Regulating AI:
The ICO's strategic approach
April 2024

ico.
Information Commissioner's Office

About the ICO

The Information Commissioner has responsibility in the UK for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003 (PECR), among others.

The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken.

The Information Commissioner's Office (ICO) sets out its strategic vision in the ICO25 plan, which highlights promoting regulatory certainty, empowering responsible innovation and safeguarding the public as key priorities.

Contents

About the ICO 2
Introduction 4
Part 1: The opportunities and risks of AI 4
Part 2: The role of data protection law 8
Part 3: Our work on AI 13
Part 4: Upcoming developments 16
Part 5: Working together 18
Annex: Our capabilities 21

Introduction

1. At the ICO, we support the government's ambition to make sure that artificial intelligence (AI) is adopted in ways that make the UK the smartest, healthiest, safest and happiest place to live and work. We believe that data protection is a crucial part of making this a reality.

2. This document sets out the ICO's strategic approach to AI regulation, in response to a request by the Secretary of State for Science, Innovation and Technology.[1] It explains how we are driving forward the principles set out in the AI Regulation White Paper[2] and the government's guidance on implementing these.[3]

Part 1: The opportunities and risks of AI

3. The potential of AI is undeniable. From unlocking medical advances to creating new forms of entertainment, it offers huge potential to transform our lives for the better. Its autonomy, adaptivity and unprecedented scaling are enabling our society to solve new problems, become more efficient – and have more fun.

4. But these benefits could be compromised if the inherent risks of AI development and deployment are not mitigated. Legitimate concerns exist about matters such as fairness and bias; transparency and explainability; safety and security; or accountability and redress. AI does not only exacerbate existing risks because of its autonomy, adaptivity or scaling, it can also create novel risks.

5. Many of these risks derive from how data – and specifically personal data – is used in the development and deployment of AI systems. Wherever processing of personal data takes place this will fall under the ICO's purview, as the UK's data protection regulator. The ICO has the ability and the tools to intervene right across the AI supply chain, from model developers to deployers, depending on where risks may be greatest or mitigations most effective.

6. Data protection law is technology-neutral. It applies to any processing of personal data, no matter what technology is being utilised to undertake

[1] Letter from DSIT Secretary of State to the Information Commissioner's Office | GOV.UK
[2] A pro-innovation approach to AI regulation | GOV.UK
[3] Implementing the UK's AI Regulatory Principles | GOV.UK

that processing. It is therefore adaptable and able to respond to new technologies, including advances in AI.

In focus: foundation models

The UK government defines foundation models as "machine learning models trained on very large amounts of data that can be adapted to a wide range of tasks."[4]

Similarly, the EU AI Act defines general purpose AI as "models displaying significant generality and capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications."

Such models are typically developed using personal data, in order to enable them to be deployed for a general set of purposes. While data protection law does not explicitly reference foundation models or general-purpose AI, the scope of the legislation enables the ICO to intervene wherever personal data is processed.

Data protection law applies to every stage of the model lifecycle and every actor within the supply chain where personal data is being processed, enabling the ICO to act on concerns around matters such as fairness and transparency both upstream and downstream. Fines for non-compliance can be set at up to 4% of annual global turnover.

7. Data protection law is risk-based. Organisations who are accountable for the processing of personal data are expected to identify the risks, mitigate them and be able to demonstrate how they achieve this. The severity and likelihood of the risks to people and their rights will heavily rely on the context in which AI is being applied and the circumstances of the people involved. By placing accountability on organisations, we allow them to adopt the approach that is most suitable to their context and operational objectives.

8. We require risks to be mitigated and managed via technical and organisational measures, but not necessarily completely removed. This enables a flexible approach that is context-specific and suitable for a technology that is probabilistic in nature and therefore has a margin of error. Where organisations identify a high risk to the rights and freedoms of

[4] A pro-innovation approach to AI regulation: government response | GOV.UK

individuals that they cannot mitigate sufficiently, they are required to consult the ICO.

9. To assist organisations in identifying and mitigating risks, the ICO has produced its award-winning AI and Data Protection Risk Toolkit,[5] which builds on our Guidance on AI and Data Protection.[6] Our Harms Taxonomy sets out how the ICO evaluates risks and harms, capturing both material and non-material impacts such as adverse effects on people's rights and freedoms.[7]

10. The ICO welcomes the approach taken by the government to build on the strengths of its existing regulators, who are well-placed to tackle the AI risks that emerge in their context. We do not consider that the risks relating to AI require new, extensive, cross-cutting legislation, but appropriate resourcing of existing UK regulators and their empowerment to hold organisations to account.

