9 September 2026

Privacy International's response to the Department for Science, Innovation & Technology's call for evidence on data regulation in the age of AI and other data-intensive technologies

Introduction

1. Privacy International (PI) is a non-governmental organisation that conducts research and advocates globally against government and corporate abuses of data and technology.[1] It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change.

2. PI conducts research on artificial intelligence (AI) and data protection and has considered it's use in the context of intelligence agencies, immigration[2] and recruitment[3] amongst others.

3. We welcome the opportunity to respond to the Department for Science, Innovation & Technology's open call for evidence on data regulation in the age of AI and other data-intensive technologies.

[1] See: https://privacyinternational.org/

[2] See for example: Privacy International, 'Privacy International issues complaint to the UK regulator regarding the deployment of two algorithms for immigration purposes suspected of failing to adequately comply with data protection law', 15 August 2025, available at: https://privacyinternational.org/press-release/5640/privacy-international-issues-complaint-uk-regulator-regarding-deployment-two

[3] Privacy International, 'Humanless Resources? Uncovering AI recruitment software' 9 July 2026, available at: https://privacyinternational.org/long-read/5798/humanless-resources-uncovering-ai-recruitment-software

Theme 4 – Transparency and rights in complex data environments

Prompt question 2: How effective are the data protection framework's transparency requirements and data subject rights in the context of data intensive technologies and will these remain fit for purpose over time as technology advances?

4. The function of data protection law is structured around the premise that data controllers know their own processing: what personal data they hold, where it came from, the purposes and legal basis for processing it, and the consequences of that processing for data subjects.[4] These premises underpin the exercise of data protection rights which is why the law requires controllers to explain this information to them.[5] The technical functioning of AI poses a challenge to these premises throughout the AI lifecycle. We focus on the following three stages of the AI lifecycle that :1) training: the data that goes into the system, 2) process: how the system uses it, and 3) output: what the system produces.

Training

5. The law assumes controllers know what personal data they hold, and its source. Several features of AI undermine this. The first concerns scale. AI systems are typically trained on large datasets,[6] which are often merged, and unstructured.[7] Such data is often widely sourced[8] and could include data scraped from the internet,[9] re-purposed data that was originally collected for a different purpose,

[4] See for example Article 5(1) of the UK GDPR which summarises the principles relating to data protection.
[5] Article 5(1)(a) of the UK GDPR which requires that personal data be processed transparently. See also Articles 12, 14 and 15 which, amongst others, give effect to the principle of transparency.
[6] Joe McKendrick, *Forbes*, 'The data Paradox: Artificial Intelligence Needs Data; Data Needs AI' 27 June 2021, available here: https://www.forbes.com/sites/joemckendrick/2021/06/27/the-data-paradox-artificial-intelligence-needs-data-data-needs-ai/
[7] Amit Yadav, Medium, 'Training Data Explained in Detail', 23 August 2024, available here: https://medium.com/@amit25173/training-data-explained-in-detail-2f152c46c290
[8] Shayne Longpre, Robert Mahari, Naana Obeng-Marnu et al, 'Data Authenticity, Consent, and Provenance for AI Are All Broken: What Will It Take to Fix Them?' *An MIT Exploration of Generative AI*, March 2024, available at: https://mit-genai.pubpub.org/pub/uk7op8zs/release/2
[9] Greg McDonough, 'Privacy Risks in Training Data and How to Adress them', 28 October 2025, available here: https://www.rsaconference.com/library/blog/privacy-risks-in-training-data-and-how-to-address-them

or data purchased from a private company specifically for training.[10] The scale and diversity of datasets may complicate controllers' ability to establish what personal data the training data contains, about whom, from what source, or whether relevant data subjects were ever notified. Another resulting risk is failure to comply with the principle of data minimisation, especially where data is collected and further processed 'just in case'.

6. Further, this data doesn't simply pass through, but can be "ingested" into the models themselves.[11] Models can memorise parts of their training data, so personal data may persist inside the model itself.[12] This "ingested data" may differ from the original training points and be "represented through mathematical objects",[13] but will likely still constitute personal data: any claims that an AI model contains only anonymous data must be carefully assessed on a case-by-case basis.[14] If training data is not stored in its original form it may make it difficult to identify, isolate, trace or remove certain aspects of it. This poses a risk to effective responses to data protection rights of access, rectification and deletion.

