal data which are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

15. Articles 24 to 39 UK GDPR set out general obligations which controllers and processors must comply with when processing personal data.

16. Article 35(1) UK GDPR requires controllers, prior to the processing, to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where those processing operations are likely to result in a high risk to the rights and freedoms of natural persons.

17. Other relevant provisions of the UK GDPR and DPA are set out below in the specific paragraphs dealing with the infringements by the Home Office (Part IV: The Commissioner's findings of infringement).

18. The legal framework for issuing an enforcement notice is set out in Part V: Decision to issue this EN.

Home Office powers

19. The Home Office's powers to grant immigration bail are governed by schedule 10 of the Immigration Act 2016. The Home Office has published guidance on immigration bail[1]. Immigration bail may be granted by the Home Office where a person is detained or is liable to be detained under specified statutory provisions[2].

20. Schedule 10 paragraph 2(1) Immigration Act 2016 requires that if immigration bail is granted to a person, it must be granted subject to one or more of the following conditions –

- a condition requiring the person to appear before the Secretary of State or, the First Tier Tribunal at a specified time and place;
- a condition restricting the person's work, occupation or studies in the United Kingdom;
- a condition about the person's residence;

[1] Immigration Bail Version 16.0 dated 8 August 2023

[2] Namely: (a) paragraph 16(1), (1A) or (2) of Schedule 2 to the Immigration Act 1971 (detention of persons liable to examination or removal); (b) paragraph 2(1), (2) or (3) of Schedule 3 to that Act (detention pending deportation); (c) section 62 of the Nationality, Immigration and Asylum Act 2002 (detention of persons liable to examination or removal); and (d) section 36(1) of the UK Borders Act 2007 (detention pending deportation).

- a condition requiring the person to report to the Secretary of State or such other person that may be specified;
- an electronic monitoring condition; or
- such other conditions as the person granting immigration bail sees fit.

21. Schedule 10 paragraph 4(1) Immigration Act 2016 confirms that electronic monitoring condition "means a condition requiring the person on whom it is imposed ("P") to co-operate with such arrangements as the Secretary of State may specify for detecting and recording by electronic means one or more of the following—

(a) P's location at specified times, during specified periods of time or while the arrangements are in place;

(b) P's presence in a location at specified times, during specified periods of time or while the arrangements are in place;

(c) P's absence from a location at specified times, during specified periods of time or while the arrangements are in place"

PART III: THE BACKGROUND

22. This section sets out the relevant facts of the infringements that are the subject of this EN.

The pilot and its scope

23. On 15 June 2022 the Home Office commenced the pilot to run initially for 12 months, and later extended this period by a further six months. The pilot extended the Home Office's use of electronic monitoring as an immigration bail condition to a new cohort:

individuals who arrive in the UK via unnecessary and dangerous routes who have claims suitable for consideration under the detained asylum casework (DAC) process. The pilot size was set at up to 600 individuals to be subject to electronic monitoring and 600 further individuals to form the control group.

24. The high-level purpose of the pilot is described as:

> "… test whether electronic monitoring (EM) is an effective means by which to improve and maintain regular contact with asylum claimants who arrive in the UK via unnecessary and dangerous routes and more effectively progress their claims towards conclusion."[3]

25. Initially the pilot also covered asylum seekers who arrived in the UK via unnecessary and dangerous routes and were considered inadmissible, but this cohort ceased as a result of a successful legal challenge.

26. Pilot participants were monitored for breach of immigration bail conditions by the Home Office's processor in the same way as the existing process for electronic monitoring as an immigration bail condition.

27. The pilot ended in December 2023, and so did the collection of personal data using electronic monitoring devices for the pilot. However, processing of personal data gathered or created during the course of the pilot will continue until such time as all pilot personal data has been deleted or anonymised. This EN relates to the extent that the Home Office has failed and is failing to deal

[3] Set out in Draft DPIA V2.3 and Pilot Guidance.

with this personal data in accordance with the requirements of the UK GDPR.

The DPIAs and other Home Office documents

28. The Commissioner has reviewed the following DPIAs provided by the Home Office:

Title	Document Date
GPS Expansion (small Boats) final version 0.1	26.01.22
Satellite Tracking Services (STS) GPS expansion version 0.2	30/05/2022 (ODPO review complete)
STS GPS expansion Version 2.0	12.12.22
Satellite Tracking Services (STS) Version 2.2 (draft) with separate risk table 7.2 ("Draft DPIA V2.2")	07.08.23
Satellite Tracking Services (STS) Version 2.3 (draft) with separate risk table 7.2 ("Draft DPIA V2.3")	13.10.23

29. The Home Office published guidance: "Immigration Bail Conditions: Electronic monitoring (EM) expansion pilot" version 1. This was updated and published as version 2 on 23 June 2023 (the "Pilot Guidance"). This document states that it must be read in conjunction with the Immigration Bail Guidance (the "Immigration Bail Guidance"). The most recent version of this document is Version 16.0 published on 8 August 2023.

30. This Pilot Guidance sets out the process for Home Office staff when considering electronic monitoring as a condition of immigration bail for persons who fall within the scope of the pilot.

31. In terms of privacy information, the Home Office provided the STS Bespoke Privacy Information Notice to the Commissioner on

30 January 2023 and the STS Privacy Information Notice GPS Expansion Pilot Cases on 21 August 2023. An updated version of the STS Privacy Information Notice GPS Expansion Pilot Cases was provided to the Commissioner on 13 October 2023 (the "STS PIN").

32. The Home Office provided copies of the Home Office EM Internal Data Request Form (the "Data Access Request Form") and the data access request guidance (the "Data Access Guidance") to the Commissioner on 6 January 2023. The Home Office provided the Process Control Document Process Data Requests v0.8SM and the Process data requests v0.10 to the Commissioner on 1 September 2023 ("the Process to Access Information"). These documents set out the process for Home Office staff to follow when accessing the trail data collected by the electronic tags.

33. In addition, the Home Office provided the Commissioner with an Appropriate Policy Document v3.0, GPS Expansion ROPA v2, and a document entitled General observations and recommendations outside pilot scope, on 21 August 2023. A "DPIA and Recs gap analysis document" was sent on 22 August 2023. A Glossary of Terms for DPIA 2 and a GPS Data Flow Map were provided to the Commissioner on 1 September 2023.

34. The Home Office did not refer to or provide any additional documents in its formal representations made following the PEN.

The purpose of the pilot

35. From paragraph 2 of the Draft DPIA V2.3 the purpose of the pilot is as follows:

> "This pilot will examine the impact of EM [electronic monitoring] on compliance with immigration bail and the

asylum process. At the end of the pilot, recommendations will be made regarding the efficacy or not of using EM as a condition of bail for those awaiting an asylum decision and/or following a negative decision.

The intended outcomes are as follows:

- The pilot is set up to tag a number of individuals who have arrived in the UK via unnecessary and dangerous routes and fail to have their claims considered under the detained asylum casework processes or are potentially inadmissible. The pilot is a mechanism for gathering the evidence to inform a future decision on wider roll out of GPS tagging, supported by the underpinning policy rationale of:

    - Increasing levels of compliance and improved and regular contact management, whilst reducing the risks of absconding;

    - Establishing whether tagging is an effective alternative to detention.

Data will be used to test whether electronic monitoring (EM) is an effective means by which to improve and maintain regular contact with asylum claimants who arrive in the UK via unnecessary and dangerous routes and more effectively progress their claims toward conclusion."

36. In Paragraph 3 of Draft DPIA V2.3, there is similar wording but with additional details. In particular, in addition to the policy rationale above, it also includes:

- "Ensuring that the data subjects are in regular contact with the Home Office throughout their application process.
- The Home Office has a duty to prevent asylum seekers absconding without appropriate leave to remain.
- Detention is the only current option that prevents absconding".

It goes on to state that "there is a potential benefit that it may assist in disrupting criminal networks – eg people traffickers". Finally in this section, the Home Office states that "The hypothesis [for the pilot] is that tagging individuals will reduce the rate of absconding".