In focus: high-risk AI applications

Consensus is building across the world around contexts in which AI risks may be greater. For example, the White House's Executive Order on the Safe, Secure and Trustworthy Development and Use of AI[8] raised concerns around the risk of harm, including discriminatory outcomes, in contexts such as education, healthcare, financial services, law, education, recruitment.

Equally, the EU AI Act lists AI applications used in education, administration of justice, welfare provision, employment and biometrics as some of the high-risk applications, with a list of banned applications that include emotion recognition in the workplace, manipulative AI and predictive policing solely based on profiling.

Data protection law can mitigate many of the risks these initiatives are seeking to address. For example, the fairness principle already requires organisations to not undertake data processing that has unjustifiably adverse effects on individuals. The ICO has already issued warnings regarding emerging AI uses such as emotion recognition technology[9].

[5] AI and data protection risk toolkit | ICO
[6] Guidance on AI and data protection | ICO
[7] Overview of Data Protection Harms and the ICO Taxonomy | ICO
[8] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | The White House
[9] 'Immature biometric technologies could be discriminating against people' says ICO in warning to organisations | ICO

11. While some risks derive from the specific contexts in which AI is deployed (e.g. healthcare, law enforcement or education) others derive from the AI development process. For example, facial recognition technology built on inaccurate or unrepresentative datasets may have discriminatory outcomes regardless of the context in which it will be applied, so due diligence and operational testing are necessary.

In focus: facial recognition technology and biometrics

Facial recognition technology (FRT) has been one of the first AI applications to become the focus of significant public debate, both in the UK and abroad. The ICO has provided clarity on our expectations around what responsible use of FRT looks like through our opinions on the use of live FRT in public spaces[10] and in particular, its use by law enforcement.[11]

We recognise the potential benefits that appropriately governed, regulated and deployed FRT can provide to issues such as security and public safety. However, whether deployments are for law enforcement purposes or other reasons, all FRT deployments must be proportionate and strike the correct balance between privacy intrusion and the purpose they are seeking to achieve.

We have also produced guidance on wider uses of biometric recognition technologies[12] which provides specific and practical issues organisations should consider when thinking of using these technologies. These range from the nature of 'decisions' made by biometric recognition systems, to how to consider data rights requests appropriately and how to keep biometric data secure.

12. Vulnerable groups including children are more exposed to risks and organisations using or deploying AI need to factor this into their overarching risk management framework.

In focus: children and AI

The Age-Appropriate Design Code ('the Children's code') requires online services to provide better privacy protections for children, ensuring their personal information is protected within the digital world – including when it is processed using AI. Through our scrutiny of organisations' practices, we

[10] The use of live facial recognition in public places | ICO
[11] The use of live facial recognition technology by law enforcement in public places | ICO
[12] Biometric data guidance: Biometric recognition | ICO

have influenced significant progress on children's privacy online, including changes from some of the largest social media and video sharing platforms.

In March 2024, we launched our children's code strategy for 2024/25 in order to drive further progress.[13] Among the issues we will prioritise when scrutinising platforms is their use of children's information in recommender systems – algorithmically-generated content feeds which may use information such as behavioural profiling and analysis of children's search results to recommend content.

We have also taken action where we have concerns about potential harm to children as a result of AI products and services. For example, we investigated Snap's risk assessment process in relation to its 'My AI' generative AI chatbot, with a particular focus on ensuring that risks to children were appropriately identified and mitigated. We will continue to act to ensure that children's privacy is protected online.

13. Many AI risks will sit outside of data protection law, or be addressed more effectively through other regulatory regimes. For example, data protection law offers little protection against the use of AI to develop new biological or chemical threats. It cannot tackle the threat to national security and election integrity from development of synthetic media ('deepfakes') by hostile states. The ICO is working with the AI Safety Institute on the risks that fall within its remit.