7. In addition, differentiating between personal and anonymous data is made more uncertain by AI. Data, which by itself may be considered innocuous or anonymised can be combined with other datasets to re-identify people or reveal more sensitive information.[15] This is known as the "mosaic effect."[16] AI may enhance abilities to do this because it can combine and analyse different data sources and identify patterns and correlations between them to reveal information or

---

[10] Eg Suzanne Rowan Kelleher, Forbes, 'Google's 'Outrageous' Plan to Train AI Using Spirit Airlines' Data Blasted By Flight Attendant Union', 18 August 2026, available here: https://www.forbes.com/sites/suzannerowankelleher/2026/08/18/google-train-ai-spirit-airlines-data/

[11] The European data Protection Board, 'Opinion 28/2024 on Certain Data protection Aspects Related to the Processing of personal Data in the Context of AI Models', adopted on 17 December 2024: available here: https://www.edpb.europa.eu/documents/opinion-of-the-board-art-64/opinion-282024-on-certain-data-protection-aspects-related-to_en. Para 31.

[12] Ibid.

[13] Ibid.

[14] Ibid, para 34.

[15] Centre for humdata, United Nations Office for the Coordination of Humanitarian Affairs, 'Mosaic Effect', available at: https://centre.humdata.org/glossary-2/mosaic-effect/

[16] Ibid.

inferences that may not be apparent from a single dataset.[17] A controller may therefore hold data it believes is anonymous, but which is in fact personal data. Although it is a criminal offence, in certain circumstances, to re-identify de-identified data, [18] this offence polices misconduct: it doesn't restore the controller's knowledge.

8. The risk of onwards identifiability – when data treated as anonymous by one actor can be re-identified by another – must also be taken seriously in the context of AI. Proposals such as those contained in the EU Commission's GDPR omnibus (ie to amend Article 4) would significantly narrow the definition of personal data, therefore creating loopholes in data protection law, and undermining people's rights.[19] They should be avoided.

9. Another challenge concerns the indeterminacy of purpose. Data protection law requires that data be collected for explicit and specified purposes,[20] with further processing confined to compatible uses.[21] But general-purpose AI models are built precisely to be turned to tasks that cannot be specified in advance.[22] An overly lax approach here could open the doorway to normalisation of large-scale data accumulation practices in breach of purpose limitation provisions. Greater upstream transparency and participation of data subjects in the design of general-purpose AI models (including through Data Protection Impact Assessments

---

[17] Gary LaFever, IAPP, 'Beyond GDPR: Unathorized Reidentification and the Mosaic Effect in the EU AI Act', 10 August 2023, available here: https://iapp.org/news/a/beyond-gdpr-unauthorized-reidentification-and-the-mosaic-effect-in-the-eu-ai-act and EDPB, 'Guidelines 02/2026 on Anonymisation v1.0' paras 83-93, available here: https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en

[18] Section 171 of the Data Protection Act, 2018.

[19] See EDPB-EDPS Joint Opinion 2/2026 'On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)', para 17, available here: https://www.edps.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf

[20] Article 5(1) of the UK GDPR.

[21] Article 8A of the UK GDPR.

[22] Florina Pop, Michaela Sullivan-Paul and Leila Debiasi, European Institute of Public Administration, 'Understanding General Purpose AI', 11 March 2025, available here: https://www.eipa.eu/blog/understanding-general-purpose-ai/

(DPIAs)) may be one way to help ameliorate these risks, if done in a meaningful way.

10. A controller that doesn't know whose data its training set contains cannot notify those data subjects.[23] Article 14(5)(e) removes the obligation to notify data subjects if doing so is "impossible or would involve a disproportionate effort."[24] The difficulties identified above make it possible that this exemption will sought to be relied on excessively as AI scraping or vast data collection becomes the norm. If such an approach is permitted, then correlative data subject rights including the rights of access, rectification, erasure, and objection, are effectively rendered meaningless. A data subject who is unaware that their information is being processed is unlikely to exercise these rights. This is particularly so in light of the limitations of DPIAs. While they can be important procedural safeguards, they don't increase transparency for affected data subjects because they are not mandatory in every instance, it is not obligatory to publish them, and data subjects are not involved in their production.[25]

11. Further, if a controller is unaware that they are processing special category data, they may unwittingly breach the provisions concerning special categories of personal data.[26] As companies seek to further integrate AI models into their products and services, this exemption must not create a loophole in data protection when large scale scraping and combining of data takes place.