37. The Pilot Guidance confirms this and sets out additional purposes (page 6):

> "…establishing whether electronic monitoring is an effective way to improve and maintain regular contact management with asylum claimants who arrive in the UK via unnecessary and dangerous routes, in order to progress their immigration case. We will also be able to test the rate of absconding and obtain data on how frequently this happens as well as developing a greater understanding of the stages in the process it is likely to occur and establish if electronic monitoring and associated improvements in contact management prevent absconding.
>
> If anyone does abscond and therefore breaches their conditions of bail, we will also be able to test whether we are able to use this knowledge to more effectively re-establish

contact with individuals or locate them for removal or detention if appropriate in their case. Trail data will be held by the EM supplier but may be accessed by the Home Office where one or more of the following applies and where proportionate and justified in the circumstances in accordance with data protection law:

- a breach of immigration bail conditions has occurred, or intelligence suggests a breach has occurred to consider what action should be taken in response to a breach up to and including prosecution
- where a breach of immigration bail conditions has occurred, which has resulted in the severing of contact via EM, trail data will be used to try to locate the person
- where it may be relevant to a claim by the individual under Article 8 ECHR
- to be shared with law enforcement agencies where they make a legitimate and specific request for access to that data."

38. The first two bullets above set out reasons why trail data will be accessed which form part of the operation of the pilot ("Operational Purposes"). The second two bullets are reasons why trail data may be accessed which do not form part of the operation of the pilot ("Non-Operational Purposes").

The pilot personal data

39. The personal data which will be processed for the pilot (the "pilot personal data") is set out in paragraph 2.1 of the Draft DPIA V2.3. The main description is:

> "**Bail Form Information** (The Bail 206) will include individuals Name, DOB, Nationality, Photograph, offending history and any vulnerabilities (for example health data) identified that the third party supplier may need to be aware of. This information is used to assess suitability for inclusion in the pilot and if selected is the identification information that links individuals to the tagging device.
>
> "**Electronic Monitoring Device**.
>
> Where individuals have an EM immigration bail condition imposed, the device (a fitted ankle tag) will send a notification where the conditions are breached using the GPS location information and time information recorded. The GPS equipment worn by individuals being monitored, transmits data events to the central servers. The data collected comprises latitudinal and longitudinal location data only. Movements around home address or other domestic addresses are not tracked. The device itself does not retain data.
>
> "Alerts received by the system are processed by EMS staff who will review the data, determine whether there is anything that amounts to a breach of the conditions and notify those breach events to the Home Office where appropriate."

40. In addition, the Draft DPIA V2.3 sets out that there will be a control group of individuals, who will meet the criteria but will not be electronically monitored. The Draft DPIA V2.3 sets out that the control group is:

> "...made up of individuals who met the condition for tagging as part of DAC or MEDP [Migration and Economic Development Partnership] but who are not tagged either following individualised assessment or as a consequence of a variety of other factors eg timing, tribunal activity etc which have no bearing on likelihood of absconding and therefore act as a legitimate comparator."

The DPIA sets out that no new data will be generated for this control group but rather the Home Office will rely on data which is already held on the Home Office systems as part of business as usual processes.

The pilot data subjects

41. The data subjects are the individuals who fall within the scope of the pilot, plus those in the control group.

ICO engagement with the Home Office

42. The ICO has been engaging with the Home Office since 11 August 2022. The Commissioner's understanding of the Home Office's processing, and his findings in this EN, are based on the information he has received over the course of his engagement with the Home Office.

43. During this engagement, the Commissioner raised concerns with the Home Office about the legality of processing of personal data captured by the GPS tags. The Commissioner raised concerns that

continuous monitoring of individuals using GPS tracking by an electronic tag is intrusive. These concerns related to the GPS tracking data which the device collects, both in terms of the volume and the nature of the data collected and the way the electronic tag is fitted and worn. The Commissioner identified concerns that the data protection impact assessment (DPIA) and privacy notice(s) provided by the Home Office did not meet UK GDPR requirements. The Commissioner also highlighted the importance of the Pilot Guidance and improvements which could be made.

44. On 6 July 2023, the Commissioner issued a report to the Home Office (the "Report"), setting out the Commissioner's concerns and recommendations for action needed to correct breaches of UK GDPR.

45. On 21 August 2023 the Home Office responded with:

- an Appropriate Policy Document regarding the Home Office's use of special category data;
- GPS Expansion ROPA v2;
- STS Privacy Information Notice (PIN) GPS Expansion Pilot Cases; the Draft DPIA V2.2 with a separate DPIA risk section 7.2;
- a DPIA and Recs gap analysis (correct version provided on 22 August 2023); and
- a document setting out General observations and recommendations outside the pilot scope.

46. On 1 September 2023, the Home Office provided the Commissioner with a Glossary of Terms for DPIA 2, GPS Data Flow Map and the Process to Access Information.

47. On 28 September 2023, the Commissioner provided the Home Office with a draft preliminary enforcement notice. The draft preliminary enforcement notice was shared at an early stage to allow the opportunity for early action by the Home Office to resolve the infringements. By email dated 13 October 2023 the Home Office responded with:

- the Draft DPIA V2.3 with an updated separate DPIA risk document (7.2(2));
- a link to the immigration bail guidance and the Pilot Guidance. This was the version published on 23 June 2023. This had not been updated after the draft preliminary enforcement notice;
- a copy of the Process to Access Information and Data Access Request Form. These documents had not been updated after the draft preliminary enforcement notice; and
- the STS PIN.

48. In the email of 13 October 2023 the Home Office confirmed that:

> "In reflecting on this draft preliminary enforcement notice, although a DPIA was in place prior to processing, it is acknowledged that initial interpretation of the legislation in this case, that a DPIA was not mandatory, resulted in the process and engagement that has since

needed to take place. Learning, following engagement with the ICO will be taken for the future."

49. On 19 December 2023, the Information Commissioner sent to the Home Office a Preliminary Enforcement Notice and a Notice of Intent to Issue a Warning which set out the Commissioner's provisional findings of infringement. They also set out how the Home Office may make both written and/or oral representations as to why the Commissioner should not issue an enforcement notice and about the Commissioner's provisional decision to issue a warning.

50. On 31 January 2024 the Home Office provided written representations to the Information Commissioner (the "Representations"). The Home Office did not request an oral hearing.

51. This EN relates to matters to which the Report and PEN were directed and takes into account the documents set out in paragraphs 28 - 33 above.

52. The Commissioner recognises the approach taken by the Home Office to address some of the issues of concern raised . Careful consideration has been given to all of the relevant material provided by the Home Office at all stages of the process.

53. This EN relates only to matters which in the view of the Commissioner have not yet been addressed and applies to the ongoing processing of pilot personal data

PART IV: THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

A. CONTROLLERSHIP AND JURISDICTION

54. The Commissioner is satisfied that the Home Office is the controller of the pilot personal data , and that UK GDPR applies to the Home Office as controller under Article 3(1).

55. The Home Office processes personal data for its management of immigration, including individuals entering or leaving the UK, securing the border, leave, settlement, citizenship or other immigration services, claiming asylum or other forms of protection. The Home Office also processes personal data as part of its functions to enforce immigration laws, law enforcement for criminal matters, and other lawful matter including those related to public health. The Home Office is the controller for this information, including when the information is collected or used by third parties on its behalf.

56. The Commissioner's assessment is that the Home Office has committed a number of infringements of the UK GDPR in relation to its processing of the pilot personal data. These are addressed below.

B. INFRINGEMENT OF ARTICLE 35 UK GDPR

57. For the reasons set out below, the Commissioner's assessment is that the Home Office has failed and is failing to comply with Article 35 UK GDPR in relation to its processing of the pilot personal data.

Legal Framework – Article 35

58. Article 35 UK GDPR requires controllers, prior to processing, to carry out a DPIA where processing is likely to result in a high risk to the rights and freedoms of individuals.

59. A DPIA is a process designed to help controllers systematically identify and analyse data protection risks to individuals arising from the processing of personal data, and to minimise those risks as far as possible.

60. Article 35(1) requires that:

> "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

61. Article 35(7) sets out the requirements for this assessment (known as a data protection impact assessment or DPIA).

62. A controller could breach Article 35(1) in several ways, including because:

- it has not carried out a DPIA at all,
- it carried out a DPIA but it does not meet the requirements of Article 35(7).

- it carried out a DPIA which meets the requirements of Article 35(7) but not prior to the relevant processing.

63. Article 35(3) lists three types of processing that automatically require a DPIA. These are:

(a) "systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale."

64. Article 35(4) requires the Commissioner to "establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1".

65. Accordingly, as required by Article 35(4) UK GDPR, the Commissioner has published a list of ten examples of processing "likely to result in high risk"[4] (referred to as "ICO DPIA Examples").

[4] Examples of processing 'likely to result in high risk' | ICO

66. Article 35(7) specifies what is required, at a minimum, to be included in a DPIA carried out in compliance with Article 35(1). The assessment must contain:

> (a) "a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
>
> (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
>
> (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
>
> (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."

The requirement for the Home Office to carry out an Article 35 DPIA prior to the start of the processing

67. The Commissioner's assessment is that the Home Office was required by Article 35(1) to have carried out a DPIA which met the requirements of Article 35(7), prior to the start of the processing of the pilot personal data, for the reasons set out below.

68. **First**, the processing of personal data for the pilot falls within Article 35(3)(a) as it involves:

> "systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;"

69. ICO guidance sets out when processing is "systematic":

> "'systematic' means that the processing:
>
> - occurs according to a system;
> - is pre-arranged, organised or methodical;
> - takes place as part of a general plan for data collection; or
> - is carried out as part of a strategy."

70. The pilot involves systematic processing as the GPS tags will systematically collect personal data regarding the location of the data subjects at specific times and dates.

71. ICO guidance sets out when processing is "extensive":

> "The term 'extensive' implies that the processing also covers a large area, involves a wide range of data or affects a large number of individuals."

72. The pilot involves extensive processing because, overall, it captures a very large volume of personal data. In particular, the processing has the potential to cover trail data sent from a large area (GPS tags will collect the trail data of the data subjects), and a wide range of data can be inferred from it.

73. The pilot involves automated processing as the GPS tags automatically collect and send the trail data of the data subjects

to the Home Office's processor. As the ICO guidance states, "the processing occurs according to a system."

74. The trail data will be used by Home Office staff to make decisions regarding the data subjects which will have legal effects. For example, whether the data subject has breached the conditions of their immigration bail and what actions the Home Office will take, for example whether the data subject should be detained as a result.

75. **Second**, the processing of personal data under the pilot falls within at least three of the ICO DPIA Examples of processing "likely to result in a high risk to the rights and freedoms of natural persons", as set out in the following paragraphs.

76. ICO DPIA Example 2: Denial of service:

> "Decisions about an individual's access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data."

77. The trail data may include special category data (see paragraphs 95-101 below). The Home Office staff will be using that data to make decisions as to whether a data subject has breached their bail conditions and whether that means those conditions need to be altered or immigration bail revoked.

78. ICO DPIA Example 3: Large scale processing:

> "any profiling of individuals on a large scale"

79. The processing of personal data for the pilot is "large scale processing" because a large volume of trail data about the data subjects will be collected. It is profiling as the trail data records

the location, movements and behaviours of the data subject. For the purpose of assessing whether processing operations require a DPIA, it is not relevant that the large volume of trail data will only be accessed by the Home Office staff in limited circumstances.

80. This is very similar to one of the examples in the Commissioner's guidance, namely "tracking individuals using a city's public transport system."

81. ICO DPIA Example 8: Tracking, when combined with any of the criteria from the European guidelines[5]:

> "processing which involves tracking an individual's geolocation or behaviour."

The Home Office processing of trail data involves tracking both geolocation and behaviour.

82. The relevant criteria within the European guidelines are: processing of sensitive data or data of a highly personal nature; processing of data on a large scale; and processing personal data concerning vulnerable data subjects.

83. The pilot is likely to involve sensitive data and data of a highly personal nature, including special category data. This is because trail data contains a data subject's time and date of visits to particular locations which could reveal this information, such as a visit to a specific medical clinic.

84. The pilot involves processing of personal data on a large scale due to the volume of trail data collected about data subjects. A

[5] "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" Adopted on 4 April 2017. As last Revised and Adopted on 4 October 2017

significant number of data subjects are likely to be vulnerable (see paragraphs 102-110 below).

The Home Office's infringement of Article 35(1) – to carry out a DPIA which meets the requirements in Article 35(7)

85. The Home Office completed its first DPIA for the pilot on 26 January 2022, GPS Expansion (small Boats) final version 0.1. Version 2.0 was signed off by the ODPO (the office of the data protection officer) before the pilot started. The ICO on behalf of the Commissioner provided detailed comments on this Version 2.0, setting out how it needed to be improved to bring it into line with Article 35.

86. This version of the DPIA has since been updated a number of times to form the Draft DPIA V2.3. The Commissioner's assessment is that none of the versions of the DPIA meet the requirements of Art 35(7).

87. For the purpose of this EN the Commissioner has focused only on the deficiencies in the most recent version, being Draft DPIA V2.3.

88. An analysis of the four component parts of Article 35(7) is set out in turn below, ie Articles 35(7)(a), 35(7)(b), 35(7)(c) and 35(7)(d).

89. Before identifying the infringements in detail, the Commissioner makes the following overarching comments in relation to the DPIAs provided by the Home Office:

    - The Commissioner is mindful of the Home Office's statutory obligations to keep citizens safe and the country secure through maintaining the integrity of the UK's borders and managing immigration effectively.

- The limited level of detail included in the DPIAs was not commensurate with the nature, context and scope of processing for the pilot, and therefore did not comply with the requirements of Article 35(7).

- The level of detail required by Article 35(7)(a) is vital for the Home Office to: make a proper risk assessment and assessment of the necessity and proportionality of the processing for its purposes; to be in a position to effectively mitigate any risks; and to document compliance with Article 5(1).

- This assessment should have demonstrated whether there were any reasonable alternatives to electronic monitoring. This would have allowed the Home Office to decide whether the level of intrusiveness of electronic monitoring was necessary and proportionate when considering those alternatives.

- As a result of the breaches of Article 35, the Home Office was unable to rely on Draft DPIA V2.3 to demonstrate it was processing personal data for the pilot in compliance with UK GDPR and was unable to meet the requirements of Article 5(2) to be able to demonstrate compliance with Article 5(1) (See from paragraph 53 onwards and below).

Assessment of whether Draft DPIA V2.3 meets the requirements of Article 35(7)

90. Set out below is the Commissioner's assessment of whether Draft DPIA V2.3 meets the requirements of each of Articles 35(7)(a) to 35(7)(d). His conclusion is that the Home Office has failed to produce a DPIA which meets these requirements.

Article 35(7)(a): "a systematic description of the envisaged processing operations and the purposes of the processing including, where applicable, the legitimate interest pursued by the controller"

91. The ICO's DPIA guidance[6], following UK GDPR recital 90, states that DPIAs must include a description of how and why the controller plans to use the personal data, and that this description must include the nature, scope, context and purposes of the processing.

92. The Commissioner's assessment is that the Home Office did not systematically describe the processing operations it was undertaking for the purposes of the pilot in the Draft DPIA V2.3, and as a result, the Draft DPIA V2.3 did not sufficiently describe the nature, scope, context and purposes of processing, as set out in the following paragraphs.

(i) The nature of the processing

93. The Commissioner's assessment is that the Home Office did not sufficiently explain in its Draft DPIA V2.3 the nature of the processing. In particular, there was insufficient information and/or not enough detail of:

- The categories of personal data being processed at each stage, for each processing operation. In particular, Draft DPIA V2.3 lacked clarity about which categories of personal data were being processed for each purpose that had been listed.

- The Data Flow map that the Home Office refers to in their Representations was not referenced in the DPIA.

[6] How do we do a DPIA? | ICO

- The circumstances under which the Home Office staff could access the trail data, and the conditions and restrictions that must or could be placed upon that access (including where the trail data is being provided to a third party agency). Section 2.1 of the DPIA lacked detail about the conditions and restrictions that must or could be placed upon any access (including where the trail data is being provided to a third party). In its Representations, the Home Office states that this information is contained in its "Process Control Document" V0.8. However, this document was not referenced in Draft DPIA V2.3.

- The safeguards in place for the access and ongoing retention of trail data to demonstrate that access and ongoing retention is necessary, proportionate and compatible with the purpose of the processing.

(ii) The scope of the processing

94. The Commissioner's assessment is that the Home Office did not sufficiently explain in its Draft DPIA V2.3 the scope of the processing (ie what the processing covers), including:

- details of the volume, frequency and nature of the trail data. It does not explain in enough detail the data sent by the electronic tags ;

- what special category data is processed for the pilot (see paragraphs 95-101 below); and

- detailed identification of the assessment of whether individuals could be vulnerable and their actual and potential vulnerabilities and risks. (see paragraphs 102-110 below).

Special category data

95. In the Draft DPIA V2.3, section 2.3 sets out that the processing included criminal conviction data, race or ethnic origin (including nationality) and health. The Home Office stated that this is data it was already processing as part of its immigration case file.

96. The Draft DPIA V2.3 set out that health data was used in the assessment of suitability for electronic monitoring. It also stated that nationality is not special category data but that the Home Office routinely treats this in the same way as it does race or ethnicity to protect the individual to the same level.

97. The Draft DPIA V2.3 accepted that trail data could be used to determine the precise type of place that the data subject is attending but stated that:

"...this information is not required for the purpose of this trial and will not be used to infer anything about their nature or behaviour."

98. The Home Office stated in its Representations that it specifically ruled out inferring any special category data from the trail data, and does not agree that trail data is "highly likely" to constitute special category data.

99. In this situation, personal data in the trail data is special category data if, in and of itself, the personal data reveals the special category data with a reasonable degree of certainty.

100. The Commissioner's assessment is that there is a likelihood (that is more than minimal) that the Home Office will on occasion be processing special category data when it processes the trail data alongside information about the places the data subject visits. For example, a map showing the use of buildings and/or the names

and locations of organisations. This likelihood is outside of the Home Office's control as it depends on the data subject's movements. The trail data when processed alongside that information, will, on occasion, in and of itself reveal special category data. For example, personal data showing a person attending a religious building each week on the day of regular worship, in and of itself reveals their religion with enough certainty that this is special category data.

101. The Home Office processed the trail data alongside this type of information when it accessed and used the trail data for its Operational Purposes. This may also be the case for its Non-Operational Purposes. How likely it is that the Home Office will process special category data is dependent on the number of data subjects whose trail data is accessed, but it is a (more than minimal) possibility with every data subject. On that basis, the Home Office must consider that using the trail data alongside this type of information will be processing special category data.

Vulnerable data subjects

102. In Draft DPIA V2.3 the conclusion is reached that the processing will not involve "mostly data concerning vulnerable data subjects." The Draft DPIA V2.3 sets out that "any material vulnerability will be considered as part of the assessment prior to tagging. Any individuals that may be unduly affected as a consequence of electronic monitoring will not be included in the pilot."

103. The Draft DPIA V2.3 does not provide any basis for this conclusion that the trail data does not "mostly" concern vulnerable data subjects.

104. In its Representations, the Home Office refers to the section in the DPIA which screens for potentially vulnerable data subjects, and states that the "Immigration Bail conditions documents provide guidance in relation to vulnerabilities".

105. The guidance on "Vulnerability consideration" is in the "Immigration Bail" guidance on pages 31 to 35. and in the "Immigration Bail conditions: Electronic monitoring expansion pilot" guidance on pages 13 and 14. The latter guidance also refers back to the main Immigration Bail guidance.

106. Both contain a non-exhaustive list of conditions/issues/ considerations which could mean that a person is not suitable for an electronic monitoring condition. The lists are very similar, but not identical. In both cases the list sets a high bar for vulnerability. For example, both lists require medical evidence that an electronic monitoring condition would cause serious harm, or evidence that a claim of torture or modern slavery has been accepted by the Home Office or a Court. Although neither are exhaustive lists, the implication is that other conditions/issues/ considerations must be of a similarly serious nature.

107. Home Office's stated purpose is to consider "material vulnerability" as part of the decision whether or not to issue an electronic monitoring condition. This is not the same as the requirement in a DPIA to consider any vulnerability of data subjects.

108. The ICO Guidance[7] sets out how to consider if an individual is vulnerable when conducting a DPIA. It says:

[7] When do we need to do a DPIA? | ICO

> "Individuals can be vulnerable where circumstances may restrict their ability to freely consent or object to the processing of their personal data, or to understand its implications.
>
> "Even if the individuals are not part of a group you might automatically consider vulnerable, an imbalance of power in their relationship with you can cause vulnerability for data protection purposes if they believe that they will be disadvantaged if the processing doesn't go ahead."

109. The Commissioner considers that a detailed assessment of vulnerabilities is required as there is a risk that a significant number of individuals within the scope of the pilot could be vulnerable. This is because of (inter alia) the conditions they have come from, the circumstances of their journey, their reception and experiences in the UK, their level of English language skills and the imbalance of power between the data subjects and the Home Office. The Home Office has not provided any Representations as to why this might not be the case.

110. The Draft DPIA V2.3 does not address the risk of vulnerabilities and therefore does not consider whether any mitigating factors should be put in place. This means the Draft DPIA V2.3 does not consider if there are increased or additional risks to the vulnerable, nor how to mitigate those risks.

(iii) The context of the processing

111. The context of the processing involves considering the wider picture, including (inter alia) how far individuals are likely to expect and understand the processing.

112. The Draft DPIA V2.3 at paragraph 2.7 sets out that individuals will be informed of their privacy rights through the privacy notice(s). The Home Office in its Representations has referred to the Immigration Bail Conditions guidance which states that:

> "It is important that decision makers inform the bailed person of their responsibilities regarding electronic monitoring and how their data can be used".

This may have assisted the understanding of some data subjects. But this is not referred to in the Draft DPIA V2.3, so could not form part of the "context" for consideration.

113. As set out at paragraphs 184-188 below, the Commissioner's assessment is that the Home Office has failed to demonstrate compliance with its transparency obligations under Article 5(1)(a) and articles 12 and 13.

114. The Commissioner's assessment is that there is a significant risk that some data subjects, in particular those who are vulnerable, will not understand how their personal data is being processed and for what purposes. He understands that for some data subjects this risk has been mitigated by Home Office staff explaining how their data would be used. This should have been noted in the DPIA as part of the context, alongside further detail as to how this information must be delivered and recorded. On that basis, his assessment is that the context of the processing has not been set out in enough detail in Draft DPIA V2.3.

(iv) The purpose of the processing

115. The Commissioner's assessment is that while the Home Office may have set out all of its purposes in processing the personal data somewhere in the Draft DPIA V2.3, they are not set out

precisely and in sufficient detail in one place, so that the Home Office could correctly carry out the assessment of necessity and proportionality of the processing operations in relation to the purposes (required by Article 35(7)(b)) and an assessment of the risks to the rights and freedoms of the data subjects (required by Article 35(7)(c)).

116. The purpose is set out in sections 2 and 3 of the Draft DPIA V2.3 (which are set out in full in paragraph 34, 35 and 36 above). Although the lawful basis for processing is set out at sections 3.2, 3.3 and 3.4 of the DPIA, for clarity, the Commissioner also recommends that the Home Office links its purposes to both its Article 6(1)(e) public task and its Article 9(2)(g) public interest condition.

Article 35(7)(b): "an assessment of the necessity and proportionality of the processing operations in relation to the purposes"

117. In accordance with Article 35(7)(b), the DPIAs must contain an assessment of the necessity and proportionality of each processing operation in relation to the purposes.

118. ICO guidance[8] explains that, in considering necessity and proportionality, controllers should assess:

- if the plans help to achieve their purpose; and
- if there is any other reasonable way to achieve the same result.

119. The assessment of proportionality and necessity is set out in section 3.1 of the Draft DPIA V2.3. For the reasons set out in the following paragraphs, the Commissioner's conclusion is that this

[8] How do we do a DPIA? | ICO

was not a complete, reasoned analysis of whether each of the processing activities in the pilot is necessary and proportionate for the purpose.

120. The details set out within the Draft DPIA V2.3, and in particular section 3.1, were too high level and did not provide a sufficient consideration of all the factors involved, nor the underlying evidence base.

121. There was insufficient consideration of any reasonable alternatives, and whether the level of intrusiveness of electronic monitoring is proportionate when considering those alternatives. The Draft DPIA V2.3 set out that to date, no options other than detention have been identified as available to control rates of absconding. The Commissioner's view is that if no other options were identified as available to control rates of absconding, then the DPIA should have specified the options or alternatives which had been considered but discounted and explain why each alternative was rejected.

122. Section 3.1 of the Draft DPIA V2.3 explains that:

> "When [trail] data is requested, the requester must prove the need for the data and that they have considered the amount of data that is required. All applications are scrutinised by the Service Delivery Team who reject any requests where they determine that proportionality and/ or necessity are not adequately proven."

This sets out how the decision was made to allow access to trail data, but it is not a complete, reasoned analysis of the necessity and proportionality when access is given to the trail data.

123. The Home Office in its Representations has referred to Section 2.1 which explains that:

> "Data collected is not accessed unless an exception alert is triggered. Authorised Home Office staff may request access to GPS trail data for a specified period and review that data in the event of [a list of specific occurrences, such as a breach of Immigration Bail Conditions].

This section sets out circumstances when Home Office staff will access trail data for their Operational Purposes. Again, it is not a complete, reasoned analysis of the necessity and proportionality when access is given to the trail data.

124. Section 3.1 of the Draft DPIA V2.3 explains that the pilot is a mechanism for gathering evidence to inform a future decision on wider roll out of electronic monitoring, supported by the underpinning policy rationale of:

- Ensuring that the data subjects are in regular contact with the Home Office throughout their application process.
- The Home Office having a duty to prevent asylum seekers absconding without appropriate leave to remain.
- Detention as the only current option that prevents absconding.

There is no detail setting out an assessment that processing personal data for the pilot (including all categories of data) is necessary and proportionate for those stated goals.

125. Section 3.1 states that data subjects are "effectively randomly assigned whether they are provided with a tag or not once their

suitability has been assessed based on factors unrelated to the likelihood of absconding." This statement, without further explanation as to the rationale for this selection process, does not sufficiently explain how choosing the particular pilot participants will assist the Home Office in meeting its stated purposes. As a result, it fails to set out how the selection of each participant is necessary and proportionate for the purpose of the pilot.

126. Section 3.1 of the Draft DPIA V2.3 also states that data subjects will not be electronically tagged if it would breach "Convention Rights" (meaning Human Rights under the Human Rights Act 1998) or if it is not practical to do so, and that this assessment is taken on a case by case basis, with representations invited. There is insufficient further detail as to the circumstances in which electronic monitoring might breach Convention Rights or be deemed not to be practical, and insufficient detail is given as to the means by which Home Office staff will identify potential Convention Rights interferences. The Commissioner's views on how the Pilot Guidance deals with Convention Rights are addressed further at paragraphs 171-174 below.

127. The tenth paragraph of section 3.1 of the Draft DPIA V2.3 sets out that data subjects will be given a new notice. There is not enough detail to demonstrate how data subjects are informed about how their data is being processed, particularly taking into account their circumstances and potential vulnerabilities. (See paragraphs 184-188 in relation to the Commissioner's assessment of the extent to which the Updated Privacy Notice(s) comply with UK GDPR). We note that Home Office has stated in its Representations that

> "Whilst privacy notices were available, the primary communication method was via direct engagement (given the limitations of privacy notices in this context)"

128. The Commissioner acknowledges the benefit of this approach, but additional details would be needed to explain how this information was effectively delivered and documented. This must be recorded within the DPIA so this can be taken into account as part of the necessity and proportionality test.

129. The DPIA should contain an assessment of the necessity and proportionality of retaining the data and the safeguards in place for access to retained data. This should include justification for the retention periods. In light of the volume and sensitivity of the trail data collected this should include an assessment of whether all the trail data is required to be retained for the stated retention periods.

130. The Home Office in its Representations explained that:

> "Standard Home Office policy applies (in most cases, this will be six years after the closure of the claim). The six year retention period was determined over a period of years and allows time for judicial reviews, complaints and legal reparation. Where information is used as part of a criminal investigation the standard law enforcement retention times will apply once the data is moved to the investigation service."

131. The DPIA should have documented that the Home Office had considered whether the standard Home Office policy of a 6 year retention period should apply, and the reasons why it was decided that it does. The Commissioner agrees that in principle a 6 year

retention period may be appropriate, provided Home Office has decided that this complies with the principle of data storage limitation for these particular types of personal data. The DPIA should also have noted that any pilot personal data which is used as part of a criminal investigation will then be retained in line with the retention periods of the Home Office investigation service.

132. Where access to the trail data forms part of the Operational Purposes of the pilot, the DPIA must set out whether this processing is also necessary and proportionate for the purposes of the pilot and is in compliance with UK GDPR generally (such as the Article 5(1)(c) principle of data minimisation). This is not in Draft DPIA V2.3.

133. Where access to the trail data is supplementary to the purposes of the pilot (the Non-Operational Purposes), there is no need for a detailed necessity and proportionality assessment within the DPIA itself as long as this assessment is made as part of the process prior to access being granted. There should be detailed guidance in place to reflect this and ensure that Home Office staff carry out the assessment correctly. The DPIA should refer to this decision process to ensure UK GDPR compliance. This is not referred to in Draft DPIA V2.3.

Article 35(7)(c): "an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1"

134. Article 35(7)(c) states that a DPIA shall contain at least:

> "...an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1."

135. The ICO's DPIA guidance[9] states that controllers should consider the potential impact of the processing on individuals, and any harm or damage the processing may cause (whether physical, emotional or material).

136. Section 7 of the Draft DPIA V2.3 set out the "Risks of the Processing." Only two risks were identified: (1) "processing of data relating to an individual's whereabouts during the monitoring period" and (2) "the individual is subjected to monitoring and the data that this produces."

137. The Draft DPIA V2.3 additional risk section 7.2(2) set out the following additional risks: 1(A)&(B) "continuous access to data/monitoring, inappropriate access and/or use of data"; 1(C)&(D) "use of data collected not compatible with purpose, misuse of special category data, unauthorised access to data"; 1(E) "unauthorised access to data"; and 1(F) "risk to vulnerable data subjects."

138. There is a column in the additional risk section 7.2(2) headed "Impact", but for each risk the detail is insufficient. For example, for risk 1(A), (B) and (C) it states "intrusion on privacy (disproportionate to the purpose of collection)."

139. The Commissioner's assessment is that more detail on risks and impact is needed here, beyond a high-level statement of the types of risk and impact. The DPIA should detail and consider:

    - the risks and impact of physical, psychological and material harm. The Home Office should refer to the ICO's

[9] How do we do a DPIA? | ICO

harms taxonomy[10]. For example, the risks of stigmatisation of data subjects and inhibited movement;

- the potential risks and impact to vulnerable data subjects;
- the potential risks and impact of processing special category data;
- the risk and impact to a data subject if a Home Office staff member mistakenly issues an electronic tag in breach of Convention Rights and/or without understanding their vulnerability;
- the risk and impact of at least some data subjects being unlikely to have a comprehensive understanding of the data processing activities associated with electronic monitoring and the associated risks to them, due to their circumstances;
- the risk and impact of a lack of transparency regarding the data processing activities associated with electronic monitoring, which may undermine, complicate or hinder the data subjects' exercise of their rights; and
- risks and impacts related to compliance with the data minimisation principle in Article 5(1)(c) when accessing trail data.

140. The above paragraph does not represent a comprehensive list of the risks arising from processing connected to the pilot and the potential harms that could be caused.

[10] Overview of Data Protection Harms and the ICO Taxonomy

141. The Home Office in its Representations has stated that "these risks are more speculative, contingent and more remote in nature than the rest listed or than is usually considered in such circumstances".

142. The Commissioner strongly disagrees with this representation. An important part of a DPIA is to undertake a comprehensive review of risks based on the likelihood and severity. Of course it is not always possible for a DPIA to cover every risk, and it is reasonable to omit risks which are too speculative and too remote. However, the risks outlined in paragraph 139 above should have been included in the risk assessment. In each case there is more than a minimal risk of occurrence, in particular given the number of data subjects, their vulnerabilities and the invasive nature of the processing.

143. The Commissioner's assessment is that, in breach of Article 35(7)(c) UK GDPR, the Home Office has either failed to assess, or has inadequately assessed, the risks to the rights and freedoms of data subjects arising from the processing connected with the pilot.

Article 35(7)(d) "the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned".

144. The Commissioner's view is that the Home Office's assessment of measures to address the risks was insufficient to meet the requirements of Article 35(7)(d).

145. The risk assessment table sets out a number of mitigating actions which the Home Office has taken to reduce or eliminate the risks identified. However, without a full and complete assessment of the potential risks to data subjects in accordance with Article 35(7)(c), the measures to address risk in the pilot are insufficient.

146. Paragraph 7.3 of the Draft DPIA V2.3 poses the question: "Can you demonstrate that the risk to the individuals is sufficiently balanced by the perceived public protection benefits[?]". In response, the Draft DPIA V2.3 states that:

> "GPS expansion is still a Pilot at this stage to test the use of Electronic Monitoring (EM) as a condition of immigration bail for those making hazardous journey to the UK. If a decision is made about its wider roll-out, the team will test and weigh the risks to the individuals against the perceived benefits."

147. The Commissioner acknowledges that the fact this is a pilot did provide allowances in the evidence base for decisions. The Commissioner's view is that a pilot still required a detailed risk assessment and effective risk mitigation, given that the data subjects involved in the pilot would have been exposed to any relevant risks.

148. The Commissioner's view is that the Home Office has not fully complied with the requirements of Article 35(7)(d). The mitigation measures listed in the Draft DPIA V2.3 were not based on a sufficiently detailed risk assessment (in accordance with Article 35(7)(c)) and so the Home Office cannot assess if the mitigations are appropriate.

INFRINGEMENT OF ARTICLE 5(2) UK GDPR

149. The Commissioner's assessment is that the Home Office has failed and is failing to comply with Article 5(2) UK GDPR in relation to its processing of the pilot personal data for the reasons set out below.

Legal Framework – Article 5

150. Article 5(1) UK GDPR imposes a requirement on controllers to only process personal data in accordance with six principles:

> "(1) Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the

purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

151. There is a seventh principle, which is set out in Article 5(2) UK GDPR:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

The Home Office's failure to comply with Article 5(2): the principle of accountability

152. The Commissioner's assessment is that the Home Office has failed and is failing to adequately demonstrate its compliance with:

- Article 5(1)(a), the principle of lawfulness, fairness and transparency; and
- Article 5(1)(c), the principle of data minimisation.

153. In these circumstances, the principle of lawfulness, fairness and transparency requires compliance with (inter alia) four key UK GDPR Articles:

- **for lawfulness**: Article 6 (lawfulness of processing) and Article 9 (processing of special categories of personal data); and
- **for fairness and transparency**: Article 12 (transparent information, communication and modalities for the exercise of the rights of the data subject) and Article 13 (information to be provided where personal data are collected from the data subject).

The Home Office must demonstrate its compliance with those four Articles, to comply with Article 5(2).

154. The Commissioner accepts the Home Office's Representation that the UK GDPR does not require compliance with Article 5(2) in any particular form. The Commissioner has based his assessment on the documents provided by the Home Office, and notes that the Home Office has not provided any further documents with its Representations for consideration. On that basis, the Commissioner concludes that there are no additional documents

which demonstrate the Home Office's compliance with the purpose of compliance with Article 5(2).

155. For '**lawfulness'**, the key documents are: the Draft DPIA V2.3, the Pilot Guidance, the Data Access Request Form, the Data Access Guidance and Process to Access Information.

156. For '**fairness and transparency'**, the key documents are those provided as privacy information. From Draft DPIA V2.3, these are:

- the departmental privacy notice (the Home Office's high level privacy notice: Borders, immigration and citizenship: privacy information notice);
- privacy information within the EMS booklet; and
- the STS PIN.

In this EN, these documents together will be referred to as the "Updated Privacy Notice".

157. For '**data minimisation'**, the key documents are Draft DPIA V2.3, the Data Access Request Form, the Data Access Guidance and the Process to Access Information.

158. The Commissioner's assessment is that the cited documents do not demonstrate compliance with the relevant Article 5(1) principles, and on that basis the Home Office has failed and is failing to comply with Article 5(2). The details are set out in the following paragraphs.

(i) LAWFULNESS: demonstrating compliance with Article 6 (lawfulness of processing) and Article 9 (processing of special categories of personal data)

159. The Commissioner's assessment is that the Home Office has failed and is failing to demonstrate its compliance with Articles 6 and Articles 9, for the reasons set out below.

Draft DPIA V2.3:

160. From Draft DPIA V2.3, the Home Office is processing pilot personal data under the Article 6(1)(e) lawful basis:

> "...processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

161. According to Draft DPIA V2.3 the Home Office is processing special category personal data for the pilot under Article 9(2)(g) and schedule 1 paragraph 6 of the DPA, which together require that processing is (a) necessary for either the exercise of a function conferred on a person by an enactment or the rules of law, or a function of a Minister of the Crown or government department; and (b) is necessary for reasons of substantial public interest.

162. In these circumstances, the public 'task' referred to in paragraph 160 above, and the public 'functions' referred to in paragraph 161 above, are the same, being those functions of the Home Office set out in various immigration statutes (see paragraphs 19-21 above) (the "relevant public tasks/functions").

163. The Commissioner's view is that the Home Office has not demonstrated in the Draft DPIA V2.3 the assessment of how

processing of pilot personal data is necessary and proportionate for each processing activity needed for the Home Office to carry out relevant public tasks/functions. More information on this is set out in paragraphs 117-133 above.

The Pilot Guidance, the Data Access Request Form, the Data Access Guidance and Process to Access Information

164. Furthermore, the Commissioner's assessment is that the guidance given to Home Office staff in the Pilot Guidance, the Data Access Request Form, the Data Access Guidance and Process to Access Information, does not demonstrate that the Home Office is only processing the pilot personal data when it is necessary and proportionate for the Home Office to carry out relevant public tasks/functions. In particular, when its staff processes pilot personal data in relation to:

(a) deciding whether or not to issue an electronic monitoring bail condition to a data subject; and

(b) accessing the trail data.

(a) In deciding whether or not to issue an electronic monitoring bail condition to a data subject

165. In deciding whether or not to issue an electronic monitoring bail condition to a data subject: the decision-making process laid out by the Pilot Guidance is that the presumption is that electronic monitoring should be used unless:

- one of only four exceptions apply, namely the data subject is under 18, has been released from detention under sections 37 or 41 of the Mental Health Act 1983 and remains subject to a supervision order, is pregnant

(18+ weeks) or has recently given birth (up to 3 months post-partum), or resides in Scotland or Northern Ireland. However this can be overridden by an Assistant Director; or

- it is impractical; or
- it would breach Convention Rights.

166. Home Office in its Representations stated that:

"These were not the only exemptions – they were merely the exemptions that definitely applied in every case. There was no presumption that EM should be used unless a limited set of exemptions applied. Decision makers were able to take a non-exhaustive list of practical reasons and representations into account.

"Immigration bail conditions guidance:

There will be some cases that may not be suitable for an EM condition for practicality reasons or because there is a risk that their rights under ECHR could be breached. When reviewing the individual circumstances of the particular case and deciding whether it is appropriate to monitor a person, the following should be taken into consideration:

- whether there is strong independent medical evidence to suggest that an EM condition would cause serious harm to the person's mental or physical health
- whether a claim of torture been accepted by the Home Office or a Court

- whether there has been a positive conclusive grounds decision in respect of a claim to be a victim of modern slavery
- whether the person's mental capacity is deemed to be a bar to understanding the EM conditions and therefore their ability to comply for example, a person suffering with dementia
- whether the individual is suffering with phlebitis or similar conditions which cause swelling of the lower legs
- whether the individual is showing any signs of frailty or age-related conditions which may impact on the person's ability to wear and/or maintain the device

The above list is not exhaustive: decision makers must consider the individual circumstances of each case."

167. It seems that the stated intention of the Home Office in its Representations, is not reflected in the Pilot Guidance. The Commissioner remains of the view that the way the decision making process is explained in the Pilot Guidance does mean there was a presumption that electronic monitoring must be used unless limited exceptions applied. In particular:

- The first key section is the list of 4 exemptions, under the heading 'Use of EM', on page 8 of the Pilot Guidance. The effect of this on the decision making process is that only those people who fit within the exemptions are ruled out of electronic monitoring.

- The second key section is on page 13 of the Pilot Guidance. It states that:

> "There will be some cases that may not be suitable for an EM condition for practicality reasons or because there is a risk that their rights under ECHR could be breached."

The effect of this sentence is that the presumption is that an electronic monitoring condition should be imposed unless there is a practicality reason or a risk to ECHR rights.

168. The fact that this is the guidance provided (in other words, that the presumption for Home Office staff is to electronically tag a data subject) means that two further actions should have been taken by the Home Office:

- first, the DPIA should have explained why adopting a default position of tagging the data subject unless one of a limited and explicit list of exceptions applies was necessary and proportionate for the relevant public tasks/functions. This is not the case here (see paragraphs 117-133); and
- second, the Pilot Guidance should have set out a detailed and (near) exhaustive set of situations in which the default presumption will be inapplicable and/or detailed guidance how to decide if the electronic monitoring is impracticable or breaches rights under ECHR. This is not the case here (see paragraphs 170-177).

169. Without this, the Home Office is unable to demonstrate why, for each data subject, the decision to tag them was necessary and proportionate for the purpose of the pilot and the relevant public tasks/functions.

170. In particular, there is no or limited guidance as to:

- when an Assistant Director should decide to issue an electronic monitoring condition despite one of the exceptions applying;
- when an electronic monitoring condition is "impractical". Just two paragraphs are provided on this point, at page 10 of the Pilot Guidance, with the only example being that "an individual may reside in a property which has both a poor GPS signal and is not served by electricity"; and
- when an electronic monitoring condition breaches Convention Rights (although this seems to be in the wrong section of the guidance).

171. The main section in the Pilot Guidance on how Home Office staff should apply Convention Rights sets out a list of considerations for staff when "deciding whether it is appropriate to monitor a person". This is the list of criteria set out in the Representations in paragraph 166 above.

172. The Pilot Guidance states that meeting one of these criteria does not prohibit imposing an electronic monitoring bail condition. The Home Office staff must consider the balance between that and other (unnamed) factors. The Pilot Guidance requires that the decision to impose in that situation must be agreed by at least an Assistant Director. There is no further detail in the Pilot Guidance as to how those decisions should be made to ensure compliance with Convention Rights and UK GDPR.

173. In finding that balance, it is not clear if the alternative is detention or alternative bail condition(s).

174. If the Home Office staff member did not consider it appropriate to issue an electronic monitoring bail condition for a different reason, this had to be signed off at least at SEO level. There is no further detail in the Pilot Guidance as to how those decisions should be made to ensure compliance with Convention Rights and UK GDPR.

175. The Pilot Guidance requires medical evidence but acknowledges that it may take time to substantiate that claim (up to 28 days). There is no reference to allowing time for the Home Office or a court to accept a claim of torture, or for a Home Office decision that the data subject is a victim of modern slavery.

176. The Pilot Guidance sets out when representations from the individuals must be invited. The Home Office has stated in its Representations that:

> "The HO is under various legal duties to consider the rights position and welfare of data subjects and this standard of care won't change materially whether a person makes representations or not or makes less or limited representation because of the power balance. The representations mechanism is designed as an additional evidence gathering route to assist carrying out HO duties. If an individual didn't make representations or limited their representations due to power imbalance that wouldn't legally or practically allow the HO to provide them with a lower level of treatment."

177. The Commissioner accepts this Representation. However the section of the Pilot Guidance which deals with data subject representations does not explain this. This means the Home Office is unable to demonstrate that proportionate influence is placed on

the representations (including where limited or no representations are made) in the decision making process.

(b) In accessing the trail data

178. There is limited detail as to when and how decisions to access and use the trail data must be made in the Draft DPIA V2.3, the Pilot Guidance, the Data Access Request Form, the Data Access Guidance or the Process to Access Information. This means that Home Office is unable to demonstrate that this processing of the trail data would be necessary and proportionate for the relevant public functions/tasks.

179. For access to the trail data for the Operational Purposes, there is insufficient assessment in the Draft DPIA V2.3 as to whether and to what extent access to trail data is necessary and proportionate for the purposes of the pilot and so the relevant public functions/tasks. (See paragraphs 132 and 133 above).

180. For access to the trail data for the Non-Operational Purposes, the Home Office could choose to make an assessment of the necessity and proportionality of each particular instance of access by reference to the purpose of the request on a case by case basis at the time of receipt. This could then be demonstrated in its guidance for staff who are deciding to access and use the trail data for those purposes.

181. For both the Operational and Non-Operational Purposes, the, there is little or no guidance in the Pilot Guidance, the Data Access Request Form, the Data Access Guidance or the Process to Access Information for Home Office staff as to how to make the decision to access the trail data.

182. Home Office has stated in its Representations that accessing and using trail data:

> "… is covered in the Process Control Document.
>
> N.B. There were 62 occasions in which trail data was accessed for the purposes of the pilot. 56 of these occasions related to alerts as a result of 'strap tamper' i.e. where the EM device was damaged and rendered inoperable. 6 related to less serious bail breaches e.g. battery depletion."

183. The Process Control Document (which we refer to as the Process to Access Information) sets out the Home Office process for data requests but does not provide guidance to Home Office staff about how to make the decision to access the trail data. The only guidance given is that when triaging the request the staff member:

> "triages it to ensure it meets the necessary data sharing protocols, eg duly authorised, and the request is necessary, justified and proportionate…"

This is not sufficient to demonstrate that access to the trail data is necessary and proportionate for the relevant public functions/tasks.

(ii) FAIRNESS AND TRANSPARENCY: Demonstrating compliance with Articles 12 and 13

184. The Updated Privacy Notice is made up of three documents, namely:

- the STS PIN;

- a privacy notice within the EMS booklet; and
- the departmental privacy notice (the Home Office's high level privacy notice: "Borders, Immigration and Citizenship: privacy information notice").

185. The Commissioner's assessment is that the Home Office has not demonstrated by its Updated Privacy Notice, that, in compliance with Article 12, all data subjects have been provided with all the information required by Article 13 in a:

> "concise, transparent, intelligible and easily accessible form, using clear and plain language",

This means the Home Office has not demonstrated compliance with Article 5(1)(a) (the principle of 'fairness and transparency').

186. The failures to demonstrate compliance with Article 12 are as follows:

- The Updated Privacy Notice, and in particular the STS PIN, fails to set out the privacy information clearly in one place. This may be a single document with clear links or references to other documents with an explanation as to how each applies and interacts.
- The purpose of processing in the STS PIN remains unclear and is not consistent with the purpose set out within the Draft DPIA V2.3. The STS PIN describes the purpose of processing as follows:

> "From 15 June 2022, the HO is running a pilot to test whether Electronic Monitoring is a better means of maintaining contact with people who have arrived in

the UK via unnecessary and dangerous routes. The HO wants to know if the use of these devices will:

- Help the HO keep in contact with more people while their application is being processed than is currently the case;
- Test out whether the device information can help the HO in regaining contact with individuals when contact is lost;

And as [a] result this may enable the HO to process applications quicker".

This does not align with the purposes set out in Draft DPIA V2.3 (see paragraph 35 and 36 above).

- The addition of the reference in STS PIN to processing applications "quicker" is at best confusing for data subjects and at worst could be misleading, as it may lead them to consider that their application will be processed more quickly if they participate in the pilot.
- The STS PIN sets out how and when trail data is accessed:

"It is not anticipated that GPS trail data will be needed other than in very exceptional circumstances and the Home Office will always consider whether to do so is necessary and proportionate before making a request to see the data."

There is no explanation or guidance on what the "very exceptional circumstances" may include.

- The term "GPS Trail data" is not defined or explained and this gap in the STS PIN is likely to inhibit understanding.

- The three documents forming the Updated Privacy Notice are not sufficiently integrated; there are inconsistencies and information gaps. For example, the Electronic Monitoring Handbook states the controller to be the Ministry of Justice.

- The information in the STS PIN provided on special category data is not clear. It states that:

> "This project will be using special category data that concerns a person's health when considering whether a GPS tag is suitable for each individual. No other special category data is used for this project. However, the Home Office does collect and use data that identifies an individual's nationality and has decided that this information will be given the same level of protection as that of special category data to protect the individual. Where geographic location is collected, this purpose will not be used to identify special category data. Geolocation is only used for the purposes outlined in your EM booklet to maintain contact with you."

This is confusing and it would be unclear to a data subject what this meant for them. It is not clear if information about a person's health and nationality are processed only as a result of the pilot, or if this is personal data which the Home Office would process in any event.

In addition, this does not accurately reflect the fact that special category data may be processed when the trail data is accessed, depending on the data subjects movements (see Paragraphs 95-101 above). This should be clearly explained to data subjects.

- The STS PIN refers to GPS coordinates, trail data, geographic location and geolocation. It is not clear if these are different types of data or different ways of referring to the same data.

187. The Commissioner has reviewed the improvements to the privacy information made by the Home Office in response to previous recommendations made by the Commissioner. However, the Commissioner's view remains that the Updated Privacy Notice, and in particular the STS PIN, still does not demonstrate compliance with the requirements of Article 12, and this means that compliance with the requirements of Article 13 has not been effectively provided.

188. The Commissioner welcomes the explanation from the Home Office in its Representations that its Home Office staff explained orally to data subjects how their data will be used. However:

- There is still a requirement in Article 12 for the information referred to in Article 13 to be provided in writing or other means such as electronic means. The information must be provided in a concise, transparent, intelligible and easily accessible form using clear and plain language. It can be provided orally if requested by the data subject.

- In any event, this oral explanation cannot be taken into account regarding Article 5(2) and demonstrating compliance with the transparency principle and Articles 12 and 13, as how this was done by Home Office staff was not set out in any detail in Draft DPIA V2.3 and/or Pilot Guidance and/or in the Updated Privacy Notice.

(iii) DATA MINIMISATION: Demonstrating compliance with Article 5(1)(c)

189. The Commissioner's assessment is that the Home Office has failed to demonstrate its compliance with Article 5(1)(c), and so is in breach of Article 5(2), for the reasons set out below.

190. This finding is further to the lack of detailed guidance available to Home Office staff when deciding whether or not to access trail data and use trail data in making decisions (see paragraphs 178-183 above).

191. The Draft DPIA V2.3 fails to expressly apply the principle of data minimisation to the occasions when the Home Office may access the trail data (for its own or a third party's purposes) and how much of the trail data to request access to. For example, there is no reference to the importance of limiting the time period for which access is requested.

192. Similarly, the Data Access Request Form, the Data Access Guidance and Process to Access Information fail to give Home Office staff any guidance on how to consider and apply the principle of data minimisation when requesting access to the trail data. For example, the Data Access Guidance does not advise Home Office staff to consider whether to make the request at all (in circumstances where, for a minor breach, the first step could

be to contact the data subject), or to only make a request for specific data and for a limited time period where required.

PART V: DECISION TO ISSUE THIS ENFORCEMENT NOTICE

193. The Commissioner requires the Home Office to take the steps set out in Annex 1. The Commissioner considers these are appropriate and proportionate steps for the purpose of remedying the failures identified by the Commissioner in this EN.

Legal Framework – Enforcement Notices

194. Under section 149(6) DPA, an enforcement notice given in reliance on section 149(2) DPA may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failures identified by the Commissioner.

195. Pursuant to section 150(1) DPA, "an enforcement notice must state what the person has failed or is failing to do, and give the Commissioner's reasons for reaching that opinion."

196. When considering whether to issue an enforcement notice in reliance on section 149(2) DPA, the Commissioner must, in accordance with section 150(2) DPA:

> "consider whether the failure has caused, or is likely to cause any person damage or distress."

197. Where an enforcement notice is issued in reliance on section 149(2) DPA, section 150(3) DPA makes it clear that:

> "the Commissioner's power under section 149(1)(b) to require a person to refrain from taking specified steps includes the power:

a) to impose a ban relating to all processing of personal data, or

b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following:

(i) a description of personal data;

(ii) the purpose or manner of the processing;

(iii) the time when the processing takes place."

198. Pursuant to section 150(4):

"an enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with."

Matters the Commissioner has had regard to:

199. The Commissioner has made an assessment (as required in accordance with section 150(2) DPA when deciding whether to serve an enforcement notice) of whether any contravention has caused or is likely to cause any person damage or distress. The Commissioner's view is that, based on the current versions of the Draft DPIA V2.3, the Pilot Guidance, Data Access Request Form, the Data Access Guidance and Process to Access Information, and Updated Privacy Notice, for at least some data subjects, damage and/or distress is likely to have been caused and there is a significant risk that damage and/or distress may be caused in future.

200. This is because (inter alia):

- the infringements which the Commissioner has identified could have had, and could have, important consequences for those data subjects who were electronically tagged, in particular as the data subjects were in a situation which was likely to make at least some of them vulnerable;

- the failure by the Home Office to adequately assess (in Draft DPIA V2.3) and give guidance to its staff on how to make the assessment of the necessity and proportionality of the processing for the purpose of the pilot meant there was no assurance for any data subject that electronic monitoring as an immigration bail condition was a fair and balanced measure, assessed alongside alternatives. Some data subjects may have been tagged when it was not necessary and proportionate;

- the Commissioner has not seen adequate evidence of safeguards against the risks to data subjects associated with electronic monitoring as an immigration bail condition. For those being monitored, for example, this could have included psychological harm for example due to actual or perceived stigmatisation and a perceived need to inhibit movement;

- data subjects may not have expected their data to be processed in the way that the Home Office is processing it, and may not expect their data to be processed in the way the Home Office and third parties may process it in future (as they have not been given an effective privacy notice); and/or

- some or all of a data subject's trail data may have been accessed when it was not necessary and proportionate for the purpose of the pilot (or for one of the Non-Operational Purposes), and may be accessed when it is not necessary and proportionate for one of the Non-Operational Purposes. In addition more trail data than is needed may have been, or may be accessed.

201. The Commissioner's assessment is that compliance with the UK GDPR provisions referred to above is a matter of importance to data protection law. Even if a failure to comply has not caused, or is not likely to cause, any person damage or distress, the issue of this enforcement notice to compel compliance would nonetheless be an appropriate exercise of the Commissioner's enforcement powers.

202. The Commissioner considers that the failures set out in this EN are important for compliance with UK GDPR by the Home Office more broadly than just this pilot. The Commissioner is concerned that failures here could be repeated by Home Office for other operations. In particular the Home Office's failure to:

- document in enough detail each processing activity for the purpose of a DPIA, including the nature, scope, context and purposes;

- carry out an assessment of necessity and proportionality for each processing activity;

- carry out a risk assessment of the risks to the rights and freedoms of data subjects for the purpose of a DPIA

- identify vulnerability in data subjects

- provide a privacy notice "in a concise, transparent, intelligible and easily accessible form, using clear and plain language", which takes into account the nature of data subject including any vulnerabilities

- provide detailed guidance to staff who need to apply key legal constructs such as applying the necessity and proportionality test, the principle of data minimisation, or applying rights under the Human Rights Act.

203. The Commissioner has taken into consideration the Representations, including the fact that the pilot has ended, including all electronic monitoring under the pilot, and no new trail data is being collected. The ongoing processing of pilot personal data is in the retention of the pilot personal data including trail data, and potential access and use of the trail data by Home Office staff and potential disclosure to the data subject and third parties of the trail data.

204. In June 2022, the Commissioner set out a revised approach to public sector enforcement to be trialled over two years.[11] To support this approach, the Commissioner committed to working proactively with senior leaders in the public sector to encourage compliance, prevent harms before they occur, and learn lessons when things have gone wrong. In practice, this means that for the public sector the Commissioner has committed to increasing the use of public reprimands and enforcement notices, only issuing fines in the most egregious cases.[12]

[11] Open letter from UK Information Commissioner John Edwards to public authorities, 30 June 2022.
[12] See ICO25 – Our Regulatory Approach, 7 November 2022, p.7.

205. The Commissioner has had regard to the revised public sector approach in reaching the decision to issue this EN. The

Commissioner is satisfied that this case is one which meets the criteria for formal enforcement action, to reflect the seriousness of the infringement and the significant risk to data subjects.

206. The Commissioner has had regard to the desirability of promoting economic growth, and the potential impact this enforcement notice might have in this regard.

Decision to issue this Enforcement Notice

207. Having had regard to those matters set out in paragraphs 199-206 above, and the nature of the infringements, the vulnerable nature of some data subjects, the scale of the personal data being processed and the context in which it is processed, the Commissioner's view is that this EN is an appropriate regulatory step to remedy the failures identified in this EN.

PART VI: APPEAL

208. The Home Office is entitled to appeal against this EN to the First-tier Tribunal (Information Rights) by virtue of Section 162(1)(c) DPA. If an appeal is brought against this EN, the EN need not be complied with pending determination or withdrawal of that appeal.

209. Information about the appeals process may be obtained from:

General Regulatory Chamber
HM Courts & Tribunals Service
PO Box 9300
Leicester Lel 8DJ

Telephone: 0203 936 8963

Email: grc@justice.gov.uk 85.

210. Any Notice of Appeal should be served on the First-tier Tribunal within 28 calendar days of the date on which this EN is sent.

Dated: 28 February 2024

John Edwards
Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

TERMS OF THE ENFORCEMENT NOTICE

Within 28 days of the date of this Enforcement Notice, the Home Office must provide to the Commissioner the following documents:

1 Updated versions of the Data Access Request Form, the Data Access Request Guidance and the Process Control Document which meet the requirements of Article 5(2) to demonstrate compliance with the Article 5(1)(a) principle of lawfulness and Article 5(1)(c) principle of data minimisation, when Home Office staff access, use and disclose trail data.

2 An updated version of the STS PIN which meets the requirements of Article 5(2) to demonstrate compliance with the Article 5(1)(a) principle of fairness and transparency and which meets all the requirements of Articles 12 and 13 ("Revised Privacy Notice"). This Revised Privacy Notice must cover the past, current and potential future processing of the pilot personal data by the Home Office.

3 Documentation of the process to provide the Revised Privacy Notice to all data subjects whose trail data is retained by the Home Office, in accordance with Article 12. This must include how this Revised Privacy Notice will be provided to data subjects with limited understanding of English.