Part 2: The role of data protection law

14. Data protection law is principles-based. This provides a flexible framework that enables organisations to adapt to evolutions in AI technology. The principles set out in the AI Regulation White Paper consultation mirror to a large extent the statutory principles the ICO already oversees (see Table 1).[14]

[13] Protecting children's privacy online: Our Children's code strategy | ICO
[14] A guide to the data protection principles | ICO

Principles of data protection law	Principles in the White Paper
• Integrity and confidentiality (security) • Lawfulness, fairness and transparency • Accountability • Purpose limitation • Data minimisation • Accuracy • Storage limitation	• Safety, security, robustness • Appropriate transparency and explainability • Fairness • Accountability and governance • Contestability and redress

Table 1: Principles of data protection law and in the AI Regulation White Paper

15. The government's voluntary guidance clarifies that its goal is not to duplicate, replace or contradict regulators' existing statutory definitions of principles. We explain below how the ICO's existing statutory principles map to the proposed AI Regulation White Paper principles. In this sense, the ICO already has active experience of implementing the aims and objectives of the AI Regulation White Paper principles.

Safety, security, robustness

> *"AI systems should function in a robust, secure and safe way throughout the AI life cycle, and risks should be continually identified, assessed and managed."*
>
> AI Regulation White Paper, UK Government, 2023[15]

16. Security is a data protection principle.[16] Organisations must ensure appropriate levels of security against data's unauthorised or unlawful access, processing, accidental loss, destruction or damage. AI introduces novel security risks that need to be mitigated and this is covered in the ICO's Guidance on AI and Data Protection.[17] These include membership inference attacks or model inversion.

17. The security of data is a pillar of other frameworks the ICO oversees such as the Network and Information Systems Regulations. We work closely with stakeholders including the National Cyber Security Centre (NCSC) to tackle security challenges. The ICO is a member of the NCSC AI Working Group and provides input into the Cyber Regulators Forum, which has been considering matters related to AI and cybersecurity.

---

[15] A pro-innovation approach to AI regulation | GOV.UK
[16] The ICO has produced guidance on security: A guide to data security | ICO including as part of its Guidance on AI and Data Protection: How should we assess security and data minimisation in AI? | ICO
[17] How should we assess security and data minimisation in AI? | ICO

Appropriate transparency and explainability

> *"AI systems should be appropriately transparent and explainable."*
>
> AI Regulation White Paper, UK Government, 2023

18. Transparency is also a data protection principle. This is about being clear, open and honest with people from the start about who organisations are, and how and why they use their personal data.

19. Transparency requirements can extend beyond the provision of information regarding the processing of personal data in the development or deployment of AI systems. Where AI powers solely-automated decisions with legal or similarly significant effects, organisations are required to be able to explain the 'logic' of their AI systems.

20. The ICO, in conjunction with the Alan Turing Institute (ATI), has produced guidance on Explaining Decisions Made with AI[18] to support organisations in explaining systems and their decisions to people.

Fairness

> *"AI systems should not undermine the legal rights of individuals or organisations, discriminate unfairly against individuals or create unfair market outcomes. Actors involved in all stages of the AI life cycle should consider definitions of fairness that are appropriate to a system's use, outcomes and the application of relevant law."*
>
> AI Regulation White Paper, UK Government, 2023

21. Fairness is a key data protection principle. Put simply, it means that organisations should only handle personal data in ways people would reasonably expect, and not in ways that have unjustified adverse effects on them.

22. The concept of fairness in data protection law is more holistic than notions of algorithmic fairness that focus on the distribution of outcomes among a group as it also accounts for the relationship between those groups and the organisations processing their data. Just because a system is statistically accurate it does not necessarily mean its use is fair under data protection law – other factors will also play a role.

23. Data protection fairness considers contextual factors such as the environment in which a system is deployed or the power dynamic between

[18] Explaining decisions made with AI | ICO

people and the organisations processing their data. It is context-specific, so organisations need the ability to evaluate their fairness-related choices (eg financial services and healthcare may need to consider fairness differently) while being accountable for them.

24. Our AI and Data Protection Guidance[19] provides a roadmap for how organisations should evaluate their data protection fairness obligations. The ICO continues our work on fairness in AI by supporting the Fairness Innovation Challenge[20], in partnership with the Department for Science, Innovation and Technology (DSIT) and the Equality and Human Rights Commission (EHRC). We have worked on concepts of fairness with counterparts in the Digital Regulation Cooperation Forum (DRCF),[21] and contributed to the ATI's 'AI Fairness in Practice' workbook.[22]

Accountability and governance

> *"Governance measures should be in place to ensure effective oversight of the supply and use of AI systems, with clear lines of accountability established across the AI life cycle.*
>
> *"AI life cycle actors should take steps to consider, incorporate and adhere to the principles and introduce measures necessary for the effective implementation of the principles at all stages of the AI life cycle."*
>
> AI Regulation White Paper, UK Government, 2023

25. Accountability is a data protection principle. It requires organisations to take responsibility for what they do with people's personal data but also how they comply with all the other data protection principles.