Process

12. The law assumes controllers understand their own processing well enough to explain it. AI challenges this assumption in two ways. First, through its opacity, also known as the "black box" problem. An AI system's immediate inputs (data)

---

[23] As required in terms of Article 14 of the UK GDPR, where personal data was not obtained directly from the data subject.
[24] Article 14(5)(e) of the UK GDPR.
[25] Information Commissioner's Office, 'Data Protection Impact Assessments', available here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-impact-assessments/
[26] Article 9 of the UK GDPR.

and outputs (predictions or decisions) can be observed, but the internal process by which it turns one into the other is often far too complex, opaque or uninterpretable to be understood by humans (including its developers).[27]

13. These opacity challenges in the process stage make it difficult for data to be processed "in a transparent manner", as required by Article 5(1)(a).[28] Various provisions in the UK GDPR[29] require that the data subject be provided with "meaningful information about the logic involved."[30] But the difficulties outlined above make this duty difficult to discharge. Information that a controller cannot itself understand or interpret is unlikely to be meaningful to a data subject.

14. This concern is heightened in the context of recent changes made to the ADM provisions of the UK GDPR[31] (discussed in more detail below). As characterised by the Information Commissioner's Office (ICO), "[t]he amendments reframe the ADM provisions from a prohibition with exceptions to a right of challenge with safeguards."[32] The safeguards require controllers to notify data subjects about ADM decisions taken,[33] enable them to make representations,[34] obtain human intervention[35] and contest such decisions.[36] These safeguards are designed to protect data subjects against (misuse of) ADM, but the challenges discussed above undermine their effectiveness. They only work if individuals can understand enough about the decision. It is difficult to challenge reasoning that is opaque

---

[27] Bartosz Brożek and Michal Furman et al, 'The Black Box Problem Revisited. Real and Imaginary Challenges for Automated Legal Decision Making' Artificial Intelligence and Law, 4 April 2023, available at: https://link.springer.com/article/10.1007/s10506-023-09356-9

[28] UK GDPR.

[29] Articles 13(2)(f), 14(2)(g) and 15(1)(h) of the UK GDPR.

[30] Ibid.

[31] Section 80 of the Data (Use and Access) Act 2025 which replaced Article 22 of the UK GDPR with Articles 22A – 22D.

[32] Ruth Boardman, Emma drake et al, Bird & Bird, 'ICO Launches Consultation on Draft Guidance on Automated Decision-Making and Profiling', 5 May 2026, available here: https://www.twobirds.com/en/insights/2026/ico-launches-consultation-on-draft-guidance-on-automated-decision-making-and-profiling

[33] Article 22C(2)(a) of the UK GDPR.

[34] Article 22C(2)(b) of the UK GDPR.

[35] Article 22C(2)(c) of the UK GDPR.

[36] Article 22C(2)(c) of the UK GDPR.

and incomprehensible, and a reviewer would need to understand it enough to intervene. So, while these safeguards exist in law, they may prove difficult to exercise in practice. The advent of AI accordingly demands greater clarity on what constitutes meaningful information about the logic involved.

15. AI systems offer features which seek to augment user prompts with additional information to provide more personalised responses to queries (such as 'memory' or retrieval-augmented Generation (RAG). Features like these process user data (which may include personal data) in ways which may be unexpected, or poorly explained to and/or understood by the data subject. Users must retain control over this further ingesting of their data, and it must be done in line with the principles of data minimisation and transparency. Caution is also needed in general over such features because of how they can consolidate large amounts of personal data (and access to user services/accounts) in one place. This can create an attractive target for malicious attacks and/or inappropriate government use.

16. Agentic AI systems can also pose questions for existing data protection frameworks. For example:

    16.1. Agentic tools may look up and then process personal data in ways that were not expected or anticipated by developers. Such processing may require fresh assessment of compliance with data protection law (eg identification of legal basis) and trigger transparency requirements. However, it is unclear how that can be done in the middle of an agentic operation.

    16.2. Agentic systems may combine AI models together in ways that result in personal data being brought together with negative consequences. For example, data that was previously successfully anonymised may become re-identifiable, or it may be combined with other data to make inferences or used in ways which have not been adequately explained to data subjects and in potential violation of purpose limitation.

Output

17. Data protection law assumes controllers can anticipate the results of their processing, and the consequences for data subjects. But AI systems can generate new personal data in the form of regurgitations or inferences,[37] including outputs that are incorrect ('hallucinations').[38] Inferences are predictions or assumptions about a person derived from data already held.[39] For example, a name may be used to infer religion or ethnicity, or shopping habits to infer pregnancy or illness. These inferences themselves can be personal data. [40] Such outputs are probabilistic and can be inaccurate or wrong.[41] They also work within the "mosaic effect", discussed above, and could turn innocuous data into personal data or special category data. Because inferences are created after collection, they may occur after the moment at which purpose and lawful bases are fixed and explained.[42] Accordingly, the data subject will be told or aware of only the data they gave, not the data that was made. This inferred data, even if incorrect, could impact a decision or outcome, even when a data controller is unaware of its existence.

18. When such inferences amount to personal data, the rights of access, rectification and erasure apply to them. However, a data subject cannot request access to an

---

[37] Information Commissioners Office and the Alan Turing Institute, 'Explaining Decisions made with AI', October 2022, available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/ page 19.
[38] Nick Evershed et al, The Guardian, 'Scary': How Misinformation and AI Hallucinations are Infiltrating Australia's Parliament', 31 August 2026, available here: https://www.theguardian.com/australia-news/2026/sep/01/how-misinformation-ai-hallucinations-infiltrating-australian-parliament
[39] Joan M Wrabetz, What is Inferred Data and Why is it Important', American Bar Association, 22 August 2022, available here: https://www.americanbar.org/groups/business_law/resources/business-law-today/2022-september/what-is-inferred-data-and-why-is-it-important/
[40] Information Commissioner's Office, 'Guidance for the Use of Personal Data in Political Campaigning' 17 October 2022, available at: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/personal-data/.
[41] Andreas Häuselmann and Bart Custers, 'The Right to Rectification and Inferred Personal Data', European Journal of Law and Technology, Vol.15 No.13 (2024), page 1, available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5116221.
[42] Article 13 of the UK GDPR requires that this information be provided to data subjects at the time of collection.

inference they don't know exists. The right to rectification assumes data can be shown to be "inaccurate"[43], but if an inference is a probabilistic estimate as opposed to a fact, it is not clear whether it passes this threshold.[44] The right to erasure assumes that data can be located and deleted, but as noted above, personal data "absorbed" by a model may not be conventionally located, and it may be impossible to make it forget or 'unprocess' the data.[45] Accordingly, it may be reproduced or recreated from the model itself, even if the input data is deleted. Guardrails are inevitably limited in their ability to prevent an AI from outputting personal data. These rights accordingly exist in principle but are difficult to exercise. Moreover, controllers cannot discharge their obligations under the accuracy principle simply by warning users that AI systems may produce errors. A disclaimer may alert users to the risk of error, but it does not mitigate the underlying data protection risks arising from inaccurate personal data being generated, reproduced or relied upon.

19. These characteristics of AI accordingly challenge the foundational assumptions of data protection law: that controllers are able to maintain sufficient knowledge and control over the personal data they hold. As discussed, this poses a significant challenge for transparency and the exercise of data protection rights.. The combination of these technological characteristics and recent legislative changes (eg to limit the right of access to what a "reasonable and proportionate search"[46] can find) should not be interpreted in a manner that creates practical exemptions from data protection obligations. Where the application of existing safeguards is uncertain or ineffective in the AI context, those gaps should be closed through

[43] Article 16 of the UK GDPR enables the data subject to obtain "the rectification of inaccurate personal data."
[44] For more on this see: Sandra Watcher and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI', Columbia Business Law Review Vol.2019, issue 2, available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829.
[45] Seth Neel, 'How to Make AI 'Forget' All the Private Data it Shouldn't Have', Harvard Business School, 22 February 2024, available at: https://www.library.hbs.edu/working-knowledge/qa-seth-neel-on-machine-unlearning-and-the-right-to-be-forgotten.
[46] Article 15(1A) of the UK GDPR.

legislative intervention to ensure that technological complexity does not erode important data protection safeguards.

Automated decision-making

20. The Data (Use and Access) Act 2025 (DUAA), made significant changes to the provisions on automated decision making (ADM).[47] Significantly, it shifted from a model where ADM was generally prohibited (subject to exceptions and the implementation of safeguards)[48] to a model where such decisions are generally permitted.[49] Now, only significant decisions involving special category data remain prohibited (subject to exceptions and conditions).[50]

21. These changes raise particular concerns relating to how AI may be used in ADM:

    21.1. **The rights of marginalised groups:** The Government has acknowledged that "those with protected characteristics such as race, gender, and age are more likely to face discrimination from ADM due to historical biases in datasets."[51] The prohibition on ADM involving special category data does not effectively mitigate the risk that marginalised groups are at greater risk of opaque, unfair and harmful automated decisions.[52] This is because personal data, not classified as special category data, can act as a proxy for protected characteristics or special category data when used in ADM.[53]

---

[47] Section 80 of the Data (Use and Access) Act 2025 which replaced Article 22 of the UK GDPR with Articles 22A – 22D.
[48] ADM was previously permitted in narrow circumstances: if it was necessary for the implementation of a contract with the data subject, authorised by law or based on data subject consent
[49] Bird & Bird 'ICO Launches Consultation on Draft Guidance on Automated Decision-Making and Profiling' 5 May 2026, available here: https://www.twobirds.com/en/insights/2026/ico-launches-consultation-on-draft-guidance-on-automated-decision-making-and-profiling
[50] Article 22B(1) of the UK GDPR. AI poses challenges to the requirements pf explainability and meaningful human oversight which are discussed above, see paras 10 – 12.
[51] Data (Use and Access Bill), Impact Assessment from DSIT, 23 October 2024: https://bills.parliament.uk/publications/56548/documents/5221, para 531, p.163
[52] Big Brother Watch, 'Briefing on the Data (Use and Access) Bill for Committee Stage in the House of Lords', December 2024, available here: https://bigbrotherwatch.org.uk/wp-content/uploads/2024/12/Big-Brother-Watchs-Briefing-on-the-Data-Use-and-Access-Bill-House-of-Lords-Committee-Stage_.pdf, para 31.
[53] Ibid, para 32.

These concerns are exacerbated because ADM outputs depend on the quality of their training data. Biases in data may act to further reinforce discrimination.[54]

21.2. **The burden shifts from controllers to data subjects:** rather than requiring controllers to justify the use of ADM, such processing is now generally assumed to be compliant unless it can be shown that the required safeguards have not been complied with.[55] This places the burden of proof on data subjects who, if the safeguards weren't complied with (and they therefore weren't notified) may not even know that such a decision was taken.

21.3. **Opacity challenges undermine remaining safeguards:** As discussed above, while safeguards remain for ADM, they depend on both the data subject and the reviewer being able to understand the reason for the decision. This is difficult, if not impossible, when the underlying reasoning is opaque. The ability to exercise these safeguards and challenge such decisions are accordingly difficult in practice.

Theme 5 – Effectiveness of data frameworks in regulating AI

Prompt question 1: Overall, what is working well, where have you observed disproportionate or unintended barriers in practice, and where have risks to data protection arisen?

[54] ADR UK, 'Bias in Administrative Data and in Linked Data', available at: https://www.adruk.org/learning-hub/skills-and-resources-to-use-administrative-data/bias-in-administrative-data-and-in-linked-data/

[55] Matt Davies, Ada Lovelace Institute, 'It's Time to Strengthen Data Protection Law for the AI Era', 18 March 2024, available here: https://www.adalovelaceinstitute.org/blog/strengthen-data-protection-law-ai-era/.

The gap concerning prohibited uses

22. Data protection laws [56] are currently the most comprehensive frameworks regulating AI in the United Kingdom.[57] However, they do not address all AI-related risks and there are accordingly significant gaps in the overall regulation of AI. The most significant of which concerns prohibited uses. Certain uses of AI, and the ways in which they process personal data, pose such a high-risk of violating human rights that they should not be permitted. This would be consistent with other prominent AI policies, including the EU AI Act. They also reflect the consensus of the international community (including UN General Assembly Resolutions[58]) and independent international human rights experts such as the UN Special Rapporteur on counter-terrorism and human rights.[59] These include:

    22.1. **Sentiment analysis:** processing personal data to detect measure or infer a person's emotional state;
    22.2. **Behavioural prediction:** processing personal data to predict the likelihood a person will commit a crime or be a threat to national security based solely on AI profiling or assessing their personality traits and characteristics;
    22.3. **Profiling based solely on protected activities:** processing personal data to profile, target or track a person based solely on the exercise of their human rights, including freedom of expression and assembly;
    22.4. **"Live" identification of a person based on biometrics:** processing biometric data for the purposes of real-time remote identification of a person;

[56] Including the United Kingdom General Data Protection Regulation (EU) 2016/679, the Data Protection Act 2018 and the Data Use and Access Act 2025.
[57] Brendan McGurk KC and Joe Tomlinson, 'Artificial Intelligence and Public Law', Bloomsbury Publishing 2025, page 60.
[58] See United Nations Resolutions A/RES/78/265 and A/RES/80/215.
[59] United Nations Office of the High Commissioner, 'Protecting Human Rights While Using Artificial Intelligence to Counter Terrorism', 15 December 2025, available here: https://www.ohchr.org/en/documents/position-papers/protecting-human-rights-while-using-artificial-intelligence-counter

22.5. **Scraping to create biometric databases:** using AI to collect personal data to create or expand biometric databases through the untargeted scraping of biometrics and personal data from the internet or CCTV footage.

The gap concerning competition and data protection

23. A further gap concerns the intersection between competition and data protection. Risks to data protection and individuals' privacy may arise where dominant firms are able to leverage their existing market power to shape the development of the AI market and accrue more control over (and potentially misuse of) people's data. This may reduce the availability and viability of more privacy-protective alternatives, limit meaningful consumer choice, and ultimately lead to poorer privacy outcomes and wider societal harm.[60]

The gap concerning intelligence services data breaches

24. There is also a significant oversight gap in relation to intelligence service data breaches which may be exacerbated by increased AI use. Section 108(1) of the Data Protection Act 2018 (DPA) requires intelligence services (when they are the controller) to notify the Commissioner if they become aware of a serious personal data breach.61 However, they do not have to do so "if the breach also constitutes a relevant error within the meaning given by section 231(9) of the Investigatory Powers Act 2016" (IPA).62

25. Section 231(9) of the IPA defines a relevant error as an error "by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment, and which are subject to review by a Judicial Commissioner […]."[63] The Investigatory Powers Commissioner's Office (IPCO) has

[60] For more on this see: Privacy International, 'Competition and Data' available here: https://privacyinternational.org/learn/competition-and-data
[61] Section 108(1) of the Data Protection Act 2018.
[62] Section 231(9) of the Investigatory Powers Act 2016.
[63] Section 231(9) of the Investigatory Powers Act 2016.

included it in its 'useful definitions' resource and defines it as "an error made by a public authority when carrying out activity overseen by IPCO."[64]

26. The effect is that if a data breach also constitutes a 'relevant error' then the intelligence services do not have to report it to the Information Commissioner. However, the IPCO has no powers or functions concerning data protection, and accordingly no relevant enforcement or remedial powers. The effect of this is to circumvent the enforcement and oversight role of the ICO related to data breaches. This gap was noted by IPCO in its 2024 Annual Report:[65]

"It is unclear what the rationale is for UKIC [United Kingdom Intelligence Community] avoiding the notification requirement to the ICO, given that we have no functions in relation to data protection compliance and cannot exercise the enforcement powers in Part 6 of the Data Protection Act 2018 (DPA). At present, this means that UKIC could commit a serious personal data breach which might not come to the attention of the competent supervisory authority for data protection unless we refer the matter. Given the possible sensitives involved, we are not best placed to do this. This may leave a gap which could be contrary to the public interest."

27. This oversight gap is likely to become increasingly significant as intelligence services make greater use of AI systems. AI can amplify the scale and consequences of data breaches, particularly in light of the large volumes of personal data involved. If breaches involving AI systems fall within the definition of a "relevant error", there is a risk that the ICO may not be notified despite the potentially significant impact on rights. In such circumstances, robust and independent oversight of personal data breaches become more, rather than less, important.

---

[64] IPCO, 'Useful Definitions', available here: https://www.ipco.org.uk/investigatory-powers/useful-definitions/

[65] IPCO, 'Annual Report of the Investigatory Powers Commissioner 2024', available here: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2024.pdf

The risks of regulatory blind spots

28. The lack of a clearly defined purpose for AI models also creates wider challenges for its effective governance beyond the data protection challenges relating to purpose limitation outlined above. Proper scrutiny of its development and deployment may be evaded if there are not adequate frameworks and institutions that can weigh up its wide range of risks, harms, public benefits and costs, and take action where necessary.

Conclusion

29. Thank you for the opportunity to submit responses to the call for evidence on data regulation in the age of AI and other data-intensive technologies. We hope the Department for Science, Innovation & Technology reviews and responds to the data protection challenges posed by AI.