SUBMISSIONS TO THE INFORMATION COMMISSIONER'S OFFICE

–

REQUEST FOR ASSESSMENT OF PROCESSING OPERATIONS BY THE SECRETARY OF STATE FOR THE HOME DEPARTMENT ("HOME OFFICE")

Contents

I. Introduction and Purpose of this Submission

1. Privacy International ("PI") is a non-profit, non-governmental organisation based in London, that works globally at the intersection of modern technologies and rights. Established in 1990, PI undertakes research, litigation and advocacy to build a better future where technologies, laws and policies contain modern safeguards to protect people and their data from exploitation. As such, PI has objectives which are in the public interest and is active in the field of the protection of data subjects' rights and freedoms. This submission relates to PI's ongoing work on the protection of migrant communities and of their data. See Annex I for more information on PI's work in the migration context.

2. Through this submission, PI raises concerns about the policy and practice of the Secretary of State for the Home Department (thereafter "HO") of collecting and processing of data using two algorithms across immigration enforcement operations.

3. The Identify and Prioritise Immigration Cases ("IPIC") tool is used on individuals who are subject to immigration control and who are therefore liable for detention and removal pursuant to the Immigration Act 1971 and subsequent legislation. The tool generates automated recommendations and prioritises casework for immigration enforcement purposes. The recommendations are generated via various '**business rules'**. They relate to decisions to detain and remove migrants without immigration status as well as to deny them access to services and benefits and to target certain groups, such as individuals who have been refused status under the EU Settlement Scheme ("EUSS"), with enforcement action.[1]

4. The Electronic Monitoring Review Tool ("EMRT") has been developed with similar functionalities as IPIC. It generates recommendations that relate to the use of GPS tracking as a condition of immigration bail pursuant to paragraph 4 of Schedule 10 to the Immigration Act 2016. The tool is used in the context of quarterly Electronic Monitoring ("EM") reviews carried out by the HO to decide if GPS tracking remains appropriate. It determines **first**, via an automated harm score, the minimum period an individual will remain subject to an ankle tag after which they *may* be 'transitioned' to a non-fitted device ("NFD"). NFDs constitute a distinct means of 24/7 GPS tracking. They are handheld devices equipped with a fingerprint scanner that requires the subject to submit biometric information several times a day. **Second**, it generates automated recommendations as regards whether an individual should remain subject to an ankle tag or be transitioned to an NFD.

[1] See PI's analysis on algorithms in immigration decision-making, PI, 'Automating the hostile environment: uncovering a secretive Home Office algorithm at the heart of immigration decision-making' (17 October 2024), https://privacyinternational.org/news-analysis/5452/automating-hostile-environment-uncovering-secretive-home-office-algorithm-heart

5. We provide the Information Commissioner's Office ("ICO") with technical evidence and legal analysis in order to assist him in assessing the data controller's compliance with data protection legislation, in particular the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") and the Data Protection Act 2018 (the "DPA 2018").

6. The evidence includes substantial disclosures regarding both IPIC and the EMRT obtained via requests submitted under the Freedom of Information Act 2000 ("FOIA") by PI and multiple other organisations.

7. We have reviewed the responses and documentation provided in response to these FOIA requests, which includes business rules documents, case worker guidance and data protection compliance documentation. We have discovered that the EMRT and IPIC tools have both been used in the large-scale processing of migrants' personal data, including special category data, as part of the HO's immigration enforcement actions under various business rules. Their use appears to often have limited human involvement, a situation which is catalysed by the unclear and inconsistent guidance provided to case workers and 'design nudges' which encourage accepting EMRT/ IPIC tool recommendations with little scrutiny. The evidence within the FOIA response documentation also reveals a concerning lack of consideration of the data protection impacts of the tools or the provision of privacy information to affected data subjects to allow them to understand how their data is being processed or object to their data being processed in this way.

8. We make this submission to challenge the HO's current practices as regards how they use both these tools in a systemic way, rather than by representing individual data subjects. This is because individual complaints would only challenge the use of either tool in relation to an individual complainant, which may engage more limited data protection rights principles, whereas PI considers that the deployments of both tools deserve holistic investigation and challenge.

9. We note that the use of automated tools to assist or replace human decision-making (hereinafter referred to as 'automated recommendation-making tools, "AMRTs") have grown considerably across the public sector.[2] The HO, which announced its plan to become 'digital by design' in 2021 sees ARMTs as an innovative means to clear immigration backlogs.[3]

10. While ARMTs have a potential to reduce departmental pressures, improve efficiency and accuracy and reduce costs, they are routinely being developed and operated behind closed doors without minimum transparency, explainability and due process safeguards. In the UK

[2] Katie Schwarzmann, ' The Computer Says So: Automated Recommendation-Making Tools in Immigration Systems - A comparative analysis between Canada, the USA and the UK' (10 November 2024), page 9, https://media.churchillfellowship.org/documents/Schwarzmann_K_Report_2023_Final.pdf

[3] Ibid.

context, such decision-making systems were described by a former UN Special Rapporteur on extreme poverty and human rights as existing in "a human rights-free zone".[4]

11. Our investigation in relation to IPIC and the EMRT demonstrates that these failings are built into the functioning and deployment of both tools. They are highly intrusive insofar as the data they process (referred to hereinafter as the "input data") could span the entirety of the information an individual provides to the HO. This includes substantial highly sensitive information such as details relating to an individual's health and vulnerabilities, data relating to their family and other relationships, information related to past periods of detention and even data collected using other surveillance technologies such as GPS tracking.

12. Moreover, individuals are denied any meaningful information about how their data is used. Where information is provided it is inconsistent and contradictory. No information is provided concerning what information the tools process and how it is used, including what consequences its deployment could have on individual data subjects.

13. The in-built opacity of both ARMTs is notwithstanding the significant scale of the processing in question. For example, between 22 May 2023 and 14 August 2023 (during which time the HO has stated that it used the EMRT in all cases[5]) – the HO has stated that it carried out 1,768 quarterly EM reviews.[6] Given that IPIC includes a significant number of distinct business rules, it is likely that both ARMTs have been used in relation to 10,000s of data subjects.

14. The potential harms arising from tools used across the immigration system at such scale include the potential for vulnerable individuals to be subjected to lifechanging decisions. This may include detention or removal from the UK based on profiling and automated decision making ("ADM") without the possibility of verifying the lawfulness and accuracy of the processing and by extension to challenge it.

15. For the reasons set out below, PI submits that the Home Office's current uses of both ARMTs breaches the UK GDPR and DPA 2018 in a number of ways. In summary:

    a. No transparency (and/or inadequate information) is provided to data subjects as to the nature and extent of data collection and processing.
    b. There is an absence of a clear, accessible and foreseeable legal basis authorising the processing in violation of the lawfulness principle.

[4] UN Special Rapporteur on extreme poverty and human rights, Report of the Special Rapporteur on extreme poverty and human rights, A/74/493, (11 October 2019), https://docs.un.org/en/A/74/493

[5] WhatDoTheyKnow, Response to Mia Leslie request to Home Office, (5 April 2023), https://www.whatdotheyknow.com/request/electronic_monitoring_review_too/response/2281853/attach/3/75193%20Leslie.pdf?cookie_passthrough=1

[6] WhatDoTheyKnow, Response to Joe Haynes request to Home Office, (19 September 2022), https://www.whatdotheyknow.com/request/reviews_of_decisions_to_impose_g/response/2422269/attach/3/78221%20Hynes.pdf?cookie_passthrough=1

c. The processing does not comply with the fairness principle and in particular falls outside the reasonable expectations of data subjects.
d. The extent of data collected and the uses of the ARMTs does not comply with the principles of necessity and proportionality.
e. The re-purposing of input datasets to generate automated recommendations is incompatible with the purpose limitation principle.
f. The retention of certain data is unjustified and in breach of the storage limitation principle.
g. The HO has failed to carry out a lawful Data Protection Impact Assessment ("DPIA") and/or undertake a DPIA at all in case of the EMRT. It has also failed to demonstrate compliance with the data protection principles pursuant to the accountability principle.
h. The human review processes implemented by the HO are inadequate as they may in certain cases be carrying out solely ADM in breach of Article 22(1) of the GPDR.

16. The submission will first summarise the evidence we have obtained, explain how both ARMTs function, address the HO's claims regarding the nature of the processing and finally set out in detail the legal framework and concerns identified.

II. <u>Summary of the evidence</u>

The Freedom of Information Act correspondence – IPIC

17. The first reference we have been able to identify to the IPIC algorithm used by the Home Office is in an Independent Chief Inspector of Borders and Immigration ("ICIBI") 2021 report on the HO's use of sanctions and penalties.[7] The 2021 report described IPIC as "triage tools" used to assess the removability and level of harm posed by immigration offenders, automate the identification and prioritisation of cases, and to provide information on the length of time a barrier to removal has been in place".

Public Law Project - Freedom of Information Request

18. In November 2021, the Public Law Project submitted a FOIA request to the HO asking for confirmation regarding use of the tool, any Equality Impact Assessments ("EIAs") and DPIAs, other reports/audits completed in relation to the tool as well as any training materials.[8]

[7] Independent Chief Inspector of Borders and Immigration (ICIBI), 'An inspection of the Home Office's use of sanctions and penalties', (November 2010 – October 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951438/An_inspection_of_the_Home_Office_s_use_of_sanctions_and_penalties__November_2019___October_2020_.pdf

[8] WhatDoTheyKnow, Response to Tatiana Kazim request to Home Office, (21 March 2022), https://www.whatdotheyknow.com/request/triage_tools_used_in_an_immigrat#incoming-2002033

19. Through this request they received a heavily redacted version of the DPIA, a redacted EIA and a redacted copy of the executive summary and background context from the then most recent evaluation of IPIC. Everything else (including the training materials) was refused based on the immigration exemption within FOIA. Some of these materials are significant and their role is addressed in detail below.

Privacy International - Freedom of Information Request

20. On 18 October 2023, PI submitted a FOIA request to the HO asking for updated versions of the DPIA, confirmation whether IPIC was developed internally (or by an external supplier), confirmation whether IPIC is used in relation to several immigration processes (such as applications for leave to remain/immigration bail conditions), the information provided to caseworkers when IPIC makes a particular recommendation, the frequency and nature of ongoing reviews and testing of the algorithm mentioned in the DPIA disclosed to Public Law Project, the training materials and confirmation regarding the "analytical purposes" for which personal data can be used (also referred to in the previous DPIA).[9]

21. We received a response from the HO on 3 November 2023 with the following:

    a. **DPIA**: A heavily redacted version of an updated DPIA completed on 17 March 2023.
    b. **Internal and external supplier:** Confirmation that the IPIC algorithm is developed internally (i.e. no external supplier).[10]
    c. **Immigration processes the tool is used in:** A denial that IPIC is used in relation to "applications for entry clearance and leave to remain under the immigration rules; decisions to impose removal directions, grant immigration bail or what bail conditions someone without immigration status should be subject to." No information was given about how it is used (i.e. what the recommendations are and what decisions the tool is used in relation to).

[9] WhatDoTheyKnow, Privacy International request to Home Office, (18 October 2023), https://www.whatdotheyknow.com/request/identify_and_prioritise_immigrat_3

[10] This is notwithstanding the HO signing a contract with the private company, BJSS on 1 April 2021 (until 31 March 2022) for the expansion of IPIC to provide for fresh uses of the tool. See, Sam Trendall, 'Home Office signs £8.5m deal to expand use of immigration casework prioritisation tool', Public Technology (17 April 2023) https://www.publictechnology.net/2023/04/17/business-and-industry/home-office-signs-8-5m-deal-to-expand-use-of-immigration-casework-prioritisation-tool/ . The contract refers to BJSS providing a number of services including the designing, building and "implementation of applications into a Cloud environment". See, Crown Commercial Service, 'G-Clidu 12 Call-Off Contract', https://atamis-8888.my.salesforce.com/sfc/p/#58000000L5A4/a/4I000001R4f7/NgeVcCAOj0yf9wByKMwmrU5XF4nGsS432.MiIL4aezQ . It refers to deliverables including "developing configurable technology modules tailored to a specific business service need: automating existing manual, paper-based processes; and supporting decision-making to drive consistency." It is unclear if there have been other contracts with other companies pertaining to the roll out of IPIC since the expiry of the above agreement.

d. **Information provided to caseworkers when a recommendation is made**: A refusal to provide the information provided to caseworkers when IPIC makes a recommendation under the immigration exemption on the grounds that “the information you requested could be used to circumvent immigration controls by providing an insight into how work in the Home Office and Immigration Enforcement is triaged.”

e. **Reviews and testing of IPIC**: Confirmation that IPIC and associated data are “assured on an annual basis”. The data tested was said to be a random “sample of data from a feature or business rule.”[11] No further information was provided on what the nature of the testing is, what personal data is used and how this is selected. The HO noted that IPIC’s outputs are recommendations only and that they are subject to human review.

f. **Training materials**: A refusal to provide these based on the immigration exemption under FOIA given that disclosing them could purportedly give migrants insights as to how work within the HO is triaged.

g. **Analytical purposes**: confirmation that the analytical purposes are “to drive improvements to workflow and inform policy and guidance”. Personal data is not anonymized for this purpose, but only biographical data said to be processed.

The internal review and response

22. We challenged this response by way of an internal review on 19 December 2023 as follows[12]:

a. **DPIA**: We noted that the heavily redacted updated version of the DPIA did not disclose the categories of personal data that are processed through the tool; the explanation as to how the tool will be able to meet data subject rights; the explanation as to the purpose of processing; and an explanation as to the legal and other significant effects that the profiling undertaken through the tool could have on the data subjects. We submitted that the HO had not demonstrated how the prejudice would arise and how this is likely to occur through disclosure.

b. **Immigration processes the tool is used in:** We argued that it was clear that the tool is being used in relation to the relevant immigration processes as per the reference in the ICIBI report above (§17).

c. **Information provided to caseworkers when a recommendation is made**: We made similar arguments as in relation to the redacted version of the DPIA.

d. **Training materials**: We again submitted that the public interest test for the application of the immigration exemption had been carried out erroneously.

e. **Analytical purposes**: We referred to the data protection principles and noted that a purpose must be “specified and explicit”. We therefore argued that the description of

[11] “Business rule” is the name given to a particular use of the algorithm (and the associated logic for that use case). The different business rules that form part of IPIC are addressed below.

[12] WhatDoTheyKnow, ‘Privacy International Request to Home Office’, (18 October 2023), https://www.whatdotheyknow.com/request/identify_and_prioritise_immigrat_3

the purpose did not meet these criteria, and the HO would need to disclose which guidance and workflows it was seeking to improve.

23. We received a response to the internal review request on 20 March 2024, which involved a revised public interest test relating to the application of the immigration exemption. With respect to the DPIA, training materials and information displayed to caseworkers when the tool makes a particular recommendation – the HO argued that disclosure would enable migrants to game the system so that it would not prioritise them for the relevant interventions. As such, no further information was provided in relation to any of these. The response erroneously argued that we were requesting fully unredacted versions of the above documents. The response also continued to deny that IPIC was used in relation to the immigration processes that we specified.

The ICO FOIA complaint

24. As far as is material to the data protection complaint, we submitted the FOIA complaint to the ICO on 1 May 2024 challenging a number of the redactions to the updated DPIA (set out above), the failure to provide confirmation as regards whether the tool was used in relation to the above immigration processes, the information provided to caseworkers when a recommendation is made and the training materials. The complaint made further submissions on why there was no evidence that the information would enable migrants to game the system in the stated way (with reference to expert literature on this issue). We also argued that the HO could not have it both ways and argue that IPIC isn't being used in relation to the above immigration processes while also stating that the tool could be gamed to avoid certain enforcement outcomes that relate to the same processes.

25. In response to the complaint, the HO provided us with redacted versions of the training materials on 1 October 2024. They also disclosed a version of the DPIA with fewer redactions at the same time. In particular, the full input data were provided. Critically, the DPIA continued to redact much of the section of the DPIA dealing with whether IPIC constitutes profiling that could result in an outcome that produces legal effects or similarly significant effects on individuals.

26. Thereafter, we engaged with further correspondence with the ICO, which sought comments from both us and the HO around any outstanding matters. In particular, we argued that the HO had failed in its duty under Section 1 of the FOIA to either confirm or deny information in relation to the ongoing failure to clarify the position as regards which immigration processes the tool is used in relation to. In support of this we cited several references to particular immigration processes in the newly disclosed training materials (see more on this below). We also maintained our challenge to specific redactions in the DPIA on the basis that they were unjustified. We also sought to challenge the failure to justify the application of the immigration exemption in relation to the above redaction in the DPIA (re profiling and legal or other significant effects).

27. The HO continued to maintain that our request required disclosure of the full DPIA and training records and to do so would enable migrants to make "spurious claims" and thereby prompt the algorithm to generate a "low priority" recommendation.

The ICO's decision notice

28. The ICO published a decision notice dealing with the outstanding issues on 11 November 2024 (namely the disclosure of the exact recommendations and decisions and outstanding redactions in the DPIA).[13] As far as is material for the purposes of the data protection complaint the notice noted as follows:

    a. That additional information was provided to the ICO by the HO, which maintained that: "*a business rule includes or excludes certain conditions to produce a recommendation as to what the next immigration action to be considered could be. The business rule will apply the widest possible pool of records, and these can then be further refined by managers based on operational demands or priorities. The results are returned in a prioritised order*."[14]
    b. The HO's denial that IPIC involves ADM or profiling.[15]
    c. The HO sought to compare our FOIA complaint to a similar complaint submitted in relation to an algorithm used to detect fraudulent marriages (the "sham marriage algorithm").[16]

29. The ICO found that:
    a. "... *IPIC is not an automated decision-making tool, it is not trained, and no profiling is used*." No explanation was given in support of this finding.
    b. The tool generates recommendations only – although there was no comment on the nature and scope of the human review the HO says is built into the system.
    c. "… *Although the complainant considers that parts of the disclosed training guide indicate a broader application, the Commissioner does not agree. The Home Office has repeatedly explained that IPIC is an automated tool which does not provide recommendations as to whether a person's application*

[13] ICO, 'Freedom of Information Act 2000 (FOIA) Decision Notice', (11 November 2024), https://ico.org.uk/media2/migrated/decision-notices/4031833/ic-304527-q0f2.pdf

[14] We address this in further detail below.

[15] This is notwithstanding the HO accepting in the DPIA that IPIC does involve profiling. The HO maintained that "IPIC provides recommendations only, and Home Office staff are encouraged to reject the recommendation where they deem the action is not appropriate." The HO also noted that "accepting a recommendation in IPIC does not mean that the action will take place, as members of staff still need to add this to core case working systems for it to happen; this is also evident in the redacted user guides." We deal with this in detail below.

[16] The marriage sham algorithm was withdrawn following pre-action correspondence by Public Law Project, which alleged that it did constitute automated profiling. The tool has since been replaced by a different algorithm.

should be granted or refused, or whether a person should be granted or refused bail. IPIC merely provides recommendations in respect of which case should be prioritised by a caseworker for action, to progress that case towards some form of conclusion."

d. Prejudice to the operation of immigration controls was made out and the causal connection between the disclosure and the prejudice was also established (based on the 'would be likely to' prejudice threshold). This was based partly on confidential information provided by the HO to the ICO, which the decision maker stated would itself prejudice immigration control if published. The ICO noted that release of the information under FOIA would entail disclosure to the world at large.

e. **Crucially, the ICO distinguished between its findings under FOIA and the application of the UK GDPR to IPIC**: "*The Commissioner notes that these arguments focus primarily on what the complainant sees as potential breaches of the UK GDPR and individuals' rights rather than being directly relevant to the exemption*."[17]

30. Further explanation of how the ICO's decision notice findings fit into the context of our claims around the application of the UK GDPR and DPA 2018 to IPIC within this submission are addressed within §184 – 192, below.

Evidence from Duncan Lewis Solicitors

31. In December 2024, Duncan Lewis Solicitors conducted an analysis of the use of the IPIC tool by reviewing the subject access request bundles that they have received from the Home Office in relation to their clients who have instructed them in their immigration matters. [*redacted]*[18]

32. In the subject access request bundle received from the Home Office, the term IPIC was found in the following quotes:

[*redacted]*

The Freedom of Information Act correspondence – the Electronic Monitoring Review Tool ("EMRT")

Public Law Project - Freedom of Information Request 1

33. The EMRT is an automated support tool that makes recommendations relating to the mandatory reviews the HO must carry out regarding the ongoing appropriateness of GPS tracking as an immigration bail condition (the nature of its recommendations is addressed in

[17] Our arguments around potential GDPR breaches related to the public interest in favour of disclosure.

[18] Annex IV, Duncan Lewis Solicitors Analysis of Home Office Subject Access Bundles.

detail below). Its existence was first disclosed to Public Law Project following a request filed in November 2022.[19] It is noted that a previous version of the Immigration Bail policy (the "Bail Policy") dated 30 August 2022 referred at page 47 to "a decision support tool which utilises automated business rules to provide decision recommendations for the decision maker to consider alongside the guidance set out in Use of EM and EM and linked supplementary conditions: Review".[20] Notably, the current version of the Immigration Bail policy (dated January 2025) continues to refer to the possibility of using an automated support tool. This is addressed in further detail below.

34. In their response to Public Law Project's FOIA request dated 11 November 2022, the HO confirmed that the EMRT is not currently part of IPIC, but that it was the department's intention for "IPIC… to eventually be the decision support tool available to Electronic Monitoring ("EM") decision makers." The EMRT was described by the HO as "an interim non-IPIC solution", which the HO had decided to develop and test. It was said that the tool utilises the same core principles as IPIC. The HO also stated that the EMRT's functionality was aligned with IPIC.

35. In response to Public Law Project's request for disclosure of any EIAs and DPIAs – the HO referred Public Law Project to the assessments completed for IPIC indicating that no discrete assessments were conducted in relation to the roll out and deployment of the EMRT. The HO refused to provide training guides requested by Public Law Project.

Public Law Project - Freedom of Information Request 2

36. Public Law Project filed a further FOIA request in March 2023. In the HO's response dated 5 April 2023, the HO clarified the differences and similarities between the EMRT and IPIC: "The EMRT does not contain all of the data points that IPIC will, and caseworkers are required to add this data manually".[21] IPIC is still being developed to contain all data points needed. Additionally, the EMRT auto-populates information in the review outcome form. Both tools utilise Home Office data, apply the principles set out in the Immigration Bail guidance and generate a decision recommendation for the caseworker to consider."

37. The HO also explained that the transfer to IPIC would take place once the "development of IPIC's EM module has been completed" and following a period of "testing, training and user familiarisation". The HO provided that there would be period where both tools would be run

[19] WhatDoTheyKnow, 'Response to Mia Leslie request to Home Office', (20 December 2022), https://www.whatdotheyknow.com/request/immigration_bail_electronic_moni#incoming-2198042

[20] Home Office, 'Immigration bail version 13.0', (30 August 2022), https://webarchive.nationalarchives.gov.uk/ukgwa/20221005205040/https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1102889/Immigration_bail_September_2022.pdf

[21] WhatDoTheyKnow, 'Response to Mia Leslie request to Home Office', (5 April 2023), https://www.whatdotheyknow.com/request/electronic_monitoring_review_too

at the same time and that a decision would then be made regarding a move to solely using IPIC.

38. The HO refused to provide access to the training materials on the basis of the Immigration Exemption under FOIA. It did however confirm that the EMRT was first used to provide recommendations from 7 November 2022.

Public Law Project - Freedom of Information Request 3

39. Public Law Project filed a further FOIA request in September 2023.[22] In their request they sought clarification on the reference to a "harm score" in a previous version of the Bail Policy, which was said to "relate to the score used within the decision support tool". In its response dated 2 October 2023, the HO refused to provide the information on the basis of the Immigration Exemption.

Duncan Lewis Solicitors - Freedom of Information Request

40. In March 2024, Duncan Lewis Solicitors filed a FOIA request seeking information relating to a number of issues pertaining to the HO's use of GPS tracking, including the training materials for the deployment of the EMRT. [23]

41. Disclosure of redacted training materials was provided with a response dated 23 April 2024. However, in its response the HO stated that: "no decision support tool is in use at present and reviews are conducted manually." We note that this request was submitted by email and both the request, and the disclosure received are not available online via the digital platform, 'What Do They Know'. As such, we have been authorised to provide copies of these documents in full together with these submissions.

Privacy International - Freedom of Information Request

42. In July 2024, we filed our own FOIA request in which we noted the mismatch between the responses received by Duncan Lewis Solicitors and Public Law Project and we sought clarification on the continuing use of the EMRT.[24]

[22] WhatDoTheyKnow, 'Mia Leslie request to Home Office', (5 September 2023), https://www.whatdotheyknow.com/request/electronic_monitoring_review_too_2?utm_campaign=alaveteli-experiments-87&utm_content=sidebar_similar_requests&utm_medium=link&utm_source=whatdotheyknow

[23] Annex XXI - Duncan Lewis FOIA Request (4 March 2024), Redacted.

[24] WhatDoTheyKnow, 'Privacy International request to Home Office', (27 July 2024), https://www.whatdotheyknow.com/request/clarification_regarding_uses_of

43. In a response dated 9 September 2024, the HO maintained that it was not currently using the EMRT and that the tool was **discontinued** in August 2023 because of insufficient evidence regarding efficiencies generated by the algorithm. The HO stated that it was not using any alternative tool (we had sought clarification on whether IPIC was now being used).

Evidence received from Wilson Solicitors

44. As is explored below (§129), we received correspondence from Wilson Solicitors ("Wilsons") sent by the HO on 20 May 2024**,** which referred to a recommendation generated by an automated support tool in an individual case.[25] This therefore contradicts the HO's assertion that the tool has been discontinued. A redacted copy of this correspondence has been provided to the ICO as a confidential Annex III to this complaint with authorisation from Wilson Solicitors.

III. <u>General information on features, design and uses of the automated recommendation making tools</u>

IPIC: what is the same across all business rules

45. This section looks at the different versions of the IPIC holistically before addressing each use in turn in detail below. As above, the HO refers to different uses of the IPIC tool as business rules. Each business rule produces different recommendations and may even have different features.

History

46. The DPIA makes clear that IPIC was first piloted in 2016 as the Immigration Enforcement Business Rules Programme. During the pilot three business rules were tested. In October 2018, a live version of the IPIC was tested again with three business rules. Since 2019, other business rules were rolled out (see below for the current uses of the IPIC).

47. The DPIA suggests that specific business rules have themselves been phased in over time with different versions of a certain use of IPIC deployed at different times.

48. The uneven development of the IPIC is likely to account for the fact that several business rules have varying features with many of these themselves introduced at different times (even as this section focuses on commonalities).

[25] Annex III – Home Office Response Letter to Wilson Solicitors Client Transition to NFD -Redacted.

The business rules

49. From the training materials it appears that there are IPIC business rules relating to the following processes[26]:
    a. Returns preparation 2 (i.e. removals from the UK)[27] [28]
    b. Failed EU Settlement Scheme ("EUSS") cases[29]
    c. Digital reporting immigration bail conditions[30]
    d. Reporting and Offender Management ("ROM")[31] [32]
    e. Central Support and Tracing Team ("CSTT")[33] [34]
    f. Interventions and Sanctions Directorate cases ("ISD")[35]

Working groups and the manager/caseworker distinction

50. All versions of the tool appear to work on the basis that recommendations will be assigned to a certain "working group".[36] A working group will correspond to a particular set of immigration enforcement interventions (that in turn correspond to the different business rules set out above). A working group will be set up by a "manager" who chooses the immigration enforcement intervention that the group will focus on. The "manager" will then assign caseworkers to the working group, and they will be charged with examining the recommendation and deciding how to action it.[37] It is clear from the DPIA that caseworkers will only have permission to access the interventions/business rules that are applicable to them.[38]

[26] As addressed in detail below, each business rule may be used in relation to several interventions meaning that it can therefore produce multiple different recommendations.

[27] Annex V: Immigration Enforcement, 'Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Returns Preparation 2 Service Reference Manual – Manager Access', (January 2023).

[28] Annex VI: Immigration Enforcement, 'Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Returns Preparation 2 Service Reference Manual – Caseworker Access', (February 2023).

[29] Annex VII: Immigration Enforcement, 'IE Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – EUSS Cases'.

[30] Annex VIII: 'IPIC Digital Reporting – Manager Training Guide'.

[31] Annex IX: Immigration Enforcement, 'Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – Reporting and Offender Management.

[32] Annex X: 'IPIC – Reporting and Offender Management User Guide', (November 2023).

[33] Annex XI: Immigration Enforcement, 'Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – CSTT (Managers).

[34] Annex XII: Immigration Enforcement, 'Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – CSTT v1.1 (Final).

[35] Annex XIII: Immigration Enforcement, *title and date redacted,* Interventions and Sanctions Directorate Training Guide.

[36] See, for instance, Annex V: Immigration Enforcement, 'Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Returns Preparation 2 Service Reference Manual – Manager Access', (January 2023), pp. 5-14.

[37] Ibid., p. 49, stating: "A 'manager' in IPIC only relates to the level of access that a given user has. It means that the user is able to set up work groups, allocate recommendations, review allocation filters and edit work groups that caseworkers are assigned to."

[38] Annex II: Data Protection Impact Assessment (DPIA), URN 77.19 (Updated), version 1.23, (17 March 2023), §2.8.a.

51. While the manager/caseworker distinction is not supposed to denote seniority, the training materials state that managers will have a specific form of access to the tool to enact the above, which caseworkers do not have.[39]

52. Managers should frequently monitor the group using the "review tab" (i.e. the tab that caseworkers use to navigate through the recommendations) to ensure that the members of a working group have sufficient cases to review.

What happens once a recommendation is generated?

53. All business rules require caseworkers to either "accept" or "reject" a recommendation (some also allow a caseworker to put a recommendation "on hold", which is addressed below). Accepting a recommendation will result in it being actioned whereas if rejected – a caseworker will have to ensure that the case is not ingested into IPIC again for the same recommendation. **Caseworkers will have to input an explanation if they reject a recommendation. The same is not the case if a recommendation is accepted.**

54. Once a recommendation is accepted, rejected or put on hold it will not immediately be actioned, but will rather remain in the review tab for differing periods of time. The periods of time are not the same for every version of the tool, so this is addressed in further detail below.

Reports and search functionality

55. Managers can generate "management information" reports that give them information on all activity undertaken within IPIC within a date range. The reports can be generated for a period of 7 days, weekly, over a month and/or the last 6 months. This can be filtered to look for the recommendations generated by a particular business rule. For example, Management Information reports for failed EUSS cases will provide a breakdown of all EUSS activity on IPIC over a particular period of time.[40]

56. IPIC business rules incorporate a search function that will display actions the person was recommended for, if the recommendation was allocated to a work group and what status the recommendation is (i.e. is it accepted, rejected or on hold) as well as the date the status changed. The recommendation(s) can be searched through the "find someone option" by using an individual's HO reference. It is unclear if this function is limited to certain staff members or if it can be used by anyone within the HO who has access to IPIC.

[39] Supra note 37.

[40] Annex VII: Immigration Enforcement, 'IE Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – EUSS Cases', p. 10.

Input data

57. The DPIA makes clear that the following personal data is processed by the tool[41]:
    a. Name
    b. Date of birth
    c. Gender
    d. Nationality
    e. Travel Document
    f. Immigration references (such as HO reference)
    g. Contact details (phone number, email address, addresses)
    h. Travel details
    i. Immigration case types and outcomes
    j. Detention details
    k. Return details
    l. Case Information Database ("CID") special conditions including markers of potential vulnerability or health markers[42]
    m. Reporting details
    n. Barriers (as in to removal/deportation)
    o. Criminality – including offences and multi-agency public protection arrangements
    p. Associations
    q. EM data

58. As above, the HO have confirmed that this is not machine learning powered algorithm. As such, there is no training data that is used with respect to this algorithm.

59. The DPIA refers to several datasets used to generate IPIC recommendations. These are not input data per se, but rather underpin the logic of the IPIC algorithm. In particular, the DPIA refers repeatedly to the "triage and management" tool ("TRAM"), which is a "structured database" containing "live" cases.[43] This database has 10 filters, which can be used to identify immigration cases for processing. The DPIA suggests that TRAM involves the use of datasets without the IPIC business rules applied to them. It is designed to "enrich HO data based on set criteria to inform triage options" and the IPIC business rules are then applied to data processed through TRAM.[44]

[41] Annex II: Data Protection Impact Assessment (DPIA), URN 77.19 (Updated), version 1.23, (17 March 2023), §2.1.

[42] Case Information Database is the HO's key case-working database, which encompasses key immigration records. Case Information Database uses markers known as "Special Conditions" to denote categories of vulnerability such as "Certified Mental Illness", "Threat of Self Harm" and "Known Suicide Attempt". The significance of these datasets is addressed in further detail below.

[43] Independent Chief Inspector of Borders and Immigration, 'A re-inspection of the Home Office's Reporting and Offender Management processes and of its management of non-detained Foreign National Offenders', (October 2018 – January 2019), https://assets.publishing.service.gov.uk/media/5cd402b6e5274a3fd79d370a/A_re-inspection_of_the_Home_Office_s_Reporting_and_Offender_Management_processes_and_of_its_management_of_non-detained_Foreign_National_Offenders.PDF

[44] Annex II: Data Protection Impact Assessment (DPIA), URN 77.19 (Updated), version 1.23, (17 March 2023), §3.1.

60. In the ICIBI's re-inspection of the Home Office's Reporting and Offender Management processes and of its management of non-detained Foreign National Offenders (October 2018 – January 2019), the use of TRAM was said to enable the Home Office to identify all individuals reporting (as a condition of their immigration bail) on a single spreadsheet thereby making "potentially removable cases easier to identify and prioritise".[45] In other words it acts as a means to structure Home Office data around particular 'populations of interest', which can then have the IPIC interventions applied to them.[46]

61. Access to TRAM data is only available to HO staff who use IPIC business rules. To be granted access to TRAM data users will need to sign a declaration. It is unclear what the contents of this declaration are.[47]

62. There is also reference to the "DEFINE" dataset. The DPIA suggests that this is a mechanism for storing case data in spreadsheets.[48] It is unclear if IPIC is applied to the DEFINE dataset in the same way as TRAM.

Retention of IPIC data

63. The DPIA suggests that from the point that an IPIC recommendation is generated the recommendation itself will be retained for a period of at least 5 years with all other personal data being deleted. This is in order to facilitate IPIC's "memory function" which enables the "navigation of historical cases for review purposes." It appears that this memory function works together with the "search" option outlined above.

64. The DPIA indicated that recommendations may be retained for periods longer than 5 years. There does not appear to be a clear process for determining when a recommendation will be retained for longer and the duration of any further retention. The privacy and retention policies/information are dealt with in detail below.

Security protocols

[45] Ibid.

[46] Immigration Enforcement, Untitled Report, evaluation of IPIC pilot, https://www.whatdotheyknow.com/request/triage_tools_used_in_an_immigrat/response/2002033/attach/5/68562%20Kazim%20Annex%20E%20Evaluation%20Background%20and%20Summary%20Redacted.pdf?cookie_passthrough=1

[47] Annex II: Data Protection Impact Assessment (DPIA), URN 77.19 (Updated), version 1.23, (17 March 2023), §2.8a-2.9.

[48] Ibid., §2.9.

65. In addition to the limiting of access to caseworkers working on particular working groups, there appear to be additional security arrangements in relation to the use of IPIC and the associated datasets/tools outlined above.

66. For DEFINE datasets – the spreadsheets appear to be password protected, whereas TRAM data is stored in a secure HO network.[49] Information is held in secure folders with restricted access or via Sharepoint to named users with varying, controlled access levels depending on business need.

67. IPIC is said to rely on security standards including 'Simple Storage Services' (essentially just cloud storage), encryption of "data at rest", while data in transit uses HTTP. Where aspects of IPIC have been piloted operational acceptance testing ("OAT") has been used.

68. Access to IPIC additionally requires security check ("SC") clearance and accessibility to the system is regularly audited by the "Business Rules team".

The IPIC business rules examined

Specific information on the features, design and uses of the IPIC business rules

69. It is important to note from the outset that our knowledge of the exact nature of the functionalities of the IPIC business rules is uneven. As above, the Home Office has refused to disclose the exact nature of the IPIC recommendations and the decisions for which they have been used. Nevertheless, we have been able to piece together significant information about the nature of the IPIC interventions through information contained in the HO's training materials, publicly available information provided by the HO to the ICIBI in the context of regular inspections carried out by the latter and evidence sent to us by legal representatives.[50] This information is sufficient to particularise the ways in which IPIC and its recommendations are used in a number of immigration enforcement operations.

70. The opacity of the system is an inbuilt, inherent feature of how the tool has been designed and deployed. By way of an example, none of the relevant Home Office policy documents pertaining to enforcement interventions in which IPIC is used refer to the tool. Where limited information has been provided it is often contradictory, inconsistent and potentially misleading.

71. The HO has maintained that the tool is not used in "relation to applications for entry clearance and leave to remain under the immigration rules; decisions to impose removal directions, grant immigration bail or what bail conditions someone without immigration status should

[49] Annex II: Data Protection Impact Assessment (DPIA), URN 77.19 (Updated), version 1.23, (17 March 2023), §2.9.

[50] This includes searches carried out by Duncan Lewis Solicitors [*redacted].* See Annex IV, Duncan Lewis Solicitors Analysis of Home Office Subject Access Bundles.

be subject to". With what we now know about the various business rules, this may be true in the strict sense. It does not appear that IPIC is used to make decisions regarding the above applications and processes (e.g. to grant or refuse leave to remain). But what is clear is that the recommendations are involved in several of the above processes and applications in the broader sense (i.e. to make recommendations with a significant effect on individuals subject to them relating to the exercise of powers such as removal, immigration detention and immigration bail).

72. The HO has also emphasised IPIC's role in workflow and triaging – maintaining that it is used to route cases to immigration enforcement rather than making substantive decisions. What this section demonstrates, however, is that specific business rules often incorporate dual features that simultaneously enable the triaging and prioritising of cases while also generating recommendations for immigration enforcement decision-making. This is supported by the description of the activities carried out by IPIC business rules as described in the contract with BJSS (see fn 10). The contract describes the tool's "high level capabilities" as "recommending interventions", "prioritising interventions", "task management" and "management of reference data".[51] Critically, "interventions" are defined in the contract as: "**a set of tasks that can be performed against a person of interest to facilitate removal from the UK**".[52] Even where specific recommendations are further back in the decision-making sequence – there is a clear causal link between recommendations and substantive decisions. This is because a recommendation that someone is suitable for a particular enforcement intervention leads, in turn, to its implementation, which we address with reference to particular examples below.

Returns preparation 2 business rules

73. This is the use of IPIC that is most opaque due to both the significant redactions within the training materials and the lack of other available information. What is clear is that these business rules are used in relation to the removals process and specifically preparing cases for removal from the UK (as is addressed below, this intersects with a number of other business rules). The returns preparation 2 rules are therefore aligned with the Home Office's Returns Preparation: Caseworker guidance[53] and specifically the policy pertaining to Arranging Removal.[54] This lists the pre-removal steps as follows:

    a. Serving the individual with a Notice of Liability to Remove

[51] Crown Commercial Service, 'G-Cloud 12 Call-Off Contract', https://atamis-8888.my.salesforce.com/sfc/p/#58000000L5A4/a/4I000001R4f7/NgeVcCAOj0yf9wByKMwmrU5XF4nGsS432.MiIL4aezQ

[52] Ibid.

[53] UK Visas and Immigration, 'Guidance, Returns preparation: caseworker guidance', (last updated on 13 May 2024), https://www.gov.uk/government/publications/returns-preparation

[54] Home Office, 'General Instructions: Immigration Returns, Enforcement and Detention, Arranging removal', version 5.0, (20 April 2024), https://assets.publishing.service.gov.uk/media/662b5e2dae7fb5d93ebf9301/Arranging+removal.pdf

b. Ensuring that they do not have any casework barrier to removal (e.g. a pending asylum or human rights claim)
c. Ensuring that the detained individual is fit to fly
d. Obtaining the necessary authorisation to conduct a family separation (where relevant)
e. Obtaining the appropriate level of authorisation for removal
f. Ensuring that the individual holds a valid travel document save for in charter flight cases. The guidance provides that removal directions may be set where an emergency travel document (ETD) is still pending agreement.

74. The redacted version of the EIA disclosed to Public Law Project (see §18 above) refers to the deployment of IPIC (specifically the "filter" components of the tool, which are addressed below) to identify cases that are appropriate for Home Office charter flights.[55]

75. The training materials corresponding to these business rules provide screenshots that show that caseworkers reviewing recommendations generated by the business rules are instructed to look at tabs relating to "person details; documentation; reporting status; barriers; harm; family status; and vulnerability."[56] By clicking on the tab relating to "person details" – a caseworker will be able to see an individual's "name; HO reference; Person ID; Duplicate person ID(s); date of birth; country of nationality; gender; and Red Notice Status." It is unclear from the relevant training materials what the data contained in the other tabs includes. The training materials also provide that caseworkers should consider information held on Home Office case management systems (in particular, the Case Information Database and Atlas) before determining "whether IPIC has appropriately recommended the individual for the given intervention action".[57]

76. As above, there is no need to provide an explanation if accepting a recommendation. To reject the recommendation, the caseworker must select information from a drop-down menu entitled "why do you want to reject this case".[58] The training materials redact the options in the drop-down menu save for a catch-all reason, which is simply "reason not listed". There is then an optional further box that allows a caseworker to provide an explanation for why they rejected the recommendation (presumably if they selected "reason not listed").

77. The training materials explain that the reason for providing reasons when rejecting a recommendation is "to assist in identifying issues in the business rules and/or data". The materials also require caseworkers to update other HO systems (e.g. Case Information

[55] Home Office, Equality Impact Assessment, https://www.whatdotheyknow.com/request/triage_tools_used_in_an_immigrat/response/2002033/attach/3/68562%20Kazim%20Annex%20C%20EIA%20Redacted.pdf?cookie_passthrough=1

[56] Annex II: Data Protection Impact Assessment (DPIA), URN 77.19 (Updated), version 1.23, (17 March 2023), page 30.

[57] Ibid.

[58] Annex II: Data Protection Impact Assessment (DPIA), URN 77.19 (Updated), version 1.23, (17 March 2023), page 32.

Database /Atlas) if a recommendation is rejected. This is designed to prevent "the individual being recommended again and routed elsewhere in the future".

78. These business rules also allow caseworkers to put a recommendation on hold. The training materials state that this is only a temporary status and should be used only to park recommendations for a short time.[59] They should not be a means to manage recommendations over a prolonged period. The training materials clarify that a recommendation that has been placed on hold will not be rerouted but will rather remain on hold until they are accepted or rejected.

79. Placing a recommendation on hold also requires a caseworker to provide reasons from a drop-down menu with several options. One of these options is "manager escalation", which suggests that recommendations may be placed on hold for caseworkers to seek guidance or authorisation from managers prior to actioning a recommendation.

80. Once a recommendation is either accepted, rejected or put on hold it will be visible in the accepted, rejected or on-hold tabs. These tabs enable a caseworker to change accepted/rejected/on hold recommendations.[60] These business rules afford caseworkers with 5 days to change accepted recommendations whereas they are afforded with 20 days to change a rejected one. On hold cases will remain in the tab until they are either accepted or rejected.

The returns preparation 2 business rules also contain workflow and filtering functions that enable prioritisation of recommendations. For example, the training materials refer to a "get next" function that automatically sets the order of recommendations presented to caseworkers via several pre-set filters. While the majority of the "get next" filters are redacted, they include "person details"; "reporting dates" and "locations".[61]

81. If a caseworker selects "person details", for example, they can filter recommendations by "age" or "nationality". The filters allow the HO to include (or exclude) particular ages or nationalities such that recommendations that meet the filter requirements will be prioritised.[62] This could be used in a charter flight context; for example, if the HO was seeking to select suitable cases of a certain nationality for deportation. Indeed, as referenced above at §74 this is how the HO has stated in its EIA that it would use the filter function. These filters could be used together with the "get next" filters to facilitate highly granular and targeted immigration enforcement operations such as selecting individuals of a particular nationality who report to a certain reporting centre or on a particular date for detention.

[59] Ibid, page 34.

[60] Ibid, page 36.

[61] Annex II: Data Protection Impact Assessment (DPIA), URN 77.19 (Updated), version 1.23, (17 March 2023), pages 15-24.

[62] Annex II: Data Protection Impact Assessment (DPIA), URN 77.19 (Updated), version 1.23, (17 March 2023), page 17.

Failed EU Settled Status cases business rules

82. This is similarly a set of business rules for which we have comparatively less information on the exact nature of the immigration enforcement intervention. It is however clear that this version of the IPIC is used to generate recommendations for failed EU Settled Status ("EUSS") cases, which the training materials state are "ingested" into the tool on a weekly basis.[63]

83. The training materials show that a caseworker is similarly able to accept, reject or place a case on hold.[64] There are no instructions to explicitly review information when accepting or rejecting a recommendation; however, the training materials show that the screens seen by caseworkers include identical information as in "returns preparation 2" (see §73 above).

84. There is similarly no mechanism for caseworkers to explain why they have accepted a recommendation, while rejected recommendations likewise requiring an explanation that can be provided via a redacted drop-down menu or alternatively an optional box to provide additional information.

85. Placing a recommendation "on hold" contains a similar set of options to justify the decision as in the case of the returns preparation 2 business rules. There is likewise a drop-down menu that allows a caseworker to select "escalate to manager"; "file requested"; and "other" (which then includes an additional box requiring a caseworker to record their reasons).

86. Rather than "accepted" or "rejected" cases remaining on the accepted/rejected tabs for a particular number of days – cases will be actioned as soon as new recommendations are fed into IPIC the following week. "On hold" cases will remain in the tab until they are either accepted or rejected.[65]

87. As above, there is no guidance given to caseworkers on what to consider when conducting a review as to whether to accept or reject a recommendation. At the point that a recommendation has already been made, the training materials provide the following by way of instructions:

> "*1. Load the Accepted, Rejected and or On Hold tab based on the previous decision assigned in the case.*
>
> *2. The user should locate and click on the name of the case which needs to have the decision changed.*

[63] Annex VII: Immigration Enforcement, 'IE Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – EUSS Cases', page 4.

[64] Ibid, pages 5-7.

[65] Annex VII: Immigration Enforcement, 'IE Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – EUSS Cases', page 8.

> *3. The user should review the data held on IPIC and other case management systems (i.e. Case Information Database/Atlas) before changing the decision of whether IPIC appropriately recommended the case for the intervention*."[66]

88. There is no reference to automated filters and other prioritisation functionalities within the failed EUSS cases business rules.

89. Notably, one of the results in the searches carried out by Duncan Lewis related to [*redacted]*.[67] The presence of a barrier to removal is most relevant to decisions to serve an individual with removal directions (since this can only be done once all barriers have been resolved) [68] and/or detention, since immigration detention powers can only be used if an individual can be removed from the UK within a reasonable period of time. [69]

90. As such, it appears likely that the failed EUSS cases business rules are used in relation to decision-making as to whether to detain or remove EEA nationals.

Digital reporting immigration bail conditions

91. The training materials for this set of business rules state that an accepted recommendation will require users "to complete the process to set the person up on Digital Reporting" as *"this will not be done automatically by accepting the recommendations in IPIC."*[70] As such, the IPIC business rules generate recommendations as to whether an individual is suitable for digital reporting.

92. In this sense the HO was able to assert that IPIC was not used in decisions as to whether to grant immigration bail or what immigration bail conditions a person would be subject to. This is because reporting conditions are one of the immigration bail conditions that the HO can impose pursuant to its powers under paragraph 2 of Schedule 10 to the Immigration Act 2016. Digital reporting conditions are the means by which the HO imposes the condition rather than a bail condition in its own right.

93. These business rules likewise allow a caseworker to either accept, reject or place a recommendation on hold.[71] The information presented to them when determining whether

[66] Ibid.

[67] See § 32. See also, Annex IV - Duncan Lewis Solicitors, 'Analysis of Home Office Subject Access Bundles'

[68] See Home Office, Immigration Removals, Enforcement & Detention General Instructions, 'Initial consideration and assessment of liability to administrative removal', (version 4.0)(, (20 February 2024), pages 8 and page 53, https://assets.publishing.service.gov.uk/media/65d4d2c52ab2b300117595ac/Initial+consideration+and+assessment+of+liability+to+administrative+removal.pdf

[69] See Home Office, 'Detention: General Instructions', (version 4.0), (27 June 2025), page 13, https://assets.publishing.service.gov.uk/media/685c154689ba18761d97613e/Detention+General+instructions__1_.pdf

[70] Annex VIII: Home Office, 'IPIC Digital Reporting – Manager Training Guide', page 86.

[71] Ibid, pages 86-118.

to accept, reject or place a recommendation on hold is identical to the other business rules. This includes the drop-down menu providing reasons for rejecting a recommendation.

94. The drop-down menu when a caseworker places a case on hold contains two options when explaining why this decision was made. One of these is "manager check" and the other is "other", which is likewise accompanied by a further box to provide any additional explanation.

95. The guidance on how to conduct the human review is limited to the instruction only to accept a recommendation if a caseworker considers that it was appropriately made. The only other instruction is that caseworkers should check whether the "person details" are correct before accepting or rejecting a recommendation.

96. As with returns preparation 2, these business rules also require recommendations to remain in separate tabs for a period before they can be actioned. The periods of time before accepted and/or rejected recommendations will be actioned are identical to the returns preparation business rules.[72] Similarly, during this time a caseworker can change an IPIC recommendation. The training materials state in the case of accepted recommendations that this should only be done if a mistake has been made. There is no guidance provided in the training materials on the circumstances in which a rejected decision should be reversed.

97. The digital reporting business rules also have a prioritisation feature. This allows users to prioritise cases for recommendations on the bases of pre-determined filters, including age and nationality. As with returns preparation 2, this feature allows a caseworker to only include or exclude certain ages and/or nationalities.[73] The filter for these business rules also appears to include certain redacted vulnerabilities, which can also be included or excluded.[74] Recommendations can also be filtered on the basis of reporting date (i.e. to display cases within certain reporting date ranges). Finally, cases can be filtered on the basis of Reporting and Offender Management ("ROM") and Immigration Compliance and Enforcement ("ICE") regions.[75]

98. The training materials show that these business rules include an "assurance" tab that allows HO officials to download reports relating to the number of individuals subjected to digital reporting (including on a monthly basis).[76]

[72] Annex VIII: Home Office, 'IPIC Digital Reporting – Manager Training Guide', pages 118-124.

[73] Ibid, pages 52-53.

[74] Ibid, pages 56-57.

[75] We note that both the Immigration Compliance and Enforcement and Reporting and Offender Management teams within the Home Office are regionally based. As such, a regional Reporting and Offender Management team may be responsible for reporting centres that fall within its assigned region.

[76] Annex VIII: Home Office, 'IPIC Digital Reporting – Manager Training Guide', page 126.

Reporting and Offender Management ("ROM") business rules

99. These business rules allow for recommendations corresponding to several immigration enforcement interventions. In its response to the ICIBI's re-inspection of the Home Office's Reporting and Offender Management processes and of its management of non-detained Foreign National Offenders (October 2018-January 2019), the HO stated that the IPIC interventions corresponding to the use of the tool in this context included: "voluntary departure intervention; "ETDs" (*emergency travel documents)*; and "detention on reporting."[77] The response to the ICIBI inspection goes on to say that: "IPIC will be fed by caseworking units and will push cases into the relevant reporting centre at the optimum time to undertake the proposed action."

100. As such, it appears that recommendations generated by the Reporting and Offender Management business rules will determine if an individual is suitable for detention on reporting. This is confirmed through analysis of client subject access request files carried out by Duncan Lewis. Duncan Lewis's searches revealed [*redacted].* [78]

101. With regard to voluntary departure interventions, we note that the HO's Voluntary and Assisted Departures policy dated 18 March 2024 states that the voluntary returns scheme includes both assisted and non-assisted returns. The former "involves is an umbrella term referring to any non-enforced departure of an immigration offender (or their family members) from the UK to the destination country."[79] The latter involves the provision of financial support of up to £3,000 if an individual agrees to voluntarily return where they meet certain financial requirements.

102. It is therefore possible that the Reporting and Offender Management business rules generate recommendations that individual is eligible for either assisted or non-assisted voluntary return. Such a recommendation could, for example, lead to an individual being contacted or served with paperwork relating to the voluntary returns scheme.

103. It is noted that the previous government (alongside the UK-Rwanda memorandum of understanding it announced in 2022) expanded the voluntary returns scheme to incorporate assisted returns to Rwanda (as opposed to an individual's country of origin) for failed asylum

[77] Home Office, 'The Home Office response to the Independent Chief Inspector of Borders and Immigration's report: A re-inspection of the Home Office's Reporting and Offender Management processes and of its management of non-detained Foreign National Offenders', (October 2018 - January 2019), https://assets.publishing.service.gov.uk/media/5cd3e056e5274a3fd5871f36/Formal_response_ICIBI_FNO_ROM.PDF

[78] Annex IV, Duncan Lewis Solicitors Analysis of Home Office Subject Access Bundles.

[79] Home Office, 'Returns, Enforcement & Detention policy General Instructions, Voluntary and assisted departures', version 6.0, (18 March 2024), https://assets.publishing.service.gov.uk/media/65f864aece4c150011a15081/voluntary+and+assisted+departures.pdf

seekers in 2024.[80] This is notable because the BBC's reporting of this change in the policy stated that immigration lawyers were aware of cases of individuals, including those with vulnerabilities, being offered voluntary return to Rwanda.[81] While we do not have confirmation to this effect, it is possible that voluntary departure intervention recommendations were deployed to select suitable cases for voluntary return to Rwanda.

104. The Emergency Travel Documentation ("ETD") recommendations relate to the steps required for the HO to obtain emergency travel documentation from the country of origin. It is unclear whether this use of the IPIC provides recommendations for individuals who are likely to require an emergency travel document or selecting individuals whose pending emergency travel document applications should be escalated to ensure that removal can be effected. As above, the DPIA completed for IPIC confirms that the tool processes travel document data (separately confirmed by the reference in disclosure received by Duncan Lewis to a rejected IPIC recommendation on the basis that [*redacted].*

105. The training materials show that a caseworker is similarly able to accept, reject or place a case on hold. There are no instructions to explicitly review information when accepting or rejecting a recommendation; however, the training materials show that the screens seen by caseworkers include identical information as in "returns preparation 2". Nor is there any guidance on how to conduct any human review when accepting or rejecting a recommendation.

106. The training materials also demonstrate that cases remain in the accepted/rejected/on hold tabs after the recommendation is actioned for an identical period as set out in the returns preparation 2 business rules.[82] The materials do not refer to any prioritisation features including the filters referenced above with respect to several other business rules.

Central Support and Tracing Team (CSTT) business rules

107. It is apparent from publicly available information, in particular the National Police Chiefs' Council's ("NPCC") *Advice to Police Forces on Adult Asylum Seekers, Undocumented Migrants and Visa Applicants who Abscond and when they should be Recorded as Missing* that these rules relate to the Central Support and Tracing Team.[83] The NPCC Guidance describes the purpose of the Central Support and Tracing Team ("CSTT") as: "…initiating tracing actions on

[80] Paul Seddon, 'Failed asylum seeker given £3,000 to go to Rwanda', BBC News, (1 May 2024), https://www.bbc.co.uk/news/uk-politics-68932830

[81] Ibid.

[82] Annex IX: Immigration Enforcement, 'Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – Reporting and Offender Management', page 9.

[83] National Police Chief's Council, 'Advice to Police Forces on Adult Asylum Seekers, Undocumented Migrants and Visa Applicants who Abscond and when they should be Recorded as Missing', (28 November 2022), page 28, https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/national-crime-coordination-committee/2023/npcc-advice-to-police-forces-on-adult-asylum-seekers-undocumented-migrants-and-visa-applicants-who-abscond-and-when-they-should-be-recorded-as-missing.pdf

all absconders with the exception of Criminal Casework absconders who are the responsibility of the Criminal Casework Trace and Locate Team”.[84] CSTT is also said to “prioritise removable cases, highest harm cases, vulnerable adults and missing children”.[85] As such, a separate team is responsible for tracing foreign national offenders who have absconded (it is not clear if they would similarly have recourse to IPIC).

108. As with the returns and EUSS business rules, the exact nature of the CSTT recommendations is not evident from the documents disclosed by the HO pursuant to our FOIA request or other information in the public domain. The *Training Guide -CSTT (Managers)* does however confirm that these rules are used in relation to absconders as it states that: “for absconders at present, there is only one action type … available.”[86] The nature of this enforcement action type is redacted. However, from the above purpose of the CSTT it is likely that the recommendations relate to enforcement actions taken to apprehend and remove absconders.

109. As with a number of the other business rules, all cases that fall within the enforcement action type can be allocated to caseworkers by way of a manager setting up and assigning them to a ‘group’, which will then only be able to consider cases of the same type.[87] Given that we know from the above that there is only one enforcement action type for these rules, it is apparent that all relevant cases would be assigned to the group that reviews recommendations relating to absconding.

110. The CSTT business rules permit a caseworker to accept, reject or put a case on hold. The sole guidance afforded to caseworkers in the Training Guide – CSTT v1.1 (Final) (the “CSTT Caseworker Training Guide”) is that they should review both the data contained in IPIC itself and information in the HO’s casework databases (in particular the Case Information Database and Atlas).[88] The screens presented to caseworkers are otherwise identical to the Reporting and Offender Management and Returns Preparation 2 business rules as set out above. In particular, a caseworker must provide reasons when rejecting a recommendation but does not have the same requirement when accepting one.

111. As with the returns preparation 2 rules, cases will stay on the ‘accepted tab’ for 5 days whereas they can stay on the ‘rejected tab’ for 20 days.[89] During this time, a caseworker can change the recommendation.

[84] Ibid.

[85] Ibid.

[86] Annex XI: Immigration Enforcement, ‘Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – CSTT (Managers), page 12.

[87] Ibid, pages 14-15.

[88] Ibid, page 4.

[89] Ibid, page 11.

112. These business rules also allow filtering such that cases that meet a pre-selected filter will be automatically prioritised and allocated to the group for consideration.[90] The filters that can be selected are wholly redacted.

113. The Management Information reports (which as above can be generated in relation to any IPIC business rules) can display the overall number of recommendations relating to absconders over the previous week. Similarly, the 'find someone' function can be used in this context to instantly find the specific case details of all Absconder activity taken on an individual within IPIC. For example, this function would allow a user to see the outcome of previous recommendations and the date they took place.

Interventions and Sanctions Directorate (ISD) business rules

114. As above, the relevant training materials and the HO's policies suggest these business rules relate to the Interventions and Sanctions Directorate (”ISD”) within immigration enforcement.[91] The training materials (which are labelled the *IPIC Detailed Reference Manual ISD*) indicate that once an IPIC recommendation is accepted the case will be "suitable for sharing with the relevant government agency".

115. The *HO's Sanctions: refer case to the ISD* Policy (the "ISD Policy") dated 17 January 2018 makes clear that other departments within the HO are charged with referring relevant cases to the Interventions and Sanctions Directorate, which will then in turn share data with the public authority in question.[92] For example, the ISD Policy suggests that cases will need to be referred to the Interventions and Sanctions Directorate where an official believes that an individual does not have leave to remain and is liable for National Health Service charging. Thereafter, the Interventions and Sanctions Directorate will share details relating to such a case with the NHS. As per Regulation 3(1) of the National Health Service (Charges to Overseas Visitors) Regulations 2015, the obligation falls on the relevant NHS trust to make and recover charges from a person it deems liable for payment of charges.

116. Similarly, the Interventions and Sanctions Directorate Policy also provides details (entirely redacted) for officials to make referrals to the Interventions and Sanctions Directorate when "they believe they are claiming benefits, while having no right to live and work in the UK."

[90] Ibid, page 15-16.

[91] The ISD's purpose is to enforce the 'hostile environment' at the operational level "through a series of legislative and non-legislative measures, built upon a framework of compliance, deterrence and data-sharing." See, ICIBI, 'An inspection of Home Office (Borders, Immigration and Citizenship System) collaborative working with other government departments and agencies', (February – October 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/774736/An_inspection_of_Home_Office_collaborative_working_with_OGDs_and_agencies_web_version.pdf

[92] Home Office, 'Immigration Removals, Enforcement and Detention General Instructions, Sanctions: refer case to Interventions and Sanctions Directorate (ISD), version 3.0, (17 January 2018), https://assets.publishing.service.gov.uk/media/5a82ccb3e5274a2e87dc30aa/ISD-referrals-and-sanctions-v3.0ext.pdf

The Interventions and Sanctions Directorate will then share "illegal migrant data with DWP to enable them to investigate whether those individuals who are in receipt of benefits and credits are entitled to them." It will similarly therefore be up to the Department for Work and Pensions to sanction the individual in question if they do not consider that they were entitled to benefits and/or tax credits.

117. Within the Interventions and Sanctions Directorate, the Civil Penalty Compliance Team ("CPCT") and the Data and Sanctions Team ("DAST") are responsible for administering the range of "Access to Work and Services" ("AWBS") sanctions and penalties on behalf of the HO and will engage with other government departments in the manner set out above.[93]

118. As such, the Interventions and Sanctions Directorate business rules recommend cases for referrals to other government departments such as the NHS or the Department for Work and Pensions, which may then in turn sanction the individual by, for example, charging them for past medical treatment. This is confirmed by the ICIBI's 2021 report on the HO's use of sanctions and penalties (cited above), which states that:

> "*DAST managers told inspectors that a "triple lock process" had been put in place to ensure that anyone with permission to remain in the UK is protected. This involved* ***applying business rules*** *to identify the right cases for sharing; dip sampling by DAST staff of 100 cases each month to ensure that the business rules were being applied correctly; and, manual checking of matched cases by DAST to ensure that the individual's status had not changed since sharing and* ***that the case was suitable for other departments to consider applying a sanction****.*"[94]

119. The training materials indicate that the ICIBI's reference to the business rules corresponds to IPIC. This is because the training materials refer to "dip sampling" by HO staff, as mentioned in the ICIBI's report.[95] Per the training materials, the ordinary review process is for a caseworker to accept an IPIC recommendation if the case details are correct (this involves checking IPIC and other HO databases, including Case Information Database after consulting the "ISD flow guidance notes"[96]. The process is reversed if a recommendation is rejected. There is no option to put a case "on hold".

120. As with other business rules, a caseworker must provide reasoning when rejecting a recommendation.[97] There is no need to do the same when accepting a recommendation. The list of rejection reasons is redacted, although it appears that if a reason is not covered in the pre-set list, then an additional explanation must be provided.

[93] ICIBI, 'An inspection of the Home Office's use of sanctions and penalties', (November 2019 – October 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951438/An_inspection_of_the_Home_Office_s_use_of_sanctions_and_penalties__November_2019___October_2020_.pdf

[94] ICIBI, 'An inspection of the Home Office's use of sanctions and penalties', supra note 93, page 72.

[95] Annex XIII - IPIC Interventions and Sanctions Directorate (ISD) Training Materials – Redacted, pages 5, 13, 16.

[96] We note that these have not been disclosed to us.

[97] Annex XIII - IPIC Interventions and Sanctions Directorate (ISD) Training Materials – Redacted, page 8.

121. The case details presented to caseworkers on IPIC for the purposes of the review is identical to other business rules. It is apparent that a caseworker can reverse a recommendation, although it is unclear how much time is afforded for an official to change their mind.

122. At the point that a caseworker has no more cases to review, they should notify the relevant IPIC manager. Thereafter, the training materials state that a manager will need to "dip sample" the accepted and rejected cases. If all cases are deemed correct the manager should confirm by clicking "approve case decisions". The training materials show that a manager can also reverse an accepted or rejected recommendation (and the materials suggest that the process is identical for managers as for caseworkers).

123. There is a notice to IPIC managers in the training materials to inform the Immigration Enforcement Business Rules ("IEBR") team if "too many cases have been rejected". It is unclear when such a threshold will be met.

124. Notably, the Interventions and Sanctions Directorate business rules incorporate "person reports" (alongside the management feature common to all the rules that is outlined above).[98] These allow a manager to search for any individual via their Personal Identification Number ("PID") to check if they have ever been recommended for sharing with the relevant government agencies (examples redacted) and the date (including month and year) on which this took place.[99]

125. The ICIBI report states that Interventions and Sanctions Directorate suspended the use of all AWBS sanctions and penalties in April 2018 in the wake of the Windrush scandal.[100] The sanctions were reintroduced three months later together with safeguards to protect members of the Windrush generation (it is unclear what the safeguards were). As of January 2020, bulk data sharing was limited to those born after 1 January 1989 (when the Immigration Act 1988 came into force as a result of which members of the Windrush generation lost immigration status). This was because the HO was confident that anyone born after that date would either have documentation or there would be official records to evidence their arrival in the UK. It is unclear if this restriction remains in place.

126. The ICIBI report stated that the CPCT continued to use matches produced through data sharing with HMRC to identify individuals working in breach of their leave conditions throughout this period. It is noted that Duncan Lewis searches of subject access requests resulted in [*redacted*]. A number of these searches referred to [*redacted*]. It is possible that this refers to automated data sharing with HMRC and other departments to locate individuals

[98] Annex XIII - IPIC Interventions and Sanctions Directorate (ISD) Training Materials – Redacted, p. 11.

[99] Ibid.

[100] ICIBI, 'An inspection of the Home Office's use of sanctions and penalties', (November 2019 – October 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951438/An_inspection_of_the_Home_Office_s_use_of_sanctions_and_penalties__November_2019___October_2020_.pdf

working in breach of their conditions of leave; although it is unclear if this is through IPIC or another tool.

The EMRT examined

The status of the EMRT

127. As above at §§ 41 & 43, the HO has asserted on multiple occasions through FOIA correspondence that it discontinued the EMRT in 2023 and that there is no decision support tool currently in use (including IPIC). We note that this is inconsistent with correspondence received by Wilsons in 2024 (a redacted version of which is enclosed as Annex III to these submissions), which refers directly to a recommendation support tool as having been used to generate a recommendation in a client's case.

128. The letter received by Wilsons relates to a client who was transferred from an ankle tag to a non-fitted device ("NFD").[101] The letter dated [*redacted]* is a response to representations submitted by Wilsons on behalf of their client on [*redacted]*, which requested a cessation of electronic monitoring (EM) altogether on the basis that the Secretary of State for the Home Department ("SSHD") had failed to consider the client's vulnerabilities when transferring them to an NFD. In the response the HO refused to cease tracking through the NFD.

129. Material for these purposes is the following reference in the HO's response:

> "*On [redacted] a review of your client's electronic monitoring was conducted. It was concluded that he met the criteria for transition to a Non-Fitted Device and he was inducted with this on [redacted].* ***During the above scheduled review of your clients electronic monitoring on [redacted], details of his case at that time were inputted into a support tool. This tool utilises automated business rules to provide decision recommendations for the decision maker to consider alongside other relevant factors set out in the Immigration Bail Policy****.*"

130. It is noted that the reference to the scheduled review is to the quarterly reviews of the appropriateness of the ongoing use of GPS tracking the HO must carry out as a matter of policy.

[101] The NFDs deployed by the UK Home Office are small handheld devices with a fingerprint scanner that record a person's location 24/7 in the same way as an ankle tag. These devices are the size of a large smartphone, and they require daily charging. Individuals subject to this form of monitoring must scan their fingerprints to verify their identity several times per day. See Privacy International, 'Non-fitted devices in the Home Office's surveillance arsenal: Investigating the technology behind GPS fingerprint scanners', (29 October 2024), https://privacyinternational.org/long-read/5457/non-fitted-devices-home-offices-surveillance-arsenal-investigating-technology-behind

131. We further note that the current version of the Immigration Bail policy (dated 31 January 2025) also states that where "the EM duty applies the HO decision maker may have access to a decision support tool which utilises automated business rules to provide decision recommendations".[102] The policy states that business rules can both be used to generate recommendations as to whether a non-detained individual is suitable for EM or whether it is appropriate to consider moving an electronically monitored person between a fitted device, a NFD and no device. As above, the HO has stated in FOIA correspondence that it deployed the EMRT in all relevant cases.

132. The reference to the EM duty is to paragraph 2(5) of Schedule 10 to the Immigration Act 2016. This provides that where an individual is subject to a deportation order or liable to deportation the HO is under a duty to subject them to EM (unless the immigration bail condition would breach the individual's rights under the European Convention on Human Rights or is impractical). The Immigration Bail policy therefore confirms that these business rules are only used in relation to the tagging of foreign national offenders that come within the EM duty rather than the now terminated EM Expansion Pilot.

How the EMRT works

133. The information in this section is based on information provided in response to FOIA requests (including the training materials disclosed to Duncan Lewis)[103] as well as information included in the Immigration Bail policy.

The nature of the EMRT recommendations and the type of review they carry out

134. The training materials disclosed pursuant to FOIA demonstrate that the EMRT generates one of two potential recommendations. A 'green' EMRT recommendation indicates that the tag wearer should be transitioned to a NFD (as took place in the case of the Wilsons client set out above).[104] Alternatively, a 'red' recommendation means that tool recommends maintaining EM by way of an ankle tag.[105] **There is no possibility for the tool to recommend that a GPS tracker is removed altogether**, which is in direct contrast to what the HO states in its Immigration Bail policy (see §132 above).[106]

135. The training materials indicate the EMRT is only used in relation to the mandatory quarterly reviews.[107] As per the Immigration Bail policy, there are other circumstances in

[102] Home Office, 'Immigration bail', version 21.0, (31 January 2025), https://assets.publishing.service.gov.uk/media/679a0ca085c5e43aa3d10dc6/Immigration+bail.pdf

[103] Annex XXI - Duncan Lewis FOIA Request (4 March 2024), Redacted.

[104] Annex XIV - EM Review Tool Training Materials, page 18.

[105] Ibid.

[106] Ibid.

[107] Annex XV - EM Review Tool Training Materials 2023, page 5.

which the HO will be obligated to review an EM condition, such as in response to representations challenging the bail condition. Such reviews will be conducted by the "EM Hub Legal Stream" without recourse to the tool.[108]

136. The training materials show that the EMRT could be used in relation to several other reviews, including "minimum period reviews; inactive monitored reviews; transition unavailable reviews; missing TRAM cases; no reporting office data; and out of scope reviews". These features cannot be used however (as of 2023 when the training materials are dated) due to the need for further updates. It is also not clear what these reviews relate to in light of redactions in the training materials and the fact that they are not mentioned in the Immigration Bail policy.

137. When using the EMRT, a caseworker inputs an individual's data into an EM review pro forma which is itself partly auto populated. Once the form is fully populated, the algorithm will generate its recommendation.

Gathering the relevant information to input into the EMRT

138. Prior to inputting the data into the digital review form for the algorithm to generate its determination, the training materials state that a caseworker should gather relevant input data in a word document. Notwithstanding many redactions, we can see that this includes the last dial in date and time of the individual's GPS tracker; information relating to battery breaches and strap tampers within the last quarter; vulnerabilities (including medical issues), barriers to removal and offence details (caseworkers are instructed to review past Detention Reviews to gather this information); and compliance with reporting bail conditions.[109]

Completing the form and the harm score

139. Once this data has been gathered, a caseworker will begin by filling in the individual's Personal Identification Number after which a number of data points will be automatically populated. This includes the tag wearer's name, gender and the nature and length of their sentence.[110] After checking that these details are correct, the reviewer will move to the next part of the EM review pro forma form.

140. At this stage the caseworker should check whether the individual has any conditions supplementary to the EM condition (e.g. an inclusion or exclusion zone) as well as the bail type (i.e. whether bail and relevant conditions were granted by the First-tier Tribunal or the HO) as these details are also automatically populated.[111]

[108] Ibid, page 2.

[109] Annex XVI - Gathering information for Electronic Monitoring Review Tool Redacted.

[110] Annex XIV - EM Review Tool Training Materials, page 4.

[111] Ibid, page 7.

141. The review form will likewise populate the individual's risk of harm based on an automatically generated harm score.[112] The Immigration Bail policy makes clear that the business rules assessing a wearer's risk of harm will determine if an offence is 'low', 'medium', 'high harm' or 'very high harm'.[113] The policy reproduces a partially redacted table with categories of example offences falling within the above 'harm types'. For example, illegal entry is said to be a low harm 'type' whereas theft would be classified as medium harm and false imprisonment would constitute a very high harm type. There are some harm types which do not correspond to a clear offence, for example 'SRP' (Somali Region Programme) is said to be a high harm type.[114]

142. The Immigration Bail policy then states that the EMRT will assign an individual a score between 600 (the highest possible harm cases) and anything below 150 (the lowest possible harm cases) within 1 of 5 tiers (1 corresponding to the greatest harm level and 5 to the lowest).[115] It is not clear from the policy or elsewhere how an individual's harm type (within the above categories) influences the harm score, although it states that the "harm score relates to the offence committed which may not automatically be reflected by the sentence imposed."[116] Neither the policy nor any other documentation we have seen explains exactly how the harm score is calculated by the tool.

143. The harm score assigned to the individual will determine the minimum period on which they are subject to both an ankle tag and a non-fitted device. The policy goes on to provide a table setting out what sentences are likely to result in particular harm scores and in turn the minimum length of time (associated with each score) a tag wearer will spend on both an ankle tag and an NFD.[117] For example, a harm score in tier 2 (greater than or equal to 400) is likely to correspond to a sentence of 6 years and an individual within this tier would remain on an ankle device for 12 months and on an NFD for 30 months.

144. The policy explains that the scores and the corresponding minimum periods of time are indicative only. This is in part because the tiers amount to a range of potential harm scores rather than an exact score (which would be specific to the facts in a tag wearer's individual case including their harm type as addressed above).

145. For example, tier 5 corresponds to sentences of 3 years or less – this could in turn occasion a harm score of anything up to 150. Consequently, the minimum period on an ankle tag and an NFD referred to in the table for tier 5 would also vary depending on the exact harm score.

[112] Annex XV - EM Review Tool Training Materials 2023, page 3.

[113] Home Office, 'Immigration bail', version 21.0, (31 January 2025), page 50, https://assets.publishing.service.gov.uk/media/679a0ca085c5e43aa3d10dc6/Immigration+bail.pdf

[114] Home Office, 'Immigration bail', version 21.0, (31 January 2025), page 51, https://assets.publishing.service.gov.uk/media/679a0ca085c5e43aa3d10dc6/Immigration+bail.pdf

[115] Ibid, page 54.

[116] Ibid.

[117] Ibid.

Moreover, the total length of time on a particular device may vary due to other factors considered by the EMRT (such as compliance with immigration bail conditions) and factors not considered by the tool (such as the availability of GPS devices). Further details relating to human intervention in the context of the harm score are addressed below.

146. The form also requires the caseworker to input information about the wearer's vulnerabilities. For example, the EM review pro forma requires a 'yes' or 'no' answer in response to the question of whether they have any safeguarding, recent mental health/medical concerns brought to light or have received a positive Conclusive Grounds Decision recognising them as a victim of trafficking.[118]

147. The vulnerabilities recognised by the tool are "mental capacity insufficient to comply with EM condition"; "physical health issues mean they are unable to comply without the assistance of others"; "18 weeks pregnant"; "evidence of historic psychological trauma that means EM condition would be unsuitable;" "other physical/mental health issues"; and "other".[119]

148. If the caseworker selects 'no' then this concludes the section of the form on vulnerability. If they select 'yes' they will be taken to another screen, which asks if their vulnerabilities are sufficiently and suitably evidenced. The training materials state that an example of this would be if detention reviews or any safeguarding notes on HO databases, such as Atlas, showed a history of "mental health issues/self-harm or suicide". Significantly, the EM training materials suggest that the caseworker "could select" "vulnerability evidenced but does not affect capacity to comply with EM".[120]

149. Where an individual has claimed that EM is impacting their physical/mental health, but no medical evidence has been submitted to support this the caseworker could select the option of "no – vulnerability unevidenced. There are also the options to select "no – vulnerability neither evidenced nor would it affect capacity to comply with EM" and "yes – vulnerability warrants device transition & evidence provided."[121]

150. As above, there is no vulnerability option that warrants removal of the EM condition altogether – instead the sole option is to transition from an ankle tag to an NFD (in line with the fact that the EMRT cannot recommend removal of the device altogether). Moreover, the Immigration Bail policy does not appear to set out how to consider when sufficient evidence has been provided to justify device transition for the purposes of the tool (albeit there are substantial redactions within the policy). We will address this further in the context of human intervention below.

[118] Annex XIV - EM Review Tool Training Materials, page 9.

[119] Ibid, page 11.

[120] Ibid, page 10.

[121] Ibid.

151. If a casework selects ‘yes’ (i.e. that vulnerabilities have been sufficiently evidenced and justify device transition) – then the EMRT asks for confirmation that the request has been made by a sufficiently authorized person (i.e. someone who is a Grade 7 or above).[122] The EMRT then skips to the end and generates a recommendation without the need to add information on compliance/breaches.

152. If the answer was ‘no’ then the caseworker will need to input further information about the subject’s record of compliance with immigration bail conditions. This includes information on “battery breaches” (i.e. failures to charge the GPS tracker); “strap tamper breaches” (i.e. attempts to interfere physical with a tracker); new offences committed (only those that resulted in a conviction/sentencing); out of contact periods (i.e. periods of time during which GPS trackers have not transmitted data); and missed reporting events[123].

153. Notably, the training materials include reference to an unpublished battery and reporting breach thresholds for each of the harm score tiers (see above) for the latest 3-month period.[124] Although the thresholds themselves are redacted, it is clear from the materials that they relate to acceptable levels of missed reporting dates and alleged failures to adequately charge the device for each harm score tier. If such a threshold is exceeded, the EMRT would recognise the subject as having a battery and/or reporting breach, which would in turn be considered by the tool. As above, there is no mention of these thresholds anywhere else (including in the Immigration Bail policy).

154. The training materials state that where the tag wearer’s device has been out of contact (“OOC”) for a period of more than 7 days without mitigation they would be regarded as non-compliant for the purpose of the EMRT regardless of their harm tier.

155. Thereafter the EMRT requires the caseworker to input information about whether removal is imminent. Where the tag wearer has a barrier to removal this question would be answered as ‘no’. Conversely, if they have no barriers to removal the caseworker would need to select yes’.

156. The final window before the EMRT generates its recommendation corresponds to “other risks deemed so high that decision is to maintain monitoring.”[125] This window consists of a drop-down menu. If there are no ‘high risk’ elements and the caseworker wants to maintain EM, then they would select ‘other’.

157. Alternatively, if the subject of the EM condition is a Multi-Agency Public Protection Arrangement (“MAPPA”) case – they will automatically be considered ‘high risk’. The training materials indicate that the drop-down menu includes a question on whether the individual

[122] Ibid, page 11.

[123] Annex XIV - EM Review Tool Training Materials, page 13.

[124] Annex XV - EM Review Tool Training Materials 2023, pages 3 and 16.

[125] Annex XIV - EM Review Tool Training Materials, page 17.

under review is a MAPPA case. If the answer is 'yes' then there is a further drop-down, which appears to be redacted.

158. However, it is clear from the training materials that MAPPA cases will only be suitable for transition to an NFD once MAPPA status has expired. This will take place at different times dependent on what MAPPA category the individual is (for example the expiry date for a category 1 MAPPA case will be the date their sex offender registration ends).

159. After this section, the EMRT generates a review form through Excel, which includes the decision recommendation (see above at §135 for the nature of recommendations that can be made by the tool).

Human intervention in the EMRT

160. It is clear from the training materials that a case will not be transitioned to a NFD if the minimum period corresponding to the harm tier has not elapsed.[126] It does not appear from the training materials that there is any human review in relation to the harm score itself. Instead, the materials state that although the minimum period will already be considered by the EMRT when generating its recommendation – caseworkers must check that the minimum period has indeed expired before transitioning from an ankle tag to an NFD.[127] The minimum period can be checked with reference to the table of the relevant tiers, potential scores and periods of time on each device (which is located in both the training materials and the Immigration Bail policy).

161. There is limited guidance on human review relating to the substantive recommendations generated by the EMRT. The training materials merely state that if a caseworker agrees with the recommendation, they should accept it and edit anything incomplete or inaccurate in the EM review form generated via Excel (such as if the offending information was blank).[128] Conversely, if a caseworker disagrees with the recommendation, they should reject it. In case of a rejection – a caseworker should "select the relevant option and proceed as required".[129] It is unclear what this entails given that the accompanying screenshot is redacted.

162. The training materials state that caseworkers should consider the need for continued monitoring, the continued necessity of any supplementary conditions (such as a curfew or inclusion/exclusion zone) and whether the individual is suitable for a change of device or removal of EM.[130] However, as above – the EMRT cannot generate recommendations as to whether an individual is no longer suitable for EM altogether. Indeed, there is no guidance

[126] Annex XV - EM Review Tool Training Materials 2023, page 15.
[127] Ibid, page 16.
[128] Annex XIV - EM Review Tool Training Materials, page 19.
[129] Ibid.
[130] Annex XV - EM Review Tool Training Materials 2023, page 2.

on how a caseworker should consider whether an EM condition should be removed entirely once the EMRT generates its recommendation.

163. The Immigration Bail policy also refers to the need to consider the requirement for continued monitoring alongside whether an individual can be transitioned between devices. It lists a number of factors that should be considered during the review process. These include overall time spent on EM as well as on a particular device, an individual's risk of harm and their vulnerabilities, however all the factors are already inputted into and considered by the tool. The policy also explains how these factors should be balanced against each other; however as above it appears that this weighting is undertaken by the tool.

164. The pro forma wording generated by the EMRT (which caseworkers are instructed to add manually if the tool fails to produce the requisite text) once the review is complete is:

> "*In line with the agreed principles for assessing harmfulness, in particular considering offending history, I have decided it is proportionate for X to be transitioned to an NFD…*"[131]

165. There is no pro forma wording relating to the consideration of the suitability of tagging as a whole and this demonstrates that the tool is being deployed to assess proportionality of tagging through a weighting of the above factors. Moreover, there is no pro forma EM review form generated by the EMRT that corresponds to removal of the tag altogether (the forms disclosed in full together with the complaint only relate to maintaining an individual on an ankle tag, maintaining them on an NFD or transitioning them to an NFD from an ankle tag).

166. The EM review form does appear to allow a caseworker to leave additional comments, but the training materials suggest that this would only be used to add additional information not populated by the tool itself (including whether there are barriers to removal).

167. If, once the review is completed, the decision is to maintain an individual on an ankle tag – the training materials instruct the caseworker to diarise the next quarterly review, complete a spreadsheet with the date of the review and any additional notes/comments and save the review within a personal SharePoint folder. The materials suggest that this decision-making is subjected to quality assurance ("QA"). It is unclear if this is done in every case and if the relevant official can change the outcome of the review. The only reference to QA states that this is carried out by designated authorising officers and that once completed the caseworker will be informed of the outcome and provided with any feedback.

168. Where the decision is to transition an individual to an NFD the process is almost identical to the above description. However, the training materials specify that the quality assurance process requires approval of the authorising officer and that if the case is not found suitable for transition the recommendation will be sent back to the caseworker for amendment.

[131] Annex XV - EM Review Tool Training Materials 2023, page 15.

169. There is a separate page in the page on quality assurance criteria for scheduled EM reviews. This states that: "Not in public interest? Criteria by which staff's work is QA'd - would we just have to release it anyway?" It is unclear what is meant by this and whether further content on this page may be redacted.[132]

IV. The provision of privacy information in relation to IPIC and the EMRT

IPIC

170. There is no bespoke privacy information relating to IPIC either conveyed to migrants whose data may be processed by the tool or in any of the HO's published privacy policies.

171. The HO's generic privacy information is located across two documents, the *Borders, immigration and citizenship: privacy information notice* (the "HO PIN") and the *personal information charter* (the "HO PIC").

172. We note that the HO PIN provides vague and generic information about the use of profiling and ADM. In particular, the HO PIN states that personal data may be used to develop fraud and risk profiles as part of border operations.

173. There is a sub-section of the HO PIN that expressly covers ADM and profiling. This states as follows[133]:

> "*Article 22 of the UK GDPR provides the right not to be subject to a decision made solely on the basis of automated processing which produces legal or other significant effects. Parts of our processing may involve degrees of automation, but complex or adverse decisions will always be taken by a trained officer or caseworker.*
>
> *We may use personal information, for example from previous applicants, to develop tools that allow us to assess and then process applications in a particular way. This helps us to target our resources and ensure our processing is efficient, allowing us to minimise costs while protecting the public effectively. However, an officer would still be available to decide and/or review any such decision. Any profiling must comply with our wider obligations under equality legislation.*"

174. As such, there is an acknowledgement that ADM and profiling may be used in the context of immigration and border operations. However, the only detail provided is that tools may be developed to "assess and then process applications in a particular way."

[132] Ibid, page 18.
[133] Home Office, 'Guidance: Borders, immigration and citizenship: privacy information notice', (16 October 2023), https://www.gov.uk/government/publications/personal-information-use-in-borders-immigration-and-citizenship/borders-immigration-and-citizenship-privacy-information-notice

175. The HO PIC, which appears to relate primarily to immigration enforcement, states that personal data may be shared with government departments. This is not particularised and the privacy information does not specify which departments and states that sharing may take place where lawful and necessary.[134] The HO PIC also indicates that personal data may be provided to other government departments, such as the DWP, "for the purposes of verifying information you supplied in support of an application, obtaining information needed for a safeguarding purpose, obtaining new address details of people we are trying to trace, or undertaking other enforcement actions."

176. There is no mention of ADM or profiling in the HO PIC.

The EMRT

177. We note that under the FOIA 2000 we requested copies of all privacy information documents disclosed to the ICO as part of its Enforcement Notice regarding the HO's EM Expansion Pilot (the "EM Enforcement Notice").[135] This included the STS Bespoke Privacy Information Notice (the "STS PIN") disclosed to the ICO on 30 January 2023, which the HO ostensibly provides to tag wearers at the point that the tag is fitted.

178. The STS PIN relates to the use of GPS tracking in cases where the HO is under the duty to impose EM (as opposed to the Expansion Pilot cases). As above, it is in relation to duty cases that the HO deploys the EMRT. Given that the STS PIN was provided in January 2023 it was clearly in use at the time when the HO acknowledges that the EMRT was in use (November 2022 – August 2023). The STS PIN states that:

"*All individuals who meet the criteria for being 'tagged' will be informed of this and will be offered the opportunity to provide reasons why they should not be tagged. These reasons will be considered on a case by case basis and there is no Automated Decision Making involved in this or any 'review' process final decision.*"

179. As per the STS PIN and the ICO's EM Enforcement Notice, further privacy information is provided through an Electronic Monitoring Handbook (the "EM Handbook") that should also be provided to tag wearers at the time the device is fitted. As with the STS PIN we secured disclosure of this by way of the above request under FOIA.[136] This likewise states that there is no ADM either in any initial decision and during review of the EM condition. The EM

[134] Home Office, 'Personal information charter', https://www.gov.uk/government/organisations/home-office/about/personal-information-charter

[135] WhatDoTheyKnow, 'Privacy International request to Home Office', (23 May 2024), https://www.whatdotheyknow.com/request/information_included_in_the_icos#incoming-2675479

[136] WhatDoTheyKnow, 'Privacy International request to Home Office', (23 May 2024), https://www.whatdotheyknow.com/request/information_included_in_the_icos#incoming-2675479

Handbook is dated 16 May 2023 and as such it was also in use at the time that the HO acknowledges that the EMRT was in use.

180. We note that there is no reference to the EMRT or any decision support tool in other privacy information (including the HO PIN and PIC).

V. Legal framework and concerns

181. This section sets out PI's concerns in relation to the compliance of the HO's use of IPIC and the EMRT with its obligations under the UK GDPR and DPA 2018. We consider that the HO's use of both systems fails to comply with the vast majority of the seven principles of data protection law alongside other requirements, including those relating to DPIAs and the prohibition on solely ADM. Where our submissions only apply to one tool and not the other this is explicitly stated.

182. Before turning to the substance of our submissions we address the ICO's Decision Notice dated 11 November 2024 as a preliminary issue.

Preliminary issue: the Decision Notice and the nature of the data processing in question

183. As above, the ICO's Decision Notice relating to our IPIC FOIA request found under the FOIA that the tool does not involve profiling and/or ADM for the purposes of the immigration procedures and applications we specified in our request.

184. The nature of the IPIC recommendations and by extension what form of data processing they constitute was at issue in the FOIA request and subsequent complaint, because the HO sought to exempt this information on the basis that migrants could 'game' the algorithm by inputting false information. The HO simultaneously argued that the tool was not used in relation to the immigration processes we specified (including for example removal and immigration bail decisions).

185. Our FOIA complaint submitted that there is a tension underlying this dual argument – namely that an algorithm can only be 'gamed' if the information submitted is capable of shaping substantive decision-making. As such, setting out our view on how IPIC processes data was material to this argument. The ICO distinguished our submissions on the nature of the data processing from its findings on the application of the section 31(1)(e) exemption by noting that our arguments focused primarily on potential breaches of the UK GDPR and individuals' rights rather than the exemption.

186. As above at §71, we accept that IPIC is not in *stricto sensu* used to make removal decisions, determine bail conditions, and/or applications for leave to remain or enter. This

has become clear to us through a more detailed consideration of the materials disclosed further to our FOIA complaint as well as other materials available in the public domain (such as the ICIBI reports cited above). For example, as noted above – the imposition of digital reporting neither relates to the decision whether to grant immigration bail nor is it an immigration bail condition itself (by contrast it is the technology used when imposing a reporting condition). Similarly, a recommendation pertaining to voluntary return or an emergency travel document is not equivalent to a decision to impose removal directions.

187. Nevertheless, while the Decision Notice makes no findings on how IPIC processes personal data for the purposes of the UK GDPR and the DPA 2018 - it is necessary at the outset of our legal analysis to clarify the nature of its processing operations.

188. While the Decision Notice does not make any reference to the EMRT, we also address the nature of its profiling in this section.

The presence of profiling and ADM

189. In support of its conclusion that IPIC does not constitute ADM and/or profiling for the purposes of the specified immigration processes – the HO explained to the ICO, in response to the ICO's investigations into our FOI complaint, that the algorithm is not trained. But deterministic, rule-based algorithms that do not employ machine learning and training data may still constitute profiling and/or ADM. [137]

190. Indeed, the deployment of such, non-trained algorithms to make decisions is common in the immigration administration and enforcement context. For example, in Sweden the Migration Agency has automated parts of their assessment of residency and citizenship applications using in-house, rule-based algorithms.[138] The rule-based systems are used to solve questions of eligibility in citizenship, work permit and residency applications in a deterministic way.[139]

191. The Decision Notice goes on to note the HO's assertion that: "IPIC merely provides recommendations in respect of which case should be prioritised by a caseworker for action so as to progress that case towards some form of conclusion." As set out above, we have demonstrated that IPIC generates recommendations that correspond to substantive immigration enforcement decisions (albeit not those we listed in our FOIA request). For example, accepted IPIC recommendations (in relation to the Reporting and Offender Management business rules) can lead to the use of immigration detention powers. This goes

[137] See ICO guidance, 'What is automated individual decision-making and profiling?', https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#id1

[138] Ozkul, Derya. (2023). Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe, page 22, 10.13140/RG.2.2.24295.46248.

[139] Ibid, page 5.

beyond the mere progression and triaging of cases and, as addressed above, automated prioritisation of cases is frequently a feature of the IPIC business rules that is distinct from their recommendations.

192. The HO's position, as maintained throughout its response to our FOIA request and in response to the FOIA complaint (see §5 of the Decision Notice) - that IPIC does not constitute ADM or profiling altogether (notwithstanding the processes the tool is used in relation to) - is not tenable considering the evidence we have adduced in support of this complaint.

193. Regarding profiling, we refer in the first instance to §4.8 of the DPIA in which the HO accepts unequivocally that IPIC involves **profiling that could result in an outcome that produces legal effects or similarly significant effects on the individual**. While some of the text in this paragraph is redacted, the HO accepts that the processing involves the use of scoring even as it states that any scores do not predict future behaviour.

194. The HO's acknowledgement that it engages in automated profiling is dispositive of any assertion to the contrary. Nevertheless, we also refer to the definition of profiling as contained in Article 4(4) of the UK GDPR:

> "*Any form of automated processing of personal data consisting of the use of personal data to* ***evaluate certain personal aspects relating to a natural person****, in particular to* ***analyse*** *or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*."

195. The Article 29 Working Party ("WP29") *Guidelines on Automated individual decision-making and Profiling* provide helpful further clarification. These guidelines were subsequently endorsed by the European Data Protection Board ("EDPB"), which has replaced the WP29. The ICO has made clear that while not directly binding, the EDPB guidelines retain significant interpretive value.[140] The WP29 made clear that Article 4(4) refers to 'any form of automated processing' rather than 'solely' automated processing referred to in Article 22 GDPR. The processing therefore must involve an element of automation to constitute profiling but may nevertheless involve human intervention.

196. This is patently satisfied in the instant case since the algorithm automatically generates the recommendation for the decision in question. Secondly, the purpose of the processing must be to evaluate personal aspects about the data subject. The W29 made clear that evaluation should involve some form of "assessment or judgement" about a person. The **evaluation of personal aspects about the data subject** occurs through the weighting of input data such as information about offending and vulnerabilities to **assess** whether they are suitable for the relevant enforcement intervention.

[140] See for example, ICO, 'Guidance on AI and data protection', (updated 15 March 2023), https://ico.org.uk/media2/ga4lfb5d/guidance-on-ai-and-data-protection-all-2-38.pdf

197. With regard to ADM, the WP29 similarly indicates that a data controller may engage in ADM even if the processing involves human intervention. This is also reflected in the ICO's *ADM and profiling Guidance*, which notes that businesses can use automated systems to make decisions about individuals unless the processing meets the definition in Article 22(1) of the UK GDPR. The HO appears to have confused the question of whether it engaged in ADM contrary to Article 22(1) with whether its processing constituted ADM altogether (hence the position taken in response to our FOIA complaint, which is repeated in the DPIA – see for example §4.9).

198. We also note by extension that the processing of personal data by the EMRT similarly constitutes both ADM and profiling (given that the EMRT was not the subject of any findings in the Decision Notice). This is with reference to the automated harm score that evaluates input data to assess how long an individual should remain subject to GPS monitoring as well as the final recommendation as to whether a tag wearer should remain on an ankle tag or be transitioned to an NFD**. PI submits the EMRT's harm score does seek to evaluate and predict future behaviour insofar as it corresponds to an individual's risk of harm and therefore how long they should remain subject to EM (which is inherently a future-facing exercise)**.

199. For the avoidance of doubt, we do not accept that the human intervention implemented by the HO is *meaningful* as is required by Article 22 of the UK GDPR. PI's submissions below address Article 22, including the ways in which the EMRT and IPIC involve decision-making with a legal effect and/or a similar significant effect.

First Principle – Lawfulness, fairness and transparency (Art 5(1)(a)

200. The DPIA (§2.2) provides that only the general processing regime under the UK GDPR/Part 2 DPA 2018 apply to the processing of data by IPIC. The HO has failed to carry out a DPIA in relation to the EMRT, however it has stated that the functionality is aligned with IPIC and relied on the IPIC DPIA to maintain that it did not need to carry out a separate impact assessment for the EMRT. For this reason, alongside the fact that the use of the EMRT does not point to a clear law enforcement purpose, we infer that the position is the same for this tool.

201. The DPIA provides the following legal bases for processing in relation to IPIC:

a) Processing under Part 2 DPA 2018 ("General processing"): "Performance of a public task" under Article 6(1)(e) UK GDPR (para 3.2.a), with "Implied statute/power" indicated as "based on implied statute power, information and data gathering for processing is pursuant with core HO functions and the Immigration Act 1971 legislation."

b) Processing of special categories data under "General processing": the Article 9 condition for processing is "Substantial Public Interest" under Article 9(2)(g) (para 3.4.a). We note that this condition requires the processing to be "necessary" for reasons of substantial public interest, and "on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". No detail is provided in the DPIA as to how the processing complies with this latter part of Article 9(2)(g).

Lawfulness of IPIC and EMRT processing

202. **First**, the specified legal basis for processing is particularly broad and ill-defined. As set out above, IPIC and the EMRT are highly intrusive tools that re-purpose datasets, including very sensitive information, from across the immigration system to generate outputs that can have extremely adverse consequences on individuals and their fundamental rights (including for example through the exercise of detention powers).

203. In the context of the EMRT, the available disclosure suggests that the HO has not considered whether the use of this tool requires a distinct legal basis. This is evident from the decision not to carry to out a DPIA (see above at §35) and the fact that there is no reference to a consideration of the EMRT's compliance with the lawfulness principle anywhere in the exhaustive disclosure requested by Public Law Project and Duncan Lewis Solicitors. We note that this disclosure included relevant internal policies and guidance as well as training materials for caseworkers. The failure to consider the lawfulness of the EMRT is notwithstanding the distinct nature of the GPS tagging legal framework, the EMRT recommendations and the impacts the EMRT has on data subjects relative to IPIC. We consider that the failure to consider this question is both of significance to the HO's compliance with lawfulness and the accountability principle as well as the requirement to carry out a DPIA (accountability and DPIAs are addressed further below).

204. Many of the data subjects, which include children (in the case of IPIC), are likely to be vulnerable. The ICO's findings on vulnerability in the EM Enforcement Notice (§109) support this submission. The ICO found that a significant number of data subjects may be vulnerable: "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."

205. PI submits that several of these conditions are satisfied with respect to both the EMRT and IPIC. This is because there are significant overlaps in the populations subjected to GPS tracking via the Pilot and anyone whose data is processed by IPIC and the EMRT. In the case of the EMRT, the data subjects are also subject to GPS tracking (albeit as individuals tagged under the EM duty). This may itself be an indicator of vulnerability considering the established mental health impacts of tagging (which we address below).

206. Both those whose data is processed by IPIC and the EMRT will be on immigration bail. As such, they may also be vulnerable due to the conditions they left or the circumstances of their

journey. By way of illustration, from January-September 2022 – 74% of individuals referred into the National Referral Mechanism, which determines if they have been subjected to trafficking, were subject to immigration control.[141] From October – December 2024, 5,733 individuals were recognised as potential victims of trafficking and 5,234 received Conclusive Grounds decisions and were therefore recognised as victims of trafficking.[142] If, as the HO has maintained, the statistics on the number of referrals subject to immigration control has remained constant since 2017[143], then the vast majority of these individuals are likely to either be on immigration bail or in immigration detention. Even if EM Expansion Pilot cases are likely to have spent less time in the UK, many of those on immigration bail are likely to speak limited or no English and the same imbalance of power exists between IPIC and EMRT data subjects and the HO.

207. Moreover, as addressed below, IPIC is likely to result in discrimination given that the functionality of the tool incorporates prioritisation and filtering features that will result in certain nationalities being targeted for immigration enforcement interventions.

208. As per the ICO's *Guidance on Lawful Basis*, the UK GDPR requires that a public task basis have a clear basis in law and be necessary and proportionate with regard to the aim pursued.[144] This applies to any task involving data processing that falls within the Article 6(1)(e) lawful basis. A public authority must pay particular heed to these principles in circumstances where processing is intrusive and may result in adverse consequences for subjects.

The clarity and foreseeability of the legal basis

209. With respect to the necessary quality of the legal basis in national law, Recital 41 to the UK GDPR clarifies that the application of the law must be clear, precise and foreseeable. PI submits that the stated basis in national law - the implied power in the Immigration Act 1971 for information and data gathering purposes - does not meet any of these requirements.

[141] Home Office, 'Annex: analysis of modern slavery NRM referrals from asylum, small boats and detention cohorts', (updated 11 July 2024), https://www.gov.uk/government/statistics/modern-slavery-national-referral-mechanism-and-duty-to-notify-statistics-uk-january-to-march-2023/annex-analysis-of-modern-slavery-nrm-referrals-from-asylum-small-boats-and-detention-cohorts#how-many-people-entering-the-nrm-are-subject-to-immigration-controls

[142] Home Office, 'Modern slavery: National Referral Mechanism and Duty to Notify statistics UK, quarter 4 2024 - October to December', (6 March 2025), https://www.gov.uk/government/statistics/modern-slavery-nrm-and-dtn-statistics-october-to-december-2024/modern-slavery-national-referral-mechanism-and-duty-to-notify-statistics-uk-quarter-4-2024-october-to-december

[143] Home Office, 'Annex: analysis of modern slavery NRM referrals from asylum, small boats and detention cohorts', supra note 125.

[144] ICO, UK GDPR guidance and resources, 'a guide to legal basis, public task', https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/public-task/

210. Information gathering in line with core functions under implied immigration powers is so broad that it encompasses the entirety of the HO's data processing. Moreover, the stated implied power is not consistent with how IPIC is used. The primary purpose of the tool is to determine suitable cases for immigration enforcement operations, which goes beyond information gathering insofar as it requires an element of evaluative analysis and judgement (see the section on profiling above). We submit that while a legal basis in national law need not describe all relevant processing operations relating to the public task, it must correspond to the processing carried out by the public authority. This submission is supported by the approaches taken by national courts when interpreting the GDPR. For example, the Austrian Federal Administrative Court ("BVwG") found profiling by a public authority in relation to jobseekers to be lawful under Articles 6(1)(e) and 9(2)(g) GDPR on the basis that the enabling legislation expressly included the data types that the authority processes about jobseekers.[145] For these reasons the application of the law is not sufficiently clear, precise and foreseeable.

211. As noted above, with regard to the EMRT - the HO has failed to demonstrate how it has considered the question of lawfulness, including the requisite grounding in national law for the Article 6(1)(e) lawful basis. PI submits that reliance on implied powers within the Immigration Act 1971 would not meet this requirement. This is because the use of GPS tracking is governed by a different legal framework – namely Schedule 10 to the Immigration Act 2016. Moreover, even if the HO were to maintain that it deployed the EMRT under implied data gathering powers within the Immigration Act 2016 – this would also not be an adequate grounding for use of intrusive and highly data intensive processing. This is for the same reasons as advanced above at §203 in relation to IPIC.

212. There is a convergence between the requirements that must be met when processing data via the public task basis and the jurisprudence of the European Court of Human Rights ("ECtHR") regarding the right to privacy that further underlines our submission.[146] In particular, for a measure to be in accordance with the law for the purposes of Article 8 ECHR - it must have "some basis in domestic law," and it must be "compatible with the rule of law," which means that it **should comply with the twin requirements of "accessibility" and "foreseeability"**, and it must contain sufficient constraints against arbitrary or disproportionate use (e.g. *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 5037 (CA) [80]).

213. The principle of "foreseeability" means that the domestic legal framework (which includes a public authority's published policies) must "give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are entitled to resort to measures affecting their rights under the Convention" (*Fernandez Martínez v Spain*

[145] Barros Vale, Sebastião and Zanfir-Fortuna, Gabriela, 'Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities', (May 2022), page 16, https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf

[146] See for example, Ireland Data Protection Commission, 'Guidance Note: Legal Bases for Processing Personal Data', (December 2019), pages 18-20, https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf

(2015) 60 EHRR 3 [GC], [117]; see also *Big Brother Watch & ors v UK* (2022) 74 EHRR 17 [GC], [333]). Further, that legal framework "must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise" (*S & Marper* v UK, [95]).

214. The need for safeguards is greater where, as in this case, the personal information in question is subject to **automatic processing** (*S & Marper v UK,* [103]) and the "powers vested in the state are obscure" creating "a risk of arbitrariness especially where the technology available is continually becoming more sophisticated" (*Catt v UK,* [114]).

215. Both IPIC and the EMRT lack a legal framework that would satisfy the requirements of accessibility and foreseeability.

216. There is nothing in the public domain which gives people who may be affected any indication of the circumstances in which: (a) the HO will use IPIC when exercising immigration powers; (b) what consequences an IPIC recommendation can have; and (c) what personal data will be processed by the tool. Notably, there is no public guidance on how IPIC is used (and any published policies that do refer to particular immigration functions in which we have established IPIC is used make no reference to it). As is addressed below, there is also no information provided to data subjects either directly through a privacy notice or indirectly through publicly available privacy information.

217. In the case of the EMRT, some of the above information is provided to data subjects by way of the Immigration Bail policy and correspondence citing use of the tool as in the case of the letter provided by Wilson Solicitors. However, this information is inconsistent and contradictory in several different ways.

218. Firstly, the HO has stated in FOIA correspondence that use of the tool ceased in August 2023. By contrast, the letter received by a client of Wilson Solicitors refers to the tool generating a decision recommendation in 2024[147]. We note that references to the tool in correspondence across individual cases are also uneven. For example, in *Nelson v Secretary of State for the Home Department* – the HO denied that the EMRT was used at all in the Claimant's case (the Claimant being fitted with a GPS tag on May 2022.[148]

219. Second, the current iteration of the Immigration Bail policy continues to refer to the possibility of using automated business rules including in EM reviews and in determinations whether to impose EM altogether (which is not stated anywhere else including in the training

[147] Annex III - Home Office Response Letter to Wilson Solicitors Client Transition to NFD -Redacted.

[148] *R (Nelson) v Secretary of State for the Home Department* [2024] UKUT 00141 §45.

materials).[149] This is inconsistent with the STS PIN, which denies that any form of ADM is in use (and which does not refer to the use of the EMRT or automated business rules).[150]

Other breaches of the lawfulness principle

220. **Second**, the uses of IPIC and the EMRT are thus in breach of Article 8 of the ECHR. This is because interferences with the rights protected by Article 8(1) ECHR will be unlawful where they are not in accordance with the law (addressed above). Establishing an interference with the right to privacy is a low threshold. The ECtHR has previously held where there is a compilation of data on a particular individual beyond that normally foreseeable, the right to privacy is engaged.[151] We submit that these requirements are satisfied on these facts given the significant volume of data processed by IPIC and the EMRT and their role in decision-making, such as detentions, removals and the use of EM, which may in their own right result in serious interferences with Article 8.

221. An Article 6(1)(e) legal basis that is more broadly contrary to the law (in this case the right to privacy) itself constitutes a discrete breach of the lawfulness principle.[152]

Necessity and proportionality

222. **Third**, the HO has failed to carry out a necessity and proportionality assessment when deploying IPIC either in the DPIA or elsewhere. This is also the case for the EMRT for which no DPIA has been prepared at all. As per the EM Enforcement Notice, failing to carry out a necessity and proportionality assessment may be incompatible with the accountability principle (addressed below). PI submits that by failing to turn its mind to the question of necessity and proportionality the HO cannot assert that processing data through the tools complies with these principles.

223. This is because controllers relying upon the public task legal basis need to ensure that the processing of the personal data of the data subject must actually be necessary to carry out the task in the public interest or exercise of official authority. For processing to be necessary to carry out the task, it must be **a targeted, reasonable, and proportionate** way of doing so.

[149] Home Office, 'Immigration bail', version 22.0, (12 June 2025), p. 48. states "Where the EM duty applies, the decision maker may have access to a decision support tool which utilises automated business rules to provide decision recommendations for the decision maker to consider alongside the guidance set out in Use of EM and EM and linked supplementary conditions: Review."

[150] The Bespoke STS PIN states in p. 1. "There is no Automated Decision Making involved in this or any 'review' process final decision." See WhatDoTheyKnow, 'Privacy International request to Home Office', (23 May 2024), https://www.whatdotheyknow.com/request/information_included_in_the_icos#incoming-2675479

[151] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Application no. 931/13, ECtHR, 27 June 2017.

[152] See for example, *Elgizouli v Secretary of State for the Home Department* [2020] UKSC 10 §153.

224. As above, the identified purpose for IPIC (information gathering) is an inadequate ground for the processing the HO carries out given its breadth and the fact that it is inconsistent with the actual role and function of the tool. The HO has appeared to fail to consider what the relevant purpose would be with respect to the EMRT; however, reliance on the purpose referenced in the IPIC DPIA would suffer from the same defect. Nevertheless, even if the purpose were to be assisting decision-making in the context of immigration enforcement operations, then the processing is unnecessary and disproportionate for the following reasons:

a) There is no possibility to limit cases in which the tools are used. Instead, the training materials for the various IPIC business rules and for the EMRT demonstrate that all cases which satisfy the relevant rule are subject to it. This is seen, for example, with respect to the EUSS business rules, which is used in relation to **failed EUSS cases that meet the criteria of the relevant business rules**. [153] Moreover, during the period in which the HO acknowledges that the EMRT was used, this was also deployed in reviews relating to all EM duty cases. [154] There is no consideration as to whether there may be cases, which due to their particular complexity, are not suitable to tools that limits the scope of human consideration and review (see below where we address the lack of meaningful human review). Similarly, there is no means to ensure that cases where individuals are particularly vulnerable, such as children, are not subjected to ADM through IPIC. This would mitigate the risk of inaccurate and/or unlawful decision-making with potentially catastrophic consequences for data subjects. We note that a selective approach of limiting the use of ADM tools (including in more complex cases) is exactly how the Swedish example cited above at §191 functions. Where the question or the answer cannot be categorised using binaries, the decision-making is devolved to a human caseworker without use of the tool.[155]

b) There appears to be no mechanism to limit the volume and categories of personal data that IPIC and the EMRT can process when generating their outputs. This is with reference to the input data set out in the DPIA (§2.1) and outlined above. The DPIA does not indicate any limitation of the extensive input data, including special categories information such as health data (addressed below), to what is necessary to achieve the relevant purpose. For example, it is unclear why special categories information relating to an individual's vulnerabilities is needed when the tool determines if they are suitable for a referral to another government department through the ISD business rules. Similarly, the retention of recommendations for a period of at least 5 years to enable the HO to search through them is unnecessary and disproportionate particularly where an individual is granted leave to remain or has left the UK (we note that this is also relevant to the storage limitation principle, which is addressed below).

[153] Annex VII: Immigration Enforcement, 'IE Business Rules (IEBR) Identify & Prioritise Immigration Cases (, IPIC) Reference Manual EUSS Training Guide – EUSS Cases' v01 Redacted.

[154] See above §§129 -131; Also see Home Office, 'Immigration bail' (Version 22.0) (12 JuneBail Policy', (31 January 2025), page 48, https://assets.publishing.service.gov.uk/media/68514c37f2ccfcfd2f823f5b/Immigration+bail.pdf

[155] Ozkul, Derya. (2023). Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe, page 22, 10.13140/RG.2.2.24295.46248.

c) In the case of the EMRT, it is unclear how the tool can be necessary and thus why the Immigration Bail policy continues to permit it to be used if the HO accepted that its use did not result in added efficiencies. As set out above, this is stated by the HO in FOIA correspondence dated 22 August 2024 in which it explained that the tool was withdrawn because it "failed to provide the efficiencies envisaged". Any continued processing using the EMRT is therefore not necessary as a less intrusive viable alternative exists (human decision-making) which achieves the same or a similar result. If the tool has indeed been withdrawn (if the Immigration Bail policy is inaccurate) then this admission may also indicate that the HO failed to adequately conduct an assessment of the EMRT's true necessity and proportionality. Given that the basis for the EMRT's use was increased efficiency rather than necessity, and that the EMRT has seemingly not been replaced by an alternative decision tool solution[156], out of necessity, the HO may not have adequately determined whether the pre-existing, less intrusive approach (of human decision-making) was always viable and the processing via the EMRT was unnecessary.

225. PI notes that neither of the submissions put forward above at §225(a) and (b) regarding IPIC would unduly limit any intended efficiencies the HO seeks to achieve using automatic processing tools while also ensuring that personal data is not processed where there is a more reasonable and proportionate, and **less intrusive way** to achieve the purpose. While not binding on the UK, this is consistent with the European Court of Justice's ("CJEU") finding in *Schecke, Eifert v Hessen*. The Court found that to comply with necessity a controller must consider alternative, less intrusive measures; any interference with data protection rights must be the least restrictive of those rights; and there ought to be no equally effective available processing alternative.[157]

Special categories information

226. **Finally**, processing special categories data requires a controller to meet an Article 9 condition alongside the Article 6 legal basis. As above, the HO has failed to provide any detail on why the Article 9(2)(g) condition is met. This is true for both IPIC and the EMRT (given the failure to complete a DPIA altogether). The HO fails to meet the Article 9 condition for two reasons. Firstly, the processing is not proportionate to the aim pursued (for the reasons outlined above). Secondly, the processing fails to provide "suitable and specific measures to safeguard the fundamental rights and the interests of data subjects", because:

a) The scope of the special categories processing is insufficiently clear from the DPIA and other documents the HO uses to set out how the tool functions, including what data it

[156] See the Home Office's response to Q5 in their FOIA correspondence of 9 September 2024: https://www.whatdotheyknow.com/request/clarification_regarding_uses_of/response/2755268/attach/3/06268%20Privacy%20International%20supplementary%20response.pdf?cookie_passthrough=1https://www.whatdotheyknow.com/request/clarification_regarding_uses_of/response/2755268/attach/3/06268%20Privacy%20International%20supplementary%20response.pdf?cookie_passthrough=1

[157] CJEU, Joined Cases C 92/09 and C 93/09, Schecke, Eifert v Hessen, 9 November 2010, § 86.

processes. This submission is linked to the arguments we make above regarding the quality of the legal basis the HO seeks to rely on but relates to special categories data specifically. While the HO acknowledges that IPIC processes health, biometric, criminal conviction and ethnic origin data – the input data also include other information that may reveal special categories data. For example, the DPIA states that IPIC processes "EM data". If this includes locational data (referred to by the HO as "trail data") then other special categories information may be inferred from it. We note that this something that the HO accepts in its amended September 2024 Privacy Information Notice relating to the EM Expansion Pilot (the "Pilot PIN").[158] As set out in our complaint regarding the HO's use of GPS tracking, such inferred special categories data could include highly sensitive information about an individual's sexual orientation, political opinions, religious, philosophical, societal or other beliefs.[159] Similarly, the Immigration Bail policy and the EMRT training materials are silent on the role of trail data and any data inferred from such information. This is particularly concerning given the prominent role that data about compliance with EM conditions (and other bail conditions) plays in the outputs generated by the tool.

b) There is no provision of information to data subjects about how their special categories information is used by both IPIC and the EMRT. This in turn increases the risk of unlawful data processing as the lack of transparency leaves data subjects with no effective remedy to challenge abusive processing (we address transparency in detail below). As recognised in the Recitals to the UK GDPR and the *ICO's Lawful basis for processing: Special category data* guidance, the purpose of the heightened protections afforded to special categories data is that the use of such information can create substantial risks for fundamental rights and freedoms. The use of special categories data by IPIC and the EMRT presents exactly such risks. For example, the HO acknowledges that it uses the tool to filter cases based on nationality to select suitable cases for deportation charter flights. As per its EIA, there is a risk that this may result in direct discrimination.

227. Notably, the HO's Appropriate Policy Document (the "APD"), which regulates the entirety of the department's special categories processing merely states that processing will always be proportionate and necessary without providing further detail.

228. With regards to the lawfulness principle, the only additional information provided in the APD concerns the provision of data protection training. The APD states that all HO staff will undertake data protection training, but this appears to be broad and generic. There is no

[158] Home Office, 'Satellite Tracking Services Privacy Information Notice (PIN), GPS Tagging Expansion Pilot', (September 2024), https://www.whatdotheyknow.com/request/information_included_in_the_icos/response/2872820/attach/6/05693%20Annex%20V%20GPS%20Pilot%20PIN%20Sep%2024.pdf?cookie_passthrough=1

[159] Privacy International, 'Submission to the Information Commissioner – Request for Assessment of Processing Operations by the Secretary of State for the Home Department ("Home Office")', (17 August 2022), https://privacyinternational.org/sites/default/files/2022-08/2022.08.17%20-%20Privacy%20International%20complaint%20against%20Home%20Office%20use%20of%20GPS%20Ankle%20Tags%20[public%20version].pdf

reference to training relating to IPIC and/or the EMRT; instead, the APD refers to additional training for those involved in data processing. Much of this training appears to be optional and relates to the assessment of necessity and proportionality. It also refers to training on case-by-case lawfulness assessments such as when considering Mutual Legal Assistance (MLA) requests by the UKCA.

229. None of this assists the HO in demonstrating that use of IPIC and the EMRT comply with the lawfulness principle. This is because IPIC and the EMRT do not incorporate a case-by-case lawfulness and proportionality/necessity analysis, instead they are used in all cases that fall within the relevant business rules on the presumption that these requirements are already satisfied. The APD also fails to provide any information on what measures are taken to safeguard fundamental rights and freedoms of data subjects in line with Article 9 of the UK GDPR and Schedule 1 of the DPA 2018.

Fairness and reasonable expectations

230. The principle of fairness in Article 5(1)(a) UK GDPR is central to data protection law. PI supports and adopts the ICO's definition and interpretation of fairness, described on its website as follows: "In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them."[160]

231. The adverse impacts on the data subjects are evident. In the case of the EMRT, there is a real risk that the tool systematically profiles subjects in ways that continue to subject them to 24/7 GPS tracking (either by way of ankle devices or NFDs) notwithstanding vulnerabilities that may make the use of such intrusive tracking technology disproportionate, all potentially without their knowledge.

232. Organisations such as the Public Law Project and Bail for Immigration Detainees have documented the impacts of tagging on migrants. These impacts include constant fear that their movements may trigger a breach alert, anxiety about the tag's battery charge levels when they go out and away from a mains power supply, uncertainty about the interpretation of their movements for purposes of assessing Article 8 representations or suffering of social stigma.[161]

233. The EIA completed for the HO's introduction of the NFDs indicates that these devices are considered to mitigate multiple adverse impacts that ankle tags may have on tag wearers.

[160] ICO, 'Guide to the General Data Protection Regulation (UK GDPR) – Principle (a): Lawfulness, fairness and transparency', (updated January 2025), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

[161] Rudy Schulkind, Woodren Brade, Jo Hynes, Dr Kathryn Allinson, 'Research reveals "inhumane" effects of GPS tagging on migrants', Public Law Project, (31 October 2022), https://publiclawproject.org.uk/resources/research-reveals-inhumane-effects-of-gps-tagging-on-migrants/

These include mental health conditions exacerbated or caused by the use of an ankle tag.[162] However, the EIA fails to engage with detrimental impacts on data subjects through the use of NFDs. These include anxiety and uncertainty caused by the randomness of alerts as well as the associated constant requirement to provide one's fingerprints, which contributes to people feeling as though they are "in a constant state of alertness and in a heightened sense of being under constant surveillance".[163] Research undertaken by other civil society organisations shows, through anonymised interviews, that this in turn impacts the enjoyment of basic everyday activities - such as being able to sleep properly. Subjects also reported that having too little time (e.g., 1 minute) to provide their fingerprints contributed to the feelings of anxiety and stress they felt.[164]

234. As above, the use of IPIC may result in wholly opaque profiling directly linked to the exercise of powers such as removal and detention as well as hostile environment sanctions. As per an extract from a previous evaluation of IPIC carried out by the HO (disclosed to Public Law Project in response to a 2021 FOIA request and referred to above at §18), use of the tool resulted in an increase in the number of cases accepted for the intervention in question (versus previous HO processes).[165] As such, there is a risk that individuals flagged for a recommendation (including through the automated filtering processes) are more likely to have enforcement action taken against them.

235. Core to fairness is that the data processing should be in line with individuals' reasonable expectations. Reasonable expectation of privacy is also a key principle in jurisprudence of the ECtHR, where it is used to assess whether there has been an interference with an individual's private life under Article 8 of the ECHR. The ECtHR has on several occasions investigated whether individuals "had a reasonable expectation that their privacy would be respected and protected".[166]

236. PI submits that the ways in which the EMRT and IPIC are used generally falls outside of data subjects' reasonable expectations.

[162] UK Visas and Immigration, 'Guidance Equality impact assessment: GPS non-fitted devices', (updated 15 April 2025), https://www.gov.uk/government/publications/offender-management/equality-impact-assessment-gps-non-fitted-devices-accessible

[163] Dr Jo Hynes, ''Constantly on Edge': The expansion of GPS tagging and the rollout of non-fitted devices', Public Law Project, (20 December 2023), https://publiclawproject.org.uk/resources/constantly-on-edge-annual-review-of-gps-tagging-in-the-immigration-system-2023/

[164] Privacy International, Long Read, 'Non-fitted devices in the Home Office's surveillance arsenal: Investigating the technology behind GPS fingerprint scanners', (29th October 2024), https://privacyinternational.org/long-read/5457/non-fitted-devices-home-offices-surveillance-arsenal-investigating-technology-behind

[165] Home Office, *untitled document,* https://www.whatdotheyknow.com/request/triage_tools_used_in_an_immigrat/response/2002033/attach/5/68562%20Kazim%20Annex%20E%20Evaluation%20Background%20and%20Summary%20Redacted.pdf?cookie_passthrough=1

[166] *Barbulescu v. Romania* [GC] App no 1496/08 (ECtHR, 5 September 2017), §73.

237. With respect to the EMRT, we rely on the fact that data subjects have a reasonable expectation that quarterly EM review decisions are undertaken by a human whose review would consider the appropriateness of GPS tracking as a whole. This is consistent with the Immigration Bail policy and the duty on the part of the HO not to impose EM where to do so would be impractical/in breach of rights under the ECHR (see §§234-235 of *ADL and Others v Secretary of State for the Home Department*).[167]

238. However, processing through the EMRT is not aligned with this expectation. Instead, the tool is designed in a way that only allows the reviewer to accept or reject a recommendation to maintain an individual on an ankle tag or 'de-escalate' them to an NFD. The wording of the EM review form pro forma indicates that a consideration of proportionality is included in the assessment conducted by the tool and there is no clear means for a caseworker to assess whether EM as a whole remains appropriate (versus whether an individual should be moved to an NFD). These 'design nudges' include the fact that there is no EM review pro forma that corresponds to the removal of an EM condition (there is only a pro forma for decisions to maintain an ankle tag, maintain an NFD or transition a wearer from an ankle tag to an NFD). There is also no guidance on how to substitute the pro forma review forms (including the automatically generated text) or conduct any proportionality assessment outside the confines of the tool's recommendations (which as above maintain EM in any event).

239. Even more concerningly, the automatically generated harm score determines the total length of time that an individual remains subject to both an ankle tag and an NFD. Human involvement in the harm score, as demonstrated by our consideration of the training materials set out above, is limited to inputting information into the tool and checking if the minimum amount of time relative to an individual's harm tier has expired (as set out in the table provided in the training materials and the immigration bail policy) before transitioning them to an NFD.

240. The **unjustified adverse effects** on data subjects stemming from this approach is indicated by statistics obtained by the Public Law Project relating to outcomes of EM reviews. This demonstrates that between 22 May 2023 and 14 August 2023 (during which the HO has stated that it used the EMRT in all cases) 1,768 quarterly EM Reviews were carried out – of which: 16 resulted in EM being ceased; 1,542 resulted in EM being maintained via an ankle tag; and 210 resulted in EM being varied from a fitted device to an NFD.[168] We address the implications of deficient review below, however it is worth noting that during this period only **0.9%** of quarterly reviews resulted in the withdrawal of EM.

241. PI also wishes to highlight the significance of the unpublished policy revealed through the FOIA request submitted by DL. This sets out the data that the EMRT considers when assessing

[167] *ADL and others v Secretary of State for the Home Department* [2024] EWHC 994 (Admin).

[168] WhatDoTheyKnow, 'Response to Jo Hynes request to Home Office', (10 September 2023), https://www.whatdotheyknow.com/request/reviews_of_decisions_to_impose_g/response/2422269/attach/3/78221%20Hynes.pdf?cookie_passthrough=1

an individual's compliance with their immigration bail conditions. The unpublished guidance seems to indicate that the HO is operating an unpublished policy where certain periods of time in which an individual's tag is out of contact ("OOC") are automatically treated as a breach of bail conditions. There is no mention of the 'breach thresholds' that will be considered by the tool in the Immigration Bail policy or in the privacy information provided to tag wearers.

242. This is antithetical to the fairness requirement since a data subject will not know when the tool treats them as having breached their bail conditions. As such, they will be unable to make representations (or know to do so), which may in turn result in a longer period of EM (and in particular a longer period subject to an ankle tag). The lack of clarity around how breach data will be treated is exacerbated by the Immigration Bail policy, which only covers breaches of digital reporting (notwithstanding the fact that tag wearers may report in-person). As above at §154, the EMRT training materials indicate that there is a redacted "allowable number" of missed reporting dates for each automatically generated harm tier across the most recent 3-month period.[169] This contrasts with the Immigration Bail policy, which suggests that a failure to acknowledge a digital reporting message may constitute a breach of bail.[170]

243. The failure to afford tag wearers the opportunity to make representations in relation to potential bail breaches has been commented on by the ICIBI: "Many of the breaches received were not processed or reviewed and so risks associated with non-compliance would not be considered. One of the other impacts of this was that individuals who had breached their EM bail conditions, for whatever reason, would not have the opportunity to provide mitigation close to the time of the breach."[171]

244. The fact that tag wearers cannot make representations in relation to the tool's processing of breach data may result in determinations that an individual has breached their bail conditions when in fact they may have a legitimate explanation. We refer to the systemic faults in GPS tags issues by the HO. The ICIBI, in the same report, found that: "instances of faults in December were exceptionally high across the whole of the MOJ contract, with 1,195 devices returned, which included "907 SOLO [EM devices]" which "[Capita EMS] had to recall and return due to a charging fault which all had to go back for repair".[172] In *Nelson*, the Applicant's tag was OOC for a period of approximately 6 months without any fault of his

[169] Annex XIV - EM Review Tool Training Materials, page 16, together with Annex XV - EM Review Tool Training Materials 2023.

[170] Home Office, 'Immigration Bail Policy', (31 January 2025), page 26.

[171] ICIBI, 'An inspection of the global positioning system (GPS) electronic monitoring of foreign national offenders (March – April 2022), §5.82, https://assets.publishing.service.gov.uk/media/62c691cd8fa8f54e8bf2fcd0/An_inspection_of_the_global_positioning_system__GPS__electronic_monitoring_of_foreign_national_offenders_March___April_2022.pdf

[172] Ibid, §5.72.

own.[173] We note that automation around breach decision-making also has implications for Article 22 of the UK GDPR, which we address further below.

245. In the case of IPIC, there cannot be said to be a reasonable expectation that individuals' data, including highly sensitive information, will be used to generate recommendations as regards the use of detention and removal powers, bail powers and hostile environment sanctions. This is with reference to the lack of any information provided to data subjects, the absence of information included in relevant policies and guidance published by the HO and the misleading information provided in the department's privacy information. For example, the HO PIN suggests that the data of previous applicants might be used to develop tools that allow the HO to process applications in a particular way. Not only is this information overly broad it might give previous applicants the impression that their data is being used to develop ADM tools. We note that none of the IPIC interventions relate to the consideration of immigration applications and nor do the business rules (to PI's knowledge) process the data of previous applicants.

246. Moreover, the clear design nudges implemented across IPIC's recommendations are also incompatible with the fairness requirement. There is no clear and adequate justification for requiring caseworkers to provide an answer when rejecting a recommendation, but not when accepting one. This is despite the fact that accepting a recommendation is likely to have an adverse impact on a data subject, which should result in heightened scrutiny. In the same way, permitting caseworkers longer to change rejected recommendations versus accepted ones disincentivises adequate scrutiny during human review, which is required to ensure fair processing in a context where the fundamental rights and freedoms of data subjects is at stake.

247. Overall, the approaches taken by the HO are inimical to the fairness criteria identified by the EDPB in its data protection by design and default guidelines. These state that any processing of data – including cases of profiling and ADM such as the ones at stake – must be non-discriminatory, ethical and transparent, and consider power and informational imbalances.[174] While not directly binding on the UK, this remains in line with the ICO's approach and is a useful reference point for interpreting the fairness requirement in practice.

Transparency

[173] Matrix Chambers, 'Upper Tribunal Gives Judgment in First Challenge to Home Office Policy of GPS Tagging Migrants', (13 March 2024), https://www.matrixlaw.co.uk/news/upper-tribunal-gives-judgment-in-first-challenge-to-home-office-policy-of-gps-tagging-migrants/ ; See for further details around the deficiencies in the functioning of GPS tags, Privacy International, 'Challenge to systemic quality failures of GPS tags submitted to Forensic Science Regulator', (17 August 2022), https://privacyinternational.org/advocacy/4940/challenge-systemic-quality-failures-gps-tags-submitted-forensic-science-regulator

[174] EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, version 2.0, (20 October 2020), p. 18.

248. As we have seen, fairness is also directly affected by the level of transparency provided around this processing: "Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data."[175]

249. It is noted that transparency is not only a stand-alone requirement pursuant to the lawfulness principle (Article 5(1)(a)), but it also requires compliance with Articles 12 and 13 of the UK GDPR. In this section, we will demonstrate how both IPIC and the EMRT fail to comply with Articles 5(1)(a) and the discrete requirements of Articles 12 and 13 (save for the specific transparency provisions regarding solely ADM, which is dealt with further below). We will address both the Article 5 requirements and those set out at Article 13 in the context of the potential application of the immigration exemption contained in the Data Protection Act 2018 schedule 2, paragraph 4.

250. Informed by legal representatives of individuals who may have been subjected to IPIC and the EMRT as well as our research, it appears data subjects are either not provided with any information about how their data is processed or the information is inadequate and potentially misleading:

a) IPIC: no information is provided at all to data subjects concerning how their data is processed by the tool. This includes a lack of information provided in the HO PIN (or other privacy information), which as above is wholly silent on the processing that IPIC involves. There is likewise a failure to publish any information on the IPIC business rules either by way of a discrete published policy or references in other existing policies regarding decision-making processes in which the algorithm is used.

b) EMRT: despite stating that the tool was used in all cases, information provided to tag wearers appears to be uneven and inconsistent. Moreover, the privacy information provided to tag wearers (in the form of both the EM Handbook and the STS PIN), which are dated during the period the HO acknowledges the EMRT was used, provide erroneous and therefore potentially misleading information. There is no reference across the HO's privacy information to either the EMRT or any other support tool. Both the STS PIN and the Handbook state in unequivocal terms that no ADM is in use in the initial decision to impose EM or during the reviews.[176] For the reasons set out above, we do not accept that the processing does not constitute profiling and/or ADM (which has been the HO's position as far as IPIC is concerned). Finally, the Immigration Bail policy does refer to the use of automated business rules and suggests that they can be used in initial EM decisions,

[175] ICO, 'Guide to the General Data Protection Regulation (UK GDPR) – Principle (a): Lawfulness, fairness and transparency', https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

[176] The Bespoke STS PIN at p. 1 and the Electronic Monitoring Services Handbook at p. 6. Both state that "There is no Automated Decision Making involved in this or any 'review' process final decision." See WhatDoTheyKnow, 'Privacy International request to Home Office', (23 May 2024), https://www.whatdotheyknow.com/request/information_included_in_the_icos#incoming-2675479

or consider moving an electronically monitored person between a fitted device, a non-fitted device and no device.[177] This is not repeated elsewhere.

251. With regard to IPIC, the DPIA states at §2.6 that data subjects would not be informed of processing as there was no requirement to do so. The only provision of information would come through the HO PIN, the contents of which are summarised above.

252. This is incompatible with the transparency principle, which as per the WP29's *Guidelines on Transparency*, requires that data subjects are "able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used."[178] This was said to be particularly important where, as in the instant case, the processing is particularly complex, technical or unexpected. In such circumstances, controllers must spell out in unambiguous language what the most important consequences of the processing will be. In this sense, the transparency requirement intersects with fairness since data subjects must be able to verify the accuracy and lawfulness of the controller's processing.

253. Considering the multiple inconsistencies relating to the EMRT's processing of data, including the statement that the tool is purportedly no longer used, notwithstanding evidence to the contrary, the EMRT similarly breaches the transparency principle.

254. PI also submits that both tools are in breach of Article 12(1) of the UK GDPR for the following reasons:

a) IPIC: the HO has failed to provide data subjects with information relating to processing that is "concise, transparent, intelligible and easily accessible". As above, the language in the HO PIN is overly broad. The HO PIN's section which addresses ADM and profiling is equally vague, it states "Parts of our processing may involve degrees of automation, but complex or adverse decisions will always be taken by a trained officer or caseworker". It goes on to state that personal information may be used "to develop tools that allow us to assess and then process applications in a particular way." This wording provides little indication of how IPIC is operating and may be misleading. It arguably gives the impression that where ADM and profiling are used, it is only in relation to procedures in which a data subject actively applies (namely those applications that confer immigration status), which is not the case at least in respect of IPIC (and the EMRT). If the HO has not added any information into the HO PIN regarding IPIC on the incorrect basis that IPIC does not constitute profiling or ADM, the HO has nonetheless failed to put its mind to the requirements of Article 12(1). We would expect the HO PIN to acknowledge IPIC's existence and describe how the use of IPIC is processing personal data, at least by reference to the various business rules.

[177] Home Office, 'Immigration bail', version 22.0, (12 June 2025), p. 48.

[178] Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679', 17/EN, WP260 rev.01, (11 April 2018), https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf

This is a potential omission which will be addressed through the prism of the accountability principle below.

b) EMRT: PI submits that the EMRT breaches the same aspects of Article 12(1) as IPIC. However, it does so, because (1) relevant privacy information is spread out over a number of documents and should be provided in one place; and (2) the information provided is likewise contradictory and potentially misleading.

255. Both tools also breach several provisions in Article 13 of the UK GDPR.

256. **First**, the HO has failed to set out the purposes of the processing. When Article 13(1)(c) is read together with the transparency principle as enshrined in Article 5(1)(a), we consider that the requirement to disclose the purpose of processing requires the HO to explain broadly what the recommendations generated by the tools are. This is because the nature of the recommendation (i.e. a recommendation that individual be subject to a digital reporting condition) is necessary to explain why the tool has been used. Any broader explanation prevents a data subject from understanding how their data is being processed and more specifically what the scope and consequences of processing are, as required by the transparency principle.

257. **Second**, the HO has failed to provide data subjects with information about how long their information will be stored in accordance with Article 13(2)(a). The HO's PIN states the following about retention periods for certain forms of personal data:

> "*Personal data will be typically retained for* ***25 years after a decision to grant settlement or naturalisation*** *and* ***for 15 years after the last action in other cases****. Information on foreign national offenders may be retained until the death of the data subject****. At the border, passenger name records data is retained for up to 5 years****.* ***Advance passenger information may be retained for 10 years****.* ***Arrest and detention records may be held for 6 years****. We continue to keep retention periods under review to ensure they meet our role of securing the UK border and ensuring we can support those who are seeking to enter or remain in the UK*."

258. There is no reference to the retention of IPIC data, notwithstanding the fact that recommendations generated by the tool are retained for a period of at least 5 years (as set out above). Given the granularity of detail provided regarding the retention periods set out above, there is no reason the HO could not do the same in relation to the retention of IPIC data.

259. Given that there is no DPIA for the EMRT, it is unclear what data processed by the tool is retained and for how long. If the recommendations and harm scores generated the EMRT are likewise retained for a minimum of 5 years, then this information should also be provided to data subjects.

260. The failure to provide this information for both the EMRT and IPIC once again inhibits data subjects from understanding what happens with their information and in turn verifying its accuracy and lawfulness.

261. It is noted that the UK GDPR is not prescriptive as regards how transparency information should be provided. As such, the requisite information could be provided by way of discrete privacy notices or incorporated into existing privacy information (for example the HO PIN and the STS PIN). The HO would, however, have to consider the vulnerabilities of data subjects (such as whether data subjects include children) when determining how to provide privacy information (this is addressed in the context of the accountability principle below).

262. Finally, we note that the HO may apply the immigration exemption to restrict transparency information provided pursuant to Articles 5(1)(a) and 13 of the UK GDPR. The starting point for any analysis of the exemption regime is that derogations or limitations on data protection rights are to be interpreted strictly.[179] In accordance with the ICO's *Guide on the Immigration Exemption* - the exemption can only be applied if the exercise of the rights in question would be likely to prejudice the maintenance of effective immigration control or the investigation or detection of activities which in turn would undermine the maintenance of effective immigration control.

263. Moreover, the exemption must be applied on a case-by-case basis so that the HO must make a separate decision each time it restricts data protection rights. This decision must consider all the circumstances of the case including any potential vulnerability of the person, and the impact it will have on their rights and freedoms. This assessment is a delicate balancing act, and the HO is only able to impose the exemption where it is satisfied that the risks to immigration control are substantial and outweigh the risks to a person's interests, including their fundamental rights. Finally, any application of the exemption must be necessary and proportionate.

264. As a matter of procedure, the HO must record any decision to use the exemption and the reasons for imposing it. The HO is also required to inform the person of the decision, unless doing so would prejudice immigration matters.

265. In the DPIA concerning IPIC, the HO states that there is no need to provide any information to data subjects on the erroneous basis that there is no legal obligation to do so (addressed above) and when:

> "*… Processing data on certain categories of individuals such as illegal migrants or a FNO, it may not be appropriate to notify them that their data is being processed. In these instances, we may apply the exemptions set out in Schedule 2 Part 1 of the DPA 2018 if deemed appropriate*."

[179] See for example, CJEU, Case C-13*/16*, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas*, 4 May 2017.

266. Given that the HO relied on the IPIC DPIA in justifying its decision not to conduct a discrete one for the EMRT, there is no reason why the HO's approach as regards the imposition of the exemption will be any different.

267. PI submits that the HO's stated approach is not in line with the ICO's guidance and the Court of Appeal's most recent judgement on the exemption.[180] The HO leaves open the possibility of imposing the exemption in relation to whole groups of data subjects on the mere basis that they are a foreign national offender and/or illegal migrant.

268. This potentially blanket approach is particularly concerning, because anyone whose data is processed by IPIC and the EMRT is very likely to fall within the stated categories of data subjects. The IPIC rules are used to generate recommendations and prioritise cases for enforcement action and as such the data subjects are individuals without leave. While there is no definition for 'illegal migrant' in legislation, it generally refers to a person who is in the country without lawful permission or who has overstayed their visa. This proceeds from the Immigration Act 1971 (and other subsequent legislation) under which anyone without leave to remain may be regarded as being in the UK unlawfully. Similarly, as above, the EMRT is only used in relation to foreign national offenders.

269. As above, the immigration exemption can only be imposed where providing information to a data subject would likely substantially prejudice the maintenance of effective immigration control. PI submits that providing general privacy information to data subjects on when IPIC may be used, what consequences its use could have and what personal data is processed (including relevant retention periods) would patently not prejudice immigration controls. Therefore, by extension the HO should not restrict the provision of information required under Article 5(1)(a) and the specific provisions in Article 13 of the UK GDPR on the mere basis that a data subject is considered an illegal migrant and/or a foreign national offender.

270. A blanket approach is not only incompatible with the proper construction of the immigration exemption, but it may also be discriminatory contrary to Article 14 ECHR. This is because foreign national offenders and/or illegal migrants are likely to come within the 'other status' ground of protection against unlawful discrimination. There is also a clear difference in treatment if individuals who fall outside these categories (and who are in analogous situation as their data is being processed by the HO) are provided with information that the data subjects in the instant case are not. It does not appear possible for the HO to demonstrate "an objective and reasonable justification"[181] for this approach particularly in circumstances where its framing of the exemption violates the UK GDPR.

271. There is also no mechanism within this approach to conduct a balancing exercise that considers **individual vulnerabilities** and assesses necessity and proportionality.

[180] [2023] EWCA Civ 1474.

[181] See for example, *Molla Sali v. Greece* [GC], no. 20452/14, ECtHR, 19 December 2018.

272. Finally, we note by extension that restrictions on the right of access as protected by Article 15 of the UK GDPR through the immigration exemption would also likely be unlawful if the above approach is taken. This is because access to raw data (such as recommendations generated by either IPIC or the EMRT) as well as the additional information pursuant to Articles 15(1)(a) - (g) (the information referred to in Article 15(1)(g) is dealt with briefly further below) cannot be denied on the mere basis that a data subject is considered an illegal migrant and/or a foreign national offender.

273. Any restriction must demonstrate the likely risk of substantial prejudice to immigration controls. While this might be made out if exempted information would notify an individual of pending enforcement action (such as the decision to detain them), the HO would not be able to satisfy this requirement by asserting that any information provided could jeopardise immigration controls. For example, where an individual has been detained and seeks information through a subject access request regarding IPIC recommendations that lead to their detention – this is unlikely to be enough to demonstrate prejudice. The individualised decision to restrict the right of access must also assess necessity and proportionality and include a consideration of the vulnerabilities of the data subject.

274. The HO has appeared to take exactly this approach in relation to the right of access as demonstrated by the fact that Duncan Lewis's search through subject access requests revealed that [*redacted]*. Moreover, even where information was provided in these cases, much of it is itself redacted making interpretation difficult. As such, PI believes that this would merit further investigation by the ICO.

Second principle - Purpose limitation (Art 5(1)(b))

275. The IPIC DPIA states that the primary purpose of the processing is to "create an easier, faster, and more effective way for Immigration Enforcement ("IE") to identify, prioritise and coordinate the services/interventions needed to manage its caseload". PI submits that the expansive re-use of multiple datasets to enable the EMRT and IPIC to generate recommendations violates he purpose limitation principle provided by Article 5(1)(b) UK GDPR, which requires that data is "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." A data controller may only process data for a new purpose if:

- "*The new purpose is compatible with the original purpose;*
- *You get the individual's specific consent for the new purpose; or*

- *You can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority*."[182]

276. We summarise the processing purposes (including the data gathering purpose specified in the domestic legal basis for IPIC) below and assess their compliance with the purpose limitation principle.

277. The input data for both IPIC and the EMRT (as set out above) includes voluminous, varied and ill-defined datasets that are in several cases collected for wholly different purposes:

a) **Detention details**: this data is so broad that it could encompass any information collected for detention purposes. This data may include highly sensitive details, including information relating to an individual's health and vulnerabilities, which could be collected through an individual's interactions with detention centre healthcare departments. Such sensitive information may also be included in HO Case Information Database case notes as well as detention and case progression reviews conducted while an individual is detained. This information may be necessary and compatible with processing required to determine if an individual is suitable for detention (including through the use of IPIC). However, the potential for such data to be used in other contexts, such as to establish if an individual should remain subject to a GPS ankle tag, does not appear necessary and may therefore already constitute an extension of purpose. This is underlined by the fact that there are no measures in place (including appropriate guidance) to ensure that such data is used only proportionately and where necessary, which also engages lawfulness as addressed above. By affording IPIC (and potentially the EMRT) access to **all** detention details (including periods of detention dating back 6 years[183]) – this processing mirrors the failings identified by the ICO in its EM Enforcement Notice. We refer here to the finding that a lack of detail as to when and how decisions to access and use trail data meant that the HO was unable to demonstrate that processing is proportionate and necessary for the relevant public functions.[184]

b) **Case Information Database special conditions including markers of potential vulnerability or health markers**: as above, these are indicators used by the HO to denote vulnerability. The markers include partly sensitive special categories information, such as "Known Suicide Attempt" and "Threat of Self Harm" and "Pregnancy".[185] The primary

[182] ICO, 'Guide to the General Data Protection Regulation (UK GDPR) – Principle (b): Purpose limitation,' (updated 10 Jnauary 2025), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

[183] This is based on reference in the HO PIN to the fact that detention records "may be held for 6 years".

[184] Ibid, §178.

[185] ICIBI, 'An inspection of the Home Office's approach to the identification and safeguarding of vulnerable adults', (February – May 2018), https://assets.publishing.service.gov.uk/media/5c35bbbf40f0b644683036ad/ICIBI_inspection_of_the_Home_Office_safegaurding_of_Vulnerable_Adults_Feb-May_2018.pdf

purpose of these markers is to identify vulnerable adults and ensure that the correct level of support is in place.[186] Indeed the only references to the processing of vulnerability data in the HO PIN relate to the provision of support and assistance as well as for safeguarding purposes. The re-use of such information for the purposes of profiling and ADM is a deeply concerning extension of purpose. It is noted that vulnerabilities data may play a role in recommendations that particular enforcement action is not carried out. However, this is not a given: as of 2018 there were 29 different special condition markers of varying severity[187] and this number is likely to have increased since. Indeed, IPIC and the EMRT appear to consider vulnerabilities against other factors processed by the tools (including offending and risk of harm). In any event, it is not enough that data is relevant or useful – any extension of purpose must be compatible, which PI submits is case specific and a question that should be considered in the light of the foreseeability and fairness of processing.

c) **Reporting details**: this re-use of data collected for the purpose of enforcing and administering reporting conditions is a worrying example of extension of purpose. Processing of all reporting data, which the HO's PIN suggests may in the case of foreign national offenders to be retained until the death of the data subject, to generate enforcement recommendations may not be necessary and proportionate. Moreover, the opaque processing of data concerning compliance with reporting conditions to generate a harm score (in the case of the EMRT) may (as above) skirt the established and stated process of breach identification, notification and investigation, leaving individuals unaware of the various circumstances in which a breach may be investigated, and unable to respond to concerns raised and their implications.

d) **Associations**: this is the opaquest of all the datasets referred to in the full list of data processed in the IPIC DPIA. It is not mentioned anywhere in the HO PIN, or any other privacy information (including the STS PIN and EM Handbook) and it is not defined in the DPIA or elsewhere in any HO documentation we have considered (including the training materials). By its everyday meaning such data is wider than information collected about an individual's family networks. PI submits that this dataset is indicative of the processing of information about individuals the HO has connected to the data subject. Such processing may automate suspicion by creating networks of association.[188] Such networks may link the data subject to individuals with a criminal history even though they have no criminal history of their own.[189] The controversial 'Gang Matrix' operated by the London Metropolitan Police involves exactly such associative processing, which may have a

[186] Ibid, §6.25.

[187] Written evidence submitted by UKLGIG (IDD0026), https://committees.parliament.uk/writtenevidence/89461/html/

[188] Katie Schwarzmann, 'The Computer Says So: Automated Recommendation-Making Tools in Immigration Systems - A comparative analysis between Canada, the USA and the UK' (10 November 2024), page 18, https://media.churchillfellowship.org/documents/Schwarzmann_K_Report_2023_Final.pdf

[189] Ibid.

discriminatory effect leading to false connections being made.[190] We do not consider that the processing of such data by either IPIC or the EMRT would comply with the first data protection principle and to the extent that it is collected for law enforcement purposes we do not consider that the re-use of such information by the EMRT and/or IPIC can constitute a compatible purpose. PI submits that the collection and use of such sensitive information may itself constitute a disproportionate interference with an individual's rights under Article 8 of the ECHR.

e) **EM data**: as with several of the other input datasets this is not clearly defined, which is likely to inhibit understanding by subjects as regards how their information is being used. PI submits that the current framing is broad enough to encompass the potential re-use of trail data or at the very least inferences drawn from this information. We note that as per the ICO's findings in the EM Enforcement Notice – inferences drawn from trail data, such as those around an individual's compliance with their bail conditions – may involve the processing of special categories information. The stated purpose of EM is "track[ing] and record[ing] the location of individuals in order to support immigration control".[191] PI submits that the use of trail data (or inferences drawn from locational tracking) to generate immigration enforcement recommendations that are wholly unrelated to GPS tracking would constitute a particularly flagrant extension of purpose. Yet even the processing of such information by the EMRT would breach the purpose limitation principle for three reasons. First, the statutory purpose for EM **only relates to the tracking of location**. Second, there is a lack of clear and consistent information provided to tag wearers about how their information will be used. The Immigration Bail policy makes no reference to trail data or information inferred from it being processed by an algorithm. Third, there is no clear and accessible legal framework permitting the re-use of EM data.

278. To summarise, it appears multiple datasets used by IPIC and the EMRT (albeit the failure to conduct a discrete DPIA means that it is not clear what data this algorithm processes) have been re-used for purposes outside the scope of their original or primary purpose. According to the purpose limitation principle (Article 5(1)(b) UK GDPR), data collected for certain purposes cannot be further processed in a manner that is incompatible with those purposes. Any use for an incompatible purpose must be supported by a new legal basis, and an updated impact assessment, which does not appear to have been done. Furthermore, there are no mechanisms by which data subjects are informed about any extension of purpose or for their consent to be sought. We note that the IPIC DPIA does not contain any analysis regarding the compatibility of purposes. Indeed, at question 9 the DPIA denies that the processing involves "matching or combining datasets that are being processed for different purposes".

[190] Ibid.

[191] Privacy International, 'Submission to the Information Commissioner – Request for Assessment of Processing Operations by the Secretary of State for the Home Department ("Home Office")', (17 August 2022), §100, https://privacyinternational.org/sites/default/files/2022-08/2022.08.17%20-%20Privacy%20International%20complaint%20against%20Home%20Office%20use%20of%20GPS%20Ankle%20Tags%20[public%20version].pdf

Third principle – Data minimisation (Art 5(1)(c))

279. The principle of data minimisation requires that personal data be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5(1)(c) UK GDPR).

280. As explained above, the HO's use of personal data when deploying both IPIC and the EMRT go beyond what is necessary and proportionate in relation to their processing purposes. In particular, the HO has failed to consider how it could ensure that the input data for both algorithms is relevant, adequate and limited to what is necessary. For instance, if the purpose is to ensure more efficient immigration decision-making it is unclear why the tool can process data relating to reporting or detention when determining if an individual should be referred to another government department by the ISD.

281. Similarly, broad and open-ended uses of datasets (such as that relating to 'associations') are also not limited to what is adequate and relevant since they have the potential to link a data subject to a wide range of other individuals with potentially adverse consequences. This could, for example, lead to enforcement recommendations that could lead to detention or removal.

282. Alongside the systemic re-purposing of information, the failure to limit the scope of information that is processed to what is adequate and relevant further contributes to processing that goes beyond what is reasonably foreseeable to data subjects.

283. PI therefore submits that the Home Office collects an amount of data in excess of what is necessary to effect the purposes stated in the national legal basis (which as above itself does not comply with the lawfulness principle) and is thereby in violation of the data minimisation principle.

Fifth principle - Storage limitation (Art 5(1)(e))

284. The storage limitation principle requires that personal data be "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" (Article 5(1)(e) UK GDPR).

285. The IPIC DPIA states that: "IPIC has a memory function to enable navigation of historical cases for review purposes. This includes being able to historically review recommended interventions on a case, but all further personal data will be erased" (§2.11). At §2.14 the DPIA goes on to explain that the retention period is aligned with the Immigration Enforcement Business Rules Retention Period Policy. The HO explains that "data will be stored for 5 years from when a decision is made in IPIC, or data is processed for Define or

TRaM." The DPIA nevertheless leaves open the possibility that personal data will be retained for longer than 5 years and such decisions will be in "line with official guidance" and involve guidance from the Knowledge and Information Management Unit ("KIMU") (§2.15).

286. Before we address the storage limitation principle substantively, we submit that there is insufficient clarity and foreseeability as regards how long IPIC and EMRT data can be retained. This is therefore relevant to compliance with the lawfulness principle addressed above.

287. The reference to a business rules retention policy suggests that all data processed by automated tools will be treated in the same way, which in turn indicates that EMRT data (in particular, recommendations generated by the tool) will be subject to similar retention practices. There is however no published document that sets out the modalities around the retention of business rules data and the HO PIN and STS PIN do not refer to IPIC, the EMRT or other ruled-based algorithms.

288. Moreover, there is a lack of clarity around exactly what information will be retained and what will be deleted. The reference at §2.14 to a retention period that starts from when a decision is made or **when data is processed for Define or TRaM** indicates that data beyond the recommendation itself may be retained. Moreover, the reference to the retention of IPIC decisions is itself opaque given that the role of ancillary outputs (such as the EMRT's harm score). As addressed below, such outputs constitute decisions in their own right and it is therefore unclear if they are retained alongside relevant recommendations.

289. Finally, the criteria regarding decisions to retain data beyond the 5-year period are not foreseeable given that the 'official guidance' cited in §2.15 does not appear to be published. The Knowledge and Information Management Unit Policy (the "HO Retention Policy") (last reviewed on 11 July 2024) does not refer to the retention/destruction of automated business rule data.[192] PI also refers to the reference in the HO PIN (see §258 above) to the potential retention of data relating to foreign national offenders until the death of the data subject.

290. PI notes that there is no justification in the DPIA for retaining decision data (or other information) for a period of 5 years or longer (which is relevant to the accountability principle addressed below). Justification for such long retention is particularly lacking where an individual is granted leave to remain or leaves the UK and as such are no longer subject to the immigration control regime.

291. By way of analogy, the HO's EM Data Access Request Guidance (updated following the ICO's Enforcement Notice) states that trail data will be deleted if an individual is granted leave

[192] Home Office, 'Knowledge and Information Management Unit Policy What to Keep – Corporate Retention Schedules', https://assets.publishing.service.gov.uk/media/6690eb900808eaf43b50ce3a/what-to-keep-corporate-records_Gov.UK_version.pdf

to remain or leaves the UK.[193] Moreover, this Guidance explains the rationale for the 6-year retention period that otherwise applies – namely that it is designed to enable the HO to defend and bring legal claims.[194] This same explanation does not appear to apply in the context of either IPIC or the EMRT.

292. For these reasons, PI submits that the current deployment of both IPIC and the EMRT violate the storage limitation principle. Individuals, including both foreign national offenders and subjects classified as unlawful migrants, may spend years on immigration bail and as such 5 years or more of IPIC and/or EMRT recommendations is likely to constitute a considerable amount of data. The retention of this information, which is itself the outcome of intrusive profiling, risks unfairly inflating a data subject's risk through 'feedback loop bias', which in turn may subject them to further similar interventions. This phenomenon arises where an algorithm's "recommendations or decisions influence the future data it receives, creating a cycle that reinforces its initial biases."[195] This risk is heightened in circumstances where the HO is developing a next generation of risk analysis tools that are likely based on machine learning technologies (see above).

Seventh Principle – Accountability (Art 5(2)) and Article 35

293. In this section, we address both the accountability principle and the HO's compliance with the requirements to undertake a lawful DPIA as provided by Article 35 of the UK GDPR. This is because a DPIA is the primary vehicle through which compliance with the accountability principle is demonstrated by a data controller. We begin by addressing the failures we have identified with respect to Article 35 before turning to the accountability principle further below.

The failure to undertake a DPIA

294. The ICO's EM Enforcement Notice provides extensive guidance on the circumstances in which Article 35(1) requires a controller to undertake a DPIA prior to the start of processing. As noted by the Enforcement Notice, the circumstances in which a DPIA will be automatically required are set out at Article 35(3) of the UK GDPR. Two of these circumstances are particularly relevant on these facts:

[193] Home Office, 'FNO RC Electronic Monitoring Service, Data Access Request Guidance', (April 2024), pages 2-3, https://www.whatdotheyknow.com/request/information_included_in_the_icos/response/2872820/attach/5/05693%20Annex%20U%20Data%20Access%20Request%20Guidance%20September%202024.pdf?cookie_passthrough=1

[194] Ibid, page 3.

[195] Katie Schwarzmann, ' The Computer Says So: Automated Recommendation-Making Tools in Immigration Systems - A comparative analysis between Canada, the USA and the UK' (10 November 2024), page 15, https://media.churchillfellowship.org/documents/Schwarzmann_K_Report_2023_Final.pdf

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."

295. With regard to the requirements of Article 35(3)(a) – the processing in the cases of both the various IPIC business rules and the EMRT is systematic. In both cases, as per the ICO's DPIA Guidance, the processing occurs **according to a system** (namely the relevant business rules). It is **pre-arranged, organised and methodical** and it **takes place as part of a general plan for data collection** (this is with reference to the algorithms' rules, the distinct recommendations that they generate and finally the varying functionalities they allow). The processing is **also carried out as part of a strategy**. This is with reference to the HO's Digital, Data and Technology Strategy, which refers to the need to adopt automated processing as part of its drive to become 'digital by design'.[196]

296. As per the DPIA Guidance, the processing is extensive because it involves a wide range of data, and it affects a large number of individuals. As per our analysis of the input data, the algorithms process information from across the immigration system. Moreover, as addressed above the scale of processing is such that individual business rules are likely to impact thousands of subjects. By way of illustration, over the 3 months between May and August 2023 almost 2,000 individuals were subject to quarterly EM reviews, which the HO acknowledges involved using the EMRT in all cases.

297. As set out above, the processing involves automated evaluation amounting to ADM and profiling. We address the quality of human review and the question of legal or similarly significant effects below. However, by way of two examples of legal effects arising from the processing – an individual may be detained or remain subject to an ankle tag (through the EMRT's harm score and/or the tool's recommendation).

298. Secondly, in accordance with Article 35(1)(b) – the deployment of both IPIC and the EMRT involves largescale processing of special categories data. This is evidenced by the HO's response to question 7 in the IPIC DPIA, which states that the processing is mostly special categories data. Given the role of offending and vulnerabilities data (as well as information inferred from trail data), the position does not appear to be any different in relation to the EMRT.

[196] Home Office, 'Corporate report - Home Office Digital, Data and Technology Strategy 2024 (accessible version)', (updated 20 October 2021), https://www.gov.uk/government/publications/home-office-digital-data-and-technology-strategy-2024/home-office-digital-data-and-technology-strategy-2024

299. Thirdly, the processing falls within multiple of the ICO DPIA Examples of processing that is likely to result in in a high risk to the rights and freedoms of natural persons:

a) Both the EMRT and IPIC (**and individual business rules**) involve "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." As above both systems involve largescale special categories data processing. While as below we consider that both tools involve solely automated processing, this example indicates that a DPIA will be required where processing involves ADM **to any extent** and decisions about access to services and/or benefits. In the case of IPIC, the ISD business rules represent the archetypical example of such processing as they seek to limit a subject's access to benefits and services if they are classified as not having immigration status.
b) Both algorithms (and the **individual business rules**) involve "profiling of individuals on a large scale." We note that the IPIC DPIA states in response to question 8 that the processing activity involves processing at a largescale. This is likely to be the same for the EMRT – with reference to the data intensive nature of its processing and the number of data subjects it impacts. We note that the HO has made contradictory statements as regards whether it considers the processing to amount to profiling. However, notwithstanding the HO's position we have demonstrated that it does constitute profiling as addressed above.

300. We submit that the above demonstrates that the conditions at Article 35(3) and the examples in the ICO's DPIA Guidance apply to **each** of the IPIC business rules and the EMRT. As such, in order to comply with Article 35(3), the HO should have conducted impact assessments across its uses of the algorithms that form the subject matter of this complaint. This is with reference to the:

a) The vastly different nature of the decision-making processes in relation to which the various business rules we have set out above correspond. For example, recommendations in relation to whether an individual should remain subject to a NFD device and whether they should be detained on reporting are identifiably distinct processing operations. They are likely to involve different sets of rules, and the input data may also be different. Moreover, as addressed above – they frequently involve wholly distinct functionalities. Not all the IPIC business rules incorporate the same prioritisation and filtering functions, for example. The fact that the business rules have been developed in tandem is not sufficient justification not to conduct additional DPIAs. Critically (as noted above), each set of business rules constitutes largescale profiling in ways that may involve the denial of a benefit/service or wider restriction of fundamental rights and freedoms.
b) The data subjects subjected to either IPIC or the EMRT will often be different. For example, the EMRT would not process the data of children whereas the HO acknowledges that IPIC business rules do. This is significant because it means that the data subjects subject to the profiling being undertaken are likely to have distinct

vulnerabilities that should be taken into consideration prior to processing. We address the failures to consider particular vulnerabilities when determining the scope and nature of processing from the perspective of the accountability principle below. Moreover, the various processing operations are likely to have different impacts on the relevant data subjects. The imposition of GPS tagging may (as addressed above) have a greater immediate impact on a data subject's well-being than being referred to the DVLA for the termination of an individual's driving license.

301. There is an overlap between the reasons why we consider the HO should have assessed the individual impacts of the different processing operations set out above and why we submit that the IPIC DPIA is unlawful (addressed below). This is because Article 35 is not prescriptive about the form in which a DPIA should be conducted; however, if the impacts of the processing were to be assessed lawfully via one document, then the HO would need to consider the above factors (the distinct nature of the business rules, data subjects and impacts of the processing).

The failure to conduct a lawful DPIA

302. By failing to consider the factors set out above, the IPIC DPIA does not comply with the requirements of Article 35(7).

303. With regard to Article 35(7)(a), the document **does not include a systematic description of the envisaged processing operations and the purposes of the processing**. The ICO's DPIA Guidance makes clear 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. Notably, the ICO's EM Enforcement Notice states that the level of detail to be provided pursuant to Article 35(7)(a) must be sufficient to enable a lawful assessment of necessity and proportionality, how any risks will be mitigated and to document compliance with the lawfulness principle (§89).

304. The HO patently fails to meet this level of detail. The description of the processing operations is limited to stating that immigration enforcement business rules are applied to TRaM data to identify, triage and recommend cases for particular enforcement interventions (see question 3 of the DPIA read together with §1.6 and §3.3).

305. With regard to the **nature of processing**, §93 of the ICO's EM Enforcement Notice must "set out the categories of personal data being processed at each stage, for each processing operation". The HO fails to provide any information on each processing operation as the consequences (namely the nature of the recommendations) of the business rules (including the EMRT) are not evident from the DPIA. The scope and nature of particular input datasets, such as "EM data", is ill-defined and critically there is no detail on what categories of data are used for each business rule or alternatively whether all rules have access to the same data.

306. The ICO also states in the GPS tracking context that the nature of processing should also set out what trail data can be accessed and any restrictions placed on doing so.[197] In the instant case there is no detail on whether there are limitations on the uses of certain datasets, such as reporting details (i.e. what periods of compliance with reporting conditions can the tools examine). Critically, outlining the bounds of processing is said to be intimately connected with the requirement to assess necessity and proportionality.

307. The DPIA also fails to provide sufficient detail regarding what special categories data is processed by IPIC and the EMRT. In relation to health data, for example, is this only collected via the Case Information Database special markers of vulnerability or does other input data (such as detention details or EM data) include special categories information?

308. In its findings relating to the EM Expansion Pilot, the ICO found that the HO's DPIA should have included a detailed assessment of whether there are likely to be vulnerable data subjects as well as what their vulnerabilities are (as relevant to Article 35(7)(c) and (d) as addressed below). This is wholly absent from the IPIC DPIA, which assumes that most data subjects will not be vulnerable without explanation (question 10) and provides no detail on whether there are likely to be vulnerable individuals. Similarly, at §2.4 – the HO acknowledges that the processing will involve individuals aged 13 or younger. It is not clear whether the data of children is included in the input data and/or whether IPIC business rules provide enforcement recommendations in relation to children aged 13 or younger (and if so which rules).

309. While there were significant flaws in how the HO assessed vulnerabilities for the purposes of the EM Expansion Pilot, the Immigration Bail policy provides guidance on vulnerability criteria to be considered when assessing whether to impose GPS tracking. With respect to IPIC and the EMRT, there is no equivalent framework for assessing vulnerability in any published policies or internal documentation disclosed to us, including the DPIA. As above, we consider that a significant number of data subjects are likely to be vulnerable for the same reasons as outlined in §108-109 of the ICO's EM Enforcement Notice (see also §§207-209 above). The failure to address risks arising from vulnerability means that the HO has not considered whether any mitigating factors should be put in place. This is of particular relevance to Articles 35(7)(b) and (c) of the UK GDPR (addressed below).

310. In its EM Enforcement Notice, the ICO makes clear that the 'context' of the processing for the purposes of Article 35(7)(a) includes an assessment of how far individuals are likely to expect and understand the processing.[198] As above, no privacy information is provided with respect to IPIC and any information provided in relation to the EMRT is uneven and

[197] ICO, 'Enforcement Notice issued by the Information Commissioner concerning contraventions of Article 5(2) and Article 35 UK GDPR by the Home Office', (28 February 2024), para. 93.

[198] ICO, 'Enforcement Notice issued by the Information Commissioner concerning contraventions of Article 5(2) and Article 35 UK GDPR by the Home Office', (28 February 20240, §111, https://ico.org.uk/media2/migrated/4028870/ho-migrant-tagging-20240228-en.pdf

contradictory with the result that we consider the HO to be in breach of the transparency principle.

311. There is therefore a significant risk that all data subjects will not understand how their personal data is being processed and for what purposes. These risks should have been addressed by the DPIA, which states that no information will be provided to data subjects because the HO's position is that there is no legal obligation to do so, and the immigration exemption can be relied upon in relation to certain groups. There is also a discrete risk arising from blanket framings of the immigration exemption (addressed above).

312. The ICO's EM Enforcement Notice also notes that the 'purpose' of the processing (for the purposes of Article 35(7)(a)) must be set out with sufficient precision and clarity to enable a lawful assessment of necessity and proportionality[199] As above, the purpose set out in the stated basis in national law (information gathering pursuant to implied immigration powers) is overly broad and does not correspond to the use of IPIC for decision-making. It is not aligned with the processing purpose as set out in the DPIA (creating an easier and more effective way for immigration enforcement to identify and prioritise interventions). Moreover, in practice the processing in IPIC and the EMRT goes beyond identifying and prioritising interventions to making decisions as to whether an individual is likely to be suitable for the action in question.

313. The stated processing purpose is also not sufficiently detailed. In particular, the HO fails to set out what the various business rules do – i.e. what are they recommendations that they generate and what decision-making processes do they relate to. PI submits that anything short of this for both IPIC and the EMRT inhibits a proper consideration of necessity and proportionality, risks to fundamental rights and freedoms of data subjects and what if any mitigation measures are required.

314. With regard to Article 35(7)(b) – the IPIC DPIA does not assess proportionality and necessity and instead proceeds on the assumption that both these requirements are de facto satisfied. This is the same with the EMRT given that no distinct DPIA was carried out and necessity and proportionality are not addressed separately in the IPIC DPIA. As per the ICO's DPIA Guidance, the controller must consider less intrusive options and, in particular, if **there is any other reasonable way to achieve the same result**.

315. As above, the processing is particularly intrusive with reference to the extensive nature of the input data, the generation of automated profiles based on this information and the lack of remedies afforded to subjects to verify the lawfulness and accuracy of the processing. There is no consideration of whether alternatives could meet the purposes of the various business rules (as addressed above through our investigation rather than based on the HO's framing of purpose).

[199] Ibid, §115.

316. For example, the HO has failed to assess whether it could limit the use of the tools where the facts are potentially particularly complex and/or data subjects have vulnerabilities that are likely to inhibit their understanding of the processing (as in the Swedish example set out above at §191). Similarly, there appears to be no means to limit the data accessed by the tool based on relevance and necessity. Given that some data subjects may have long immigration histories in the UK and considering the HO's lengthy retention periods for certain data (addressed above), there are no safeguards on disproportionate uses of personal information. PI submits that this could compromise fairness where an individual's circumstances have changed, such as in the event that several years previously they did not comply with an immigration bail condition but have since demonstrated exemplary compliance.

317. With respect to Article 35(7)(c) – PI submits that any assessment of the risks to the rights and freedoms of data subjects in the IPIC DPIA is extremely limited. The short section on risks (§5.1) is redacted, however it appears likely the identified risk pertains to solely ADM. This is because the mitigation steps are said to be: "IPIC makes recommendations only for interventions. The final decision always rests with a user." As per the DPIA Guidance, the controller must consider potential impacts of processing – whether physical, emotional or material. This has plainly not been carried out:

a) The DPIA has failed to consider potential adverse impacts of the interventions themselves on data subjects. For example, in the case of the EMRT – the risks to data subjects arising from GPS tracking (including the NFDs) is well established. There has been no assessment as regards the risk of decisions based on inaccurate or older data, which as above may not account for changes in circumstances including the reduction in an individual's risk of harm. Removal and detention cases often engage several ECHR rights, including but not limited to the right to life, the right to liberty and the right to privacy. As such, this assessment should have been conducted with particularly strict scrutiny.

b) The DPIA does not consider the risk of discriminatory impacts resulting from the functionalities of the tools and the data they process. For example, the automated prioritisation feature within several of the business rules may have a directly discriminatory effect given that it allows the HO to filter cases based on nationality. Equally, the possibility for business rules to process 'associations data' may be indirectly discriminatory. This is because the collection of such information may unfairly link a data subject to others who have come into contact with the criminal justice system, which may in turn disproportionately impact certain nationalities and/or ethnicities.

c) It also fails to assess the risk and impact on data subjects from the lack of transparency about the nature of the processing by both IPIC and the EMRT. The lack of transparency may in turn compromise the data protection rights of data subjects, inhibit their capacity to verify the accuracy and lawfulness of the processing and challenge unlawful processing.

d) Finally, any consideration of the risks around solely ADM must incorporate an assessment of impacts that this could have around compliance with other data protection rights and principles. This should include an assessment of whether human review is likely to be sufficient to ensure that the processing falls outside of Article 22(1) of the UK GDPR; and if not, whether the HO is likely to be able to meet the exceptions set out at Article 22(2); and whether it may be required to provide additional transparency information as per Article 13(2)(f).

318. As per the ICO's EM Enforcement Notice, a DPIA does not have to assess every possible risk, but it should address risks **that have more than a minimal chance of occurring**. This low threshold is met by all the above identified risks (which should not be taken as an exhaustive list of all risks that the DPIA should have addressed). Therefore, the HO has failed to assess or inadequately assessed the risks the processing poses to the rights and freedoms of data subjects in violation of Article 35(7)(c).

319. The HO has also failed to comply with Article 35(7)(d). This is because this provision requires the consideration of mitigation measures to address the above risks in circumstances where the HO has failed to adequately identify the risks in the first instance.

320. The sole reference to any mitigation measures in the DPIA is the human review of the algorithms' outputs. As above, §5.2 explains that the final decision will always rest with the user. Secondly, §5.3 explains that: "ongoing review and testing mitigates the risk of individuals being incorrectly recommended for interventions, additionally any action to an individual's case rests with the end user who can reject any recommendation made". As addressed below, there are algorithmic outputs, such as the EMRT's harm score, which bind the discretion of the human reviewer, thereby resulting in final decisions that do not rest with the user. Similarly, as also addressed below, the scope and nature of additional audits and reviews cited at §5.3 are often unclear and uneven across the various business rules.

321. However, in any event the information included at §5.2 and 5.3 of the DPIA is insufficiently detailed. There is no reference to the quality of the human review, which is vital to ensuring that it is *meaningful* (as addressed below). Again, this is coupled with the fact that the tool's design makes it easier for the user to accept a recommendation without further explanation than to reject it and justify the rejection in writing. Therefore, the tool does not fall afoul of the Article 22(1) prohibition on solely ADM. For example, what training is provided to caseworkers to ensure that they give adequate consideration to recommendations before actioning them? Similarly, there is no assessment of how the HO ensures that all relevant information is considered during a review. Finally, the HO does not assess any risks arising from the generation of automated parameters, such as the EMRT's harm score, which as below may constitute ADM in its own right.

The accountability principle

322. Given that the accountability principle is concerned with demonstrating compliance with the data protection principles, we have already addressed the substantive failings in detail above. Therefore, in this section we briefly frame the failures to comply with Articles 5(1)(a), (b), (c) and (e) through the prism of accountability:

a) **Lawfulness**: the HO has failed to demonstrate (in the DPIA or in its internal and published guidance) that its stated legal basis is sufficiently clear and accessible to data subjects. As above, there is an overlap between the lawfulness principle and the requirement for interferences with the right to privacy to be "in accordance with the law" for the purposes of Article 8 of the ECHR. PI submits that the HO has not shown how implied data gathering powers within the Immigration Act 1971 gives subjects an adequate indication as to the circumstances in which their information may be used for profiling and ADM purposes. This is particularly the case given the failure to publish any policies or guidance in relation to IPIC. The HO has also failed to demonstrate that using IPIC and the EMRT in all relevant cases as well as affording the tools access to extensive volumes of highly sensitive information is necessary and proportionate for both the legal and processing purposes. There was no consideration as regards whether less intrusive means could be deployed to achieve the same ends (such as refraining from using the tools in particularly complex/high vulnerability cases).

b) **Fairness and transparency**: the HO has failed to demonstrate compliance with the minimum transparency requirements as set out at Articles 12 and 13 of the UK GDPR. In relation to IPIC, no bespoke privacy information was provided. The HO PIN also does not provide any information on IPIC and information that is provided on ADM is not consistent with how the algorithm works in practice, which in turn is incompatible with the reasonable expectations of data subjects. With regard to the EMRT, information was not provided consistently to data subjects and the STS PIN denies the use of any ADM while the Immigration Bail policy does refer to the use of business rules. PI submits that the HO has not put its mind to the question of compliance with Articles 12 and 13, given that the DPIA states that there is no obligation to provide privacy information, and that processing is generally set out in the HO PIN. An assessment of how transparency should be effected was not undertaken in relation to the EMRT given the failure to conduct a DPIA altogether. Finally, the HO has failed to consider the fact that data subjects may be vulnerable and children when determining what if any transparency information to provide. Recital 38 to the UK GDPR read together with 58 requires that controllers processing data relating to children should ensure that any information and communication must be conveyed in clear and plan language. Similarly, where a controller is aware that they are processing data relating to vulnerable members of society, then the vulnerabilities of such data subjects should be taken into account in any assessment of how to ensure that it complies with its transparency obligations.[200] Instead of carrying out such an assessment (given that a significant number of subjects are likely to be vulnerable for the reasons outlined above), the HO stated that the majority of data subjects were not likely to be vulnerable without any explanation.

c) **Storage limitation**: the HO failed to provide any justification or explanation as to why it retains certain data (in particular IPIC recommendations) for a period of 5 years. There is no consideration at all in relation to applicable retention periods for the purposes of the EMRT

[200] Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679', (last revised and adopted 11 April 2018), §16, https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf

given that no distinct DPIA was conducted. These failures have significant implications for the foreseeability and fairness of the processing.

d) Data minimisation: the HO has failed to demonstrate the necessity and relevance of all the input data. This is particularly the case with respect to potentially intrusive datasets such as those related to 'associations'. Given the lengthy retention periods for certain data subjects (such as foreign national offenders), it is not clear what limits there around the processing of data relating to an individual's detention and reporting records (by way of two examples). The fact that most data processed by IPIC is special categories information underlines the failure to ensure that only necessary and relevant information is processed.

Profiling and ADM in breach of Article 22(1) of the UK GDPR

323. As addressed above, both the EMRT and IPIC involve elements of ADM and profiling notwithstanding the HO's inconsistent assertions on this point.[201] The outstanding question is therefore whether the quality of the HO's human review is sufficient not to fall foul of Article 22(1). This provides that data subjects: "shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." The question of legal effects and/or decisions that similarly significantly affect data subjects is also addressed below. We note however that the legal effect and significance of decisions should not be controversial and as such on these facts the question of compliance with Article 22 hinges above all on the human oversight (or absence thereof) implemented by the HO.

324. There is no definition as regards what constitutes solely ADM for the purposes of Article 22. However, the WP29's *Guidelines on Automated individual decision-making and Profiling* (adopted by the European Data Protection Board)[202] from February 2018 (the "WP29 Automated Decision-Making Guidelines") state:

> "*To qualify as human involvement, the controller must ensure that any oversight of the decision is* ***meaningful****, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider* ***all the relevant data*****.**"

325. In a recent determination of the Amsterdam Court of Appeal (Case 295.742/01) related to the automated termination of platform workers by Uber based on alleged fraud, the Court provided guidance on when human review would be considered meaningful for the purposes of Article 22.[203] In that case Uber argued that one or more human members of its risk team

[201] As above, the HO acknowledges at §4.8 of the IPIC DPIA (Annex II) that the processing constitutes profiling that could result in an outcome that produces legal effects or similarly significant affects on the individual.

[202] European Commission, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) ', (22 August 2018), https://ec.europa.eu/newsroom/article29/items/612053

[203] Court of Appeal of Amsterdam, 200.295.742/01, (04 April 2023), §§3.23-3.25.

would remotely investigate after a potential fraud signal was received.[204] The Court found that the human review was not meaningful (and therefore that Uber carried out ADM contrary to Article 22) on the basis that the review process did not examine all relevant information and did not include a process by which workers could make representations.[205] Moreover, Uber had not demonstrated that the reviewers had the requisite knowledge or training. In short, it held that the oversight of the decision-making process was not meaningful and did not go further than a "symbolic act".

326. Should the ICO find that the EMRT and/or IPIC involved processing that engages Article 22 of the UK GDPR, this may entitle data subjects to additional transparency (beyond that outlined above) regarding the functioning and consequences of the ADM tools. In particular, this would be likely to include information to be provided directly to data subjects (under Article 13(2)(f)) as well information on request following the submission of a subject access request (Article 15(1)(h)). This is addressed in further detail below.

327. Given the differences in features between IPIC and the EMRT, our below submissions address each tool separately. We then address the exceptions to the prohibition on solely ADM and the potential further transparency information required.

The EMRT and processing contrary to Article 22 of the UK GDPR

328. We submit that there are certain features relating to this tool that are effectively solely automated. The harm score generated by the EMRT is an example of ADM without sufficient human review. The human involvement in the generation of the score occurs at two stages.

329. Firstly, a caseworker inputs data into the tool to generate the harm score. We do not consider that the mere inputting of data in circumstances where the caseworker has no role in what outcome the tool generates constitutes human review. This submission is consistent with the findings of other Data Protection Authorities when interpreting Article 22 of the GDPR. For example, the Garante found that a job allocation algorithm deployed by the gig economy platform, Foodinho, constituted solely ADM notwithstanding the fact that the algorithm's parameters were manually set by the company's employees.[206]

330. Secondly, human intervention once the harm score has been generated is limited to checking that the minimum amount of time relative to the indicative harm tiers set out in the table in the Immigration Bail policy and the EMRT training materials has expired before transitioning the subject to an NFD. PI submits that this does not constitute meaningful human review, because the caseworker does not have the authority to change the decision

[204] Ibid, §3.24.

[205] Ibid, §3.24.

[206] Barros Vale, Sebastião and Zanfir-Fortuna, Gabriela, 'Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities', (May 2022), page 33, https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf

in question. They cannot determine that the EMRT has inflated an individual's risk of harm and that as such they should be transitioned to a NFD before the minimum period has expired or no longer be subject to EM altogether. Moreover, there is no means for a data subject to make representations given that there is no information at all that is provided to tag wearers about the harm score (any client correspondence as per Annex V only refers to the use of business rules and even then, the inclusion of this information has been inconsistent).

331. The implementation of the harm score results in legal effects or similarly significantly affects the data subject. The decision to continue to tag an individual via an ankle (in event that the minimum period for each harm tier has not expired) affects the legal rights of data subjects. It is also likely to significantly affect them considering the established impacts of both ankle tags and NFDs on the mental state and well-being of tag wearers (as summarised above).

332. That this amounts to a decision with legal effects or similarly significantly affects the data subject is notwithstanding the fact that the harm score is ancillary to the tool's final recommendation. As confirmed by Recital 71 to the UK GDPR, a 'decision' for the purposes of Article 22 has a broad scope and can cover everything from the automatic refusal of an online credit application or e-recruiting practices without human intervention.

333. The CJEU examined the application of Article 22 in relation to 'preparatory acts' (i.e. ancillary outputs that significantly affect the outcome of final decisions) in its recent decision in SCHUFA (case C-634/21). While the facts in that case relate to the distinct context of credit reference agencies, the legal questions it raised are identical to those in the instant case. The case revolved around the denial of credit by a bank based on an automated score provided by a third-party. The score was itself found to constitute an automated decision with significant effects on the data subject even though the bank made the final decisions. This was because if certain credit scores were generated, they would lead "**in almost all cases**" to the refusal of a loan by the bank.[207]

334. PI submits that the ICO should take the same approach as the CJEU in SCHUFA. This is because (a) failing to regulate preparatory acts would create a protection gap that could result in controllers designing superficial human oversight mechanisms to escape the purview of Article 22; and (b) ADM systems are increasingly made up of chains of decisions all with varying implications for data subjects.[208] A binary conception of when a decision engages Article 22 is not reflective of the technological realities that underpin ADM systems.

335. As with the credit score in SCHUFA, the EMRT's harm score is **determinative of the outcome of the EM review** where an individual has not spent the minimum period on an

[207] CJEU, OQ v Land Hessen, SCHUFA Holding AG (Case C-634/21), §48.

[208] Katie Schwarzmann, ' The Computer Says So: Automated Recommendation-Making Tools in Immigration Systems - A comparative analysis between Canada, the USA and the UK' (10 November 2024), page 10, https://media.churchillfellowship.org/documents/Schwarzmann_K_Report_2023_Final.pdf

ankle tag relative to their harm tier. As per the above statistics obtained through FOIA, during a three-month period in which the HO acknowledges that the EMRT was used in all cases, EM conditions were only withdrawn altogether in **0.9%** of cases.[209] This underlines the defective nature of human oversight in relation to the harm score and the final recommendations (addressed below) given that EM was maintained in some form in virtually all cases.

336. We note that the current use of automated breach thresholds for each harm tier (as addressed above) may also contravene Article 22(1) of the UK GDPR for the same reasons as the harm score.

337. The inputting of data to generate the thresholds does not amount to human review for the purposes of Article 22 (for the reasons set out above). Furthermore, there does not appear to be a means for a human reviewer to assess whether previous breaches may be counterbalanced by other factors thereby resulting in a decision to remove an EM condition or transition an individual to an NFD. Moreover, given the secret nature of the automated breach thresholds there is no means for an individual to make representations as to whether the threshold has in fact been reached (the possibility to make representations providing mitigation in relation to the allegation of breach itself is addressed below). It is not clear exactly what weight is afforded to the breach thresholds (in contrast to the harm score), which is of relevance to the question of the significance of the decision and the extent to which it determines the final recommendation. As such, we reserve our position on this point, but we recommend that the ICO investigates it further.

338. With respect to the EMRT's final recommendations, we submit that these are also decisions that both have a legal effect and significantly affect data subjects. In the same way that the harm score is determinative of the minimum period an individual spends on an ankle tag, the recommendation determines how long a tag wearer is subject to each type of device and the period they remain subject to EM altogether.

339. It is PI's submission that the human review incorporated into the EMRT's recommendation is superficial and cannot qualify as meaningful for the purposes of Article 22(1). In particular, HO caseworkers do not have the authority to change the decision in question and/or to consider all relevant information. The review process also fails to incorporate a mechanism for data subjects to make representations nor has the HO demonstrated that its officials have the requisite knowledge or training.

340. As addressed above, the EMRT's design only generates recommendations as to whether an individual should remain subject to an ankle tag or be moved to an NFD. Despite the training materials stating that a caseworker should consider the proportionality of tagging altogether, there is no mechanism to do so in practice.

[209] WhatDoTheyKnow, 'Response to Jo Hynes request to Home Office', (10 September 2023), https://www.whatdotheyknow.com/request/reviews_of_decisions_to_impose_g/response/2422269/attach/3/78221%20Hynes.pdf?cookie_passthrough=1

341. **First**, there is no recommendation for the cessation of EM. **Second**, the relevant EM review forms generated by the tool do not include a pro forma relating to the removal of an EM condition. **Third**, the pro forma text generated for the EM review forms states that proportionality is already considered by the tool itself inhibiting a wider assessment. **Fourth**, there is no clear guidance in the training materials or the Immigration Bail policy on how to conduct such a wider proportionality assessment when deploying the EMRT.

342. It appears that the HO will only conduct a review of the appropriateness of EM altogether in response to representations received by an individual regarding their EM condition (rather than the quarterly review process). This is consistent with the fact that the EMRT training materials indicate that the tool will only be used in the quarterly reviews.[210] Indeed, the letter received by the client of Wilson Solicitors is an example of a review carried out in response to representations submitted by the tag wearer's legal representatives.

343. For the human review process to be meaningful, caseworkers must (when using the EMRT) be able to properly consider the appropriateness of EM as a whole. This is because as per the High Court's judgement in *ADL and Others* (cited above), the system of quarterly reviews is how the HO complies with its duty not to impose EM where impractical and/or in breach of the ECHR. As such, the HO decision-maker is both denied the authority to remove EM altogether and inhibited from considering all relevant information (there is a clear overlap between these failings). The failure to operate a system that allows for an assessment of whether EM as a whole is appropriate by its very nature subverts the implementation of the HO's legal duties as interpreted by the High Court. This is reflected in the negligible rate (cited above) of quarterly reviews resulting in the removal of an EM condition.

344. We note that the training materials refer to the fact that the recommendations are subject to 'quality assurance' ("QA"). This does not alter the inadequacy of the HO's review process for the following reasons:

a) The criteria considered by the QA process are extremely opaque. The sole reference in the training materials to what the QA process considers states that: "Not in public interest? Criteria by which staff's work is QA'd - would we just have to release it anyway?"[211] There is also no guidance in the training materials or elsewhere as regards how any QA should be undertaken.

b) The training materials suggest that the QA process would only result in a reversal of decisions to transition tag wearers to an NFD.[212] This is because the materials state that in "EM maintained cases" (i.e. where the individual remains subject to an ankle tag) the QA process would result in a caseworker receiving a "report detailing the outcome and

[210] EM review must at least be carried out on a quarterly basis, in response to representations and when a request is made by another decision-maker. Home Office, 'Immigration Bail Policy', (31 January 2025), page 46, https://assets.publishing.service.gov.uk/media/68514c37f2ccfcfd2f823f5b/Immigration+bail.pdf

[211] Annex XV - EM Review Tool Training Materials 2023, page 18.

[212] Ibid, page 17.

any feedback." By contrast, in cases where a tag wearer is deemed suitable for transition to an NFD – the QA process can result in the case being found unsuitable with the consequence that it is returned to the caseworker for amendment.

c) Neither caseworkers nor the designated authorising officials appear to have received training on how to carry out reviews of automated decisions in compliance with data protection law. We place reliance on our IPIC FOIA in which we requested: "all training materials provided to caseworkers to ensure that they use IPIC correctly. This includes any training information provided to ensure that caseworkers comply with the Public Sector Equality Duty and their obligations under the UK GDPR and Data Protection Act 2018." There is however no information in the training materials disclosed to us that details how HO officials should carry out human reviews in compliance with the UK GDPR and the DPA 2018. Moreover, the references to data protection training in the HO's APD (see above) are generic and do not concern the human reviews of EMRT recommendations.

d) Finally, the statistics set out above regarding the outcomes of quarterly EM reviews correspond to decisions that would have undergone the QA process. As above, the statistics assist in evidencing the deficient nature of the review process, which includes the QA implemented by authorising officials.

345. The harms arising from the inadequacies in the human review procedure include the risk that individuals are subject to disproportionate periods of EM contrary to their rights under the ECHR. This is likely to be heightened by the opacity of processing, which inhibits individuals from understanding how their data is being used and by extension to challenge automated decisions made about them.

346. Where individuals do not have legal representation, any recourse and effective remedy in relation to the EMRT is even further reduced. We note that due to systemic issues in the provision of legal aid an estimated 57% of individuals claiming asylum (a group that overlaps with tag wearers) are doing so without access to a legal aid representative as of November 2024.[213] The absence of legal aid will in turn frequently mean that an individual does not have legal representation due to the lack of means to instruct private immigration solicitors. This could for example mean that tag wearers are not able to make representations challenging the use of EM, which in turn means that they would only be subject to review via the EMRT through the quarterly review process. Similarly, they may not be aware of the need to submit evidence by way of mitigation in response to potential breach allegations. This could in turn lead to the EMRT drawing adverse inferences about an individual's risk when the allegation of non-compliance may have resulted from a malfunctioning of the individual's GPS tag.

IPIC and processing contrary to Article 22 of the UK GDPR

[213] Frances Timberlake, 'Threadbare: The Quality of Immigration Legal Aid', (2025), Migrants Organise, page 15, https://www.migrantsorganise.org/app/uploads/2025/04/Threadbare-Quality-of-Immigration-Legal-Aid-2025.pdf

347. IPIC recommendations likewise have substantial legal effects and significantly impact data subjects. We have demonstrated above that the use of the tool goes beyond triaging cases and involves recommendations concerning particular enforcement actions. Where individuals are, for example, detained on reporting or subjected to removal this engages several of the most fundamental human rights, including the right to life, to liberty and to privacy. Similarly, where an individual is denied access to social security benefits following a recommendation by IPIC business rules they may suffer financial hardship, particularly in circumstances where this consists of their only or primary source of income.

348. The HO maintains that the processing does not constitute ADM on the basis that there is human review in place. As above, this is an erroneous position given that profiling and ADM can take place with a human in the loop. Such processing may still be highly invasive and engages all the data protection rights and principles addressed above. Nevertheless, based on the available evidence PI submits that the human review undertaken by the HO cannot be considered meaningful and may therefore lead to breaches of Article 22(1).

349. As with the EMRT, caseworkers reviewing IPIC recommendations are not able to consider all relevant information and data, data subjects cannot make representations in relation to the use of the tool, and there is insufficient evidence of training in place.

350. PI submits that the ICO should take the substantial design nudges built into the tool into consideration in any assessment of Article 22. These include the requirement to provide explanations when refusing an IPIC recommendation, but not conversely when accepting one. This nudge is built into all the business rules, as addressed above. Several of the rules, including those that engage particularly fundamental rights and freedoms such as returns preparation, also afford caseworkers longer periods of time to change a rejected recommendation than they do an accepted one.

351. The nudges incentivise rubberstamping of decision-making particularly in circumstances where the HO is seeking to clear immigration casework backlogs. These risks have been recognised by the HO itself. For example, in the executive summary of its evaluation of IPIC disclosed to Public Law Project under the FOIA, the HO noted there was an "increased accepted rate" compared to previous systems (described as 'business as usual' or "BAU").[214] Similarly, the evaluation also notes a recommendation to amend the list of rejection reasons to counter the catch-all "not listed" reason being disproportionately selected by users. While this relates to rejected recommendations, it does demonstrate an awareness of the risks of unexplained decision-making. It is not clear if this recommendation has since been put into effect given that the "not listed" option may still be used.[215]

[214] Immigration Enforcement, *Untitled Report*, evaluation of IPIC pilot, page 1, https://www.whatdotheyknow.com/request/triage_tools_used_in_an_immigrat/response/2002033/attach/5/68562%20Kazim%20Annex%20E%20Evaluation%20Background%20and%20Summary%20Redacted.pdf?cookie_passthrough=1

[215] Ibid, page 2.

352. Moreover, none of the training materials provide caseworkers with clear guidance on how to conduct reviews of recommendations.

353. The training materials state that caseworkers should only accept IPIC recommendations where it is appropriate to do so. Officials are told to check both information held on IPIC (which appears to contain summary information concerning vulnerabilities, barriers to removal and other immigration data) as well as other information held on HO systems (in particular, the Case Information Database and Atlas databases). However, there is no guidance on what information to examine on HO databases and how to weigh up different factors before accepting/rejecting a recommendation. To make a lawful decision to detain an individual, for example, the HO must carry out a complex balancing exercise. This requires a detailed assessment of how long it is likely to take to remove the individual (this may require consideration of county of origin information where for example the destination country needs to issue the individual with travel documentation), their risk to the public, and their vulnerabilities (including expert evidence submitted to the HO).[216]

354. As with the EMRT, IPIC caseworkers are inhibited from carrying out such a consideration by the human review process. This is also evidenced by [*redacted].* While the references to IPIC include [*redacted]* these are indicative of a superficial review process since they relate to very clean-cut cases where an individual is as a matter of certainty not suitable for an intervention (because they require an emergency travel document or have a clear barrier to removal). There is no evidence of detailed consideration and weighing up of all relevant factors (set out above for detention, for example), which may in certain cases involve very vulnerable individuals who have less definitive barriers to removal. The WP29 Automated Decision-Making Guidelines state that this assessment must involve the consideration of all **available input and output data**.

355. Moreover, we note that the details provided in the IPIC review tab (summarised above at §82), such as the subject's age, may correspond with the wholly automated filters that can be applied to prioritise certain recommendations. Where, for example, filters are applied to exclude individuals above or below a certain age from the intervention then this may further automate the review process in ways that reduces human scrutiny of the IPIC recommendation.

356. The same considerations around the absence of any mechanism for data subjects to be able to make representations in relation to IPIC recommendations apply as in the Amsterdam Court of Appeal's judgement regarding the profiling carried out by Uber. For the avoidance of doubt, we note that both the IPIC and EMRT involve processing, which would not be compatible with the proposed changes to the UK GDPR's/ DPA 2018's automated decision-

[216] See for example as regards how this assessment should be carried out in relation to vulnerable detainees, Home Office, 'adults at risk in immigration detention', version 10.0, (21 May 2024), pages 20-22, https://assets.publishing.service.gov.uk/media/664b61e0993111924d9d3844/Adults+at+risk+in+immigration+detention.pdf

making rules contained in clause 80 of the Data Use and Access Act ("DUAA"). In particular, both tools process special categories data, result in potentially significant "adverse legal effects" and are made without meaningful involvement.[217] Similarly, due to the lack of transparency regarding use of the tool and how it processes personal data we do not consider that individuals can ask for meaningful human intervention or challenge decisions made by ADM (the failure to ensure that individuals can make representations is addressed above).[218]

357. Finally, as with the EMRT – we do not consider that any QA process undertaken with respect to IPIC is sufficient to remedy the failures identified above. Firstly, several of the training materials do not refer to any assurance process at all. Secondly, where there is an assurance process it is either not carried out in all cases, or it does not involve a further substantive review of the IPIC recommendation. For example, in the case of the digital reporting business rules, the assurance process is limited to officials being able to review specified reports concerning the implemented recommendations.[219] With respect to the ISD rules. the QA process involves 'dip sampling' and thus while officials may overturn recommendations this will only be undertaken in selected cases.[220] In any event, there is no evidence that officials involved in the assurance process have access to further training or additional information relative to caseworkers first engaging with the recommendation.

The exceptions to the Article 22(1) prohibition on solely ADM

358. We note that Article 22(2) permits solely ADM in specified and limited circumstances where safeguards are in place. The sole potential exception that could in principle apply here is that set out at Article 22(2)(b) – in particular that the decision is authorised by national law and lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

359. PI submits that the HO would not be able to avail itself of this exception because there is no legal basis authorising the use of solely ADM. As above, we do not consider that the stated lawful basis under Article 5(1)(a) is sufficient for the processing as a whole. Article 22(2)(b) requires a lawful basis that **explicitly authorises solely ADM** and the HO would not be able

[217] Ada Lovelace Institute, 'Policy Briefing – Data (Use and Access) Bill: Committee Stage', (4 March 2025), page 5, https://bills.parliament.uk/publications/59409/documents/6109

[218] Ibid

[219] Home Office, 'IPIC Digital Reporting – Manager Training Guide', pages 125-129, https://www.whatdotheyknow.com/request/identify_and_prioritise_immigrat_3/response/2784289/attach/2/Annex%20D%20iv%20OFF%20SEN%20ipic%20digital%20reporting%20manager%20training%20guide%20PDF%20REDACTED.pdf?cookie_passthrough=1

[220] Immigration Enforcement, *title and date redacted,* Interventions and Sanctions Directorate Training Guide, pages 13-16, https://www.whatdotheyknow.com/request/identify_and_prioritise_immigrat_3/response/2784656/attach/2/Annex%20D%20ix%20OFF%20SEN%20IPIC%20Detailed%20Reference%20Manual%20ISD%20REDACTED%201.pdf?cookie_passthrough=1

to rely on its inadequate Article 5 basis particularly when it has failed to consider the risk that it could be processing data contrary to Article 22(1).

360. Article 22(3) requires controllers to implement suitable measures to safeguard data subjects' rights, freedoms and legitimate interests. Such measures should include as a minimum a way for the data subject to obtain human intervention, express their point of view, and contest the decision. As addressed above, none of the Article 22(3) safeguards are in place as there is currently no means to obtain human intervention (i.e. by way of an appeal mechanism) and make representations. More broadly, the WP29 Automated Decision-Making Guidelines emphasise the need for transparency to ensure that the specific safeguards can be relied upon in practice.[221] As we have emphasised throughout this complaint, there is a systemic lack of transparency in the use of both the EMRT and the IPIC, which prevents data subjects from understanding how their data will be used.

The additional transparency information that is required where the HO has engaged in solely ADM

361. Under Article 13(2)(f) controllers who engage in solely ADM must provide data subjects with (a) confirmation that they are engaging in this type of activity; (b) meaningful information about the logic involved; and (c) an explanation of the significance and envisaged consequences of the processing. In addition, controllers may also need to provide the same information further to a subject access request pursuant to Article 15(1)(h) (albeit the controller should have already provided this information in line with their Article 13 obligation).

362. For the reasons addressed above, the HO is currently failing to comply with its general transparency obligations let alone the additional obligations relating to processing that engages Article 22(1). However, for the avoidance of doubt we also submit that the current transparency information does not comply with the additional requirements. In particular, the STS PIN denies any form of ADM as far as the EMRT is concerned. The HO PIN's references to ADM lack sufficient specificity and detail to meet these requirements in relation to IPIC and what's more they refer only to undertaking such processing in relation to "applications", which is arguably inconsistent with the uses of the algorithm. There is no provision of information about the logic of the systems or their consequences for data subjects.

363. In this section we also address what information we consider should be provided to data subjects if the ICO finds that the HO has processed data contrary to Article 22. This is because this information is of real relevance to the question of remedies, which is addressed below.

[221] Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 17/EN WP 251, (3 October 2017), page 16, https://ec.europa.eu/newsroom/document.cfm?doc_id=47742

364. We consider that confirmation that the HO is engaging in ADM should not be generic, but rather must include notification that it is deploying either and/or both systems in relation to a data subject.

365. Meaningful information about the logic involved is not defined in the GDPR. However, the CJEU's recent decision in *Dun & Bradsheet* provides helpful interpretative guidance on what such information should include. The CJEU found that meaningful information about the underlying logic has a very broad scope and "covers all relevant information concerning the procedure and principles relating to the use, by automated means, of personal data with a view to obtaining a specific result." The explanation must be sufficiently concise and intelligible and therefore cannot be unduly complex. We consider that at a minimum this must include:

a) A detailed description of the categories of data processed to generate the profile and/or decision (which should incorporate an explanation of the source of all inputs).
b) An accessible explanation of the formula used.
c) The specific outputs relating to the data subject (for example their harm score in relation to the EMRT).
d) The weighting of all inputs and parameters.

366. The ICO should follow the approach of the CJEU in this regard given that this is the minimum information required to enable data subjects to verify the lawfulness and accuracy of the processing. We refer in this regard to §73 of *X v Transcription Agency* [2023] EWHC 1092, which confirms that in relation to the right of access – the purpose of Article 15 GDPR is to enable data subjects to verify the lawfulness of a data controller's processing operations.

367. PI submits that the HO must have regard to the transparency principle and the requirements concerning the communication of this additional information pursuant to Article 12 of the UK GDPR. We further submit that to ensure sufficient clarity, accessibility and intelligibility – the HO should provide the above information clearly and coherently to data subjects. It may be appropriate to provide data subjects discrete, bespoke privacy notices that ensure that all the information is consolidated in one place and is conveyed to them directly. The HO must consider the vulnerability of data subjects, including in particular where they are children, in determining the modalities surrounding how it communicates any additional transparency information.

368. Moreover, existing privacy information, in particular the HO PIN and the STS PIN, should be corrected where they provide erroneous and/or inconsistent information (see above).

369. Finally, we accept that the information provided pursuant to Articles 13(2)(f) and/or 15(1)(h) is potentially subject to the immigration exemption under Schedule 2, paragraph 4 to the DPA 2018. However, the exemption is not a trump card, and it must be interpreted strictly given that it potentially interferes with the fundamental rights and freedoms of the data subject. As above, the current framing of the exemption in the IPIC DPIA is not lawful

since it fails to follow the approach following the Court of Appeal's judgement in *R (The 3Million) v Secretary of State for the Home Department* [2023] EWCA Civ 1474. Any use of the exemption cannot be on a blanket basis, there must be a substantial risk of prejudice to immigration control and any risks must be balanced against the rights of data subjects.

VI. Applications/Remedies

370. For the reasons provided above, PI requests that the ICO issue an assessment notice under section 146 of the DPA 2018, investigate the HO's use of the EMRT and the IPIC tool under Article 58(1) of the UK GDPR, and consider the HO's compliance with the seven data protection principles, data subject rights requirements and processing obligations under the UK GDPR when collecting and processing data through the use of these ARMTs within their immigration enforcement operations.

371. PI invites the Commissioner to consider, in particular:

a) The lawfulness, fairness and transparency principle – in light of the imprecise and inadequate lawful basis provided by the HO for their processing activities, a subversion of affected data subjects' expectations as well as a disregard for the processing's adverse impacts and finally, a failure to provide meaningful, clear and consistent information to data subjects describing the processing of their data.

b) The failure by the HO to meet their DPIA obligations under article 35 of the UK GDPR – in light of the HO's failure to adequately meet any of the requirements set out in article 35(7) of the UK GDPR.

c) The HO breaches the UK GDPR in relation to ADM – in light of the lack of meaningful human involvement in the ADM conducted by the ARMTs, and a failure by the HO to provide adequate explanations to data subjects about the ADM and how it is being conducted, as required by article 13(2)(f).

372. PI requests that the ICO issue an enforcement notice under section 149 of the DPA 2018 requiring the HO to cease all collection and processing of personal data of data subjects through its use of the EMRT and the IPIC tool within immigration enforcement operations, under Article 58(2)(f) of the UK GDPR.

373. In the alternative, PI requests that the ICO issue an enforcement notice requiring the HO to bring its collection and processing of personal data in relation to the EMRT and the IPIC tool in compliance with the UK GDPR, under Article 58(2) of the UK GDPR. In particular, PI requests that the ICO require that the HO provide meaningful transparency information to affected data subjects in accordance with the requirements of the UK GDPR, including by providing information about the logic involved in the ADM conducted by the ARMTs.

374. PI also requests that if the HO has withdrawn the EMRT or an equivalent tool, data subjects still be informed that an ARMT was used in their cases, in particular where the use of that ARMT breached the UK GDPR or DPA 2018 and may entitle the affected data subjects to pursue compensation.

Privacy International

18 August 2025

VII. Annexes

- Annex I – Privacy International's Work on Migration and Technology
- Annex II - DPIA v 1.23 Redacted
- Annex III – **(Confidential)** Home Office Response Letter to Wilson Solicitors Client Transition to NFD -Redacted
- Annex IV- **(Confidential)** Duncan Lewis Solicitors Analysis of Home Office Subject Access Bundles
- Annex V - IPIC Reference Manual Manager Access Redacted
- Annex VI - IPIC Reference Manual Caseworker Access Redacted
- Annex VII - Immigration Enforcement, 'IE Business Rules (IEBR) Identify & Prioritise Immigration Cases (IPIC) Training Guide – EUSS Cases'.
- Annex VIII - IPIC Digital Reporting Manager Training Guide Redacted
- Annex IX - IPIC Training Guide for Caseworkers Reporting and Offender Management (ROM) Redacted
- Annex X - IPIC Reporting and Offender Management (ROM) User Guide November 2023 Redacted
- Annex XI - IPIC Training Guide - CSTT (Managers) Redacted
- Annex XII - IPIC Training Guide - CSTT v 1.1 (Final) Redacted
- Annex XIII - IPIC Interventions and Sanctions Directorate (ISD) Training Materials Redacted
- Annex XIV - EM Review Tool Training Materials
- Annex XV - EM Review Tool Training Materials 2023
- Annex XVI – Gathering information for Electronic Monitoring Review Tool Redacted
- Annex XVII - FNO RC GPS Electronic Monitoring Version 1.0
- Annex XVIII - Electronic Monitoring Review Form - EM Maintained
- Annex XIX - Electronic Monitoring Review Form - Already on NFD
- Annex XX - Electronic Monitoring Review Form - NFD Suitable
- Annex XXI - Duncan Lewis FOIA Request Redacted
- Annex XXII -Presentation - Cerberus and the future of risk at the UK Border - Travis Van Isacker