26. Accountability is allocated on the basis of roles defined in legislation (controllers, processors or joint controllers[23]), according to who defines the means and purposes of the processing. A crucial step in demonstrating accountability is undertaking a data protection impact assessment (DPIA) to identify and mitigate the data protection risks associated with the processing.

27. The ICO has developed an overarching Accountability Framework[24] and AI-specific guidance on accountability[25] that we continue to update. Following

---

[19] How do we ensure fairness in AI? | ICO
[20] Fairness Innovation Challenge
[21] Fairness in AI: A View from the DRCF | DRCF
[22] AI Ethics and Governance in Practice: AI Fairness in Practice | The Alan Turing Institute
[23] Controllers and processors | ICO
[24] Accountability Framework | ICO
[25] What are the accountability and governance implications of AI? | ICO

recommendations by the Vallance Review[26], we intend to further clarify the responsibilities of AI developers and deployers as part of our generative AI consultation series.[27]

28. We are also working to ensure that organisations procuring systems can be assured that AI supply chain actors providing their services and products have undertaken the appropriate to due diligence. In conjunction with the EHRC, the London Office of Technology and Innovation, and the Local Government Association, we plan to develop guidance for local authorities who are procuring AI products and services. This follows the work we have done with our DRCF partners on transparency in AI procurement.[28]

Contestability and redress

> *"Where appropriate, users, impacted third parties and actors in the AI life cycle should be able to contest an AI decision or outcome that is harmful or creates material risk of harm."*
>
> AI Regulation White Paper, UK Government, 2023

29. The AI White Paper's contestability and redress principle is not a principle of data protection law but is instead reflected in a set of information rights that individuals can exercise, such as the right of access to personal data being processed about them. Of particular note are the rights in relation to solely automated decision-making with legal or similarly significant effects on individuals.[29]

30. A legal effect is something that affects someone's legal rights. For example, someone's entitlement to child or housing benefit. A similarly significant effect is generally something that has the same sort of impact on someone's circumstances or choices. For example, a computer decision to offer someone a job, or a decision to agree or decline a person's mortgage application. These effects can be positive or negative.

31. These data protection provisions enable people to contest decisions they deem unfair when they are solely automated. When decision-making is assisted by AI and is not captured by these provisions, people can still exercise their information rights such as the rights to access, rectification and exercise control on data that relates to them and by implication any

---

[26] HMG_response_to_SPV_Digital_Tech_final.pdf (publishing.service.gov.uk)
[27] ICO consultation series on generative AI and data protection | ICO
[28] Transparency in the procurement of algorithmic systems: Findings from our workshops | DRCF
[29] See Article 22 of the UK GDPR, Sections 49 and 50 of the DPA 2018. These provisions are subject to amendment by the Data Protection and Digital Information Bill.

decisions this data led to. Facilitating the exercise of these rights also aligns with the fairness principle.

Changes in data protection law

32. UK data protection law is changing, but the ICO's role in regulating AI continues. The Data Protection and Digital Information Bill, which is currently passing through Parliament, will complement the existing framework comprising the UK GDPR and the Data Protection Act 2018. Our future approach to AI regulation will be informed by the new legal framework we will be tasked with overseeing.

Part 3: Our work on AI

33. AI is not new, and the ICO has been regulating this field for well over a decade. Our landmark report on Big Data, Artificial Intelligence, Machine Learning and Data Protection[30] was first published in 2014. Below, we summarise the range of guidance, advice, assurance and enforcement we have taken forward.

Our policy and guidance

34. We provide a range of guidance products to help organisations apply data protection law to AI. These include:

- Our guidance on AI and Data Protection[31], which is regularly updated to address emerging risks and opportunities.
- Complementary guidance on Automated Decision-Making and Profiling[32], addressing these specific provisions of data protection law.
- Supplementary guidance on Explaining Decisions Made with AI[33], co-badged with the ATI.
- An accompanying AI and Data Protection risk toolkit[34], which won a Global Privacy and Data Protection Award in 2022[35].

We also provide guidance on specific applications of AI, for example in relation to biometric recognition technologies[36] and age assurance technologies[37].

---

[30] Big data, artificial intelligence, machine learning and data protection | ICO
[31] Guidance on AI and data protection | ICO
[32] Automated decision-making and profiling | ICO
[33] Explaining decisions made with AI | ICO
[34] AI and data protection risk toolkit | ICO
[35] Global Privacy and Data Protection Awards 2023 | Global Privacy Assembly
[36] Biometric data guidance: Biometric recognition | ICO
[37] Age assurance for the Children's code | ICO

35. We track developments in AI to ensure organisations have access to the latest guidance. For example, we issued rapid advice to developers and users of generative AI[38] as interest in the area grew last year. We conduct horizon-scanning to detect new data protection risks and opportunities, issuing reports on neurotechnologies[39], emerging biometric technologies[40], personalised large language models and next-generation search engines[41], among others. We also run a programme of post-doctoral AI fellowships that research issues such as model inference attacks.

Our advice and support

36. We offer a range of advice services for AI innovators, providing them with regulatory clarity and certainty as they introduce their ideas.

37. Our Regulatory Sandbox provides in-depth support to supports organisations developing products and services which use data in innovative and novel ways. Previous participants include Onfido[42], which provides remote biometric identity verification technology, and GoodWith[43], which sought to develop a 'financial virtual assistant' for young adults.

38. Our Innovation Advice service aims to respond to regulatory questions from innovators in 10-15 days, ensuring our advice is as rapid as developments in the market. The service, which was named Best Innovative Privacy Project in the 2023 PICCASO awards, has advised on topics from generative AI to automated calling systems.

39. Our Innovation Hub, which partners with accelerators, incubators and other agencies to mentor innovators as they engineer data protection into the fabric of their new ideas. Our collaborations have included:

    - working with DSIT, the Home Office and GCHQ on the SafetyTech Innovation Challenges;[44]
    - collaborating with DSIT, Innovate UK and the EHRC on the Fairness Innovation Challenge[45]; and
    - working with the Digital Catapult Bridge AI[46] cohorts.

[38] Generative AI: eight questions that developers and users need to ask | ICO
[39] ICO tech futures: neurotechnology | ICO
[40] ICO tech futures: biometrics | ICO
[41] Tech Horizons Report | ICO
[42] Onfido Regulatory Sandbox Final Report | ICO
[43] Good With Regulatory Sandbox Final Report | ICO
[44] Safety Tech Challenge
[45] Fairness Innovation Challenge
[46] BridgeAI | Digital Catapult

40. With our DRCF partners, we are currently piloting the AI and Digital Hub[47], which allows innovators to obtain answers to complex queries which span the regulatory remits of DRCF member regulators.

41. To help educate and assist organisations to meet their regulatory obligations, we also undertake a programme of consensual audits[48] of organisations to assess their processing of personal information using AI and provide practical advice to improve the way they deal with information rights issues. We are currently conducting audits of companies offering AI-based age estimation and verification services and AI-based products within the recruitment sector.

Our regulatory action

42. We act to enforce the law and safeguard people from harm, ensuring that organisations developing and deploying AI face a level playing field. We use our full regulatory toolbox to ensure compliance with the law, including:

- Information Notices, which can be used to require information from the organisations that we regulate;
- Assessment Notices, which can be used to request access to premises to examine equipment and processing activities on the ground;
- Enforcement Notices, which can be used to order organisations to stop processing, delete data or take forward other remedies; and
- Monetary Penalty Notices, which can be used to levy fines where organisations breach the law.

43. We communicate the outcomes of our regulatory action as appropriate to promote compliance and safeguard people from harm. Recent action in relation to AI includes:

- Clearview AI, Inc[49] – we fined the facial recognition database company more than £7.5m and ordered UK data to be deleted; this matter is subject to ongoing legal challenge[50].
- Serco Leisure[51] and others – we issued enforcement notices ordering them to stop using facial recognition technology and fingerprint scanning to monitor employee attendance.

---

[47] AI and Digital Hub | DRCF
[48] A Guide to ICO Artificial Intelligence (AI) Audits | ICO
[49] ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted | ICO
[50] Information Commissioner seeks permission to appeal Clearview AI Inc ruling | ICO
[51] ICO orders Serco Leisure to stop using facial recognition technology to monitor attendance of leisure centre employees | ICO

- Snap, Inc[52] – we issued the social media firm with a preliminary[53] enforcement notice in respect of their 'My AI' generative AI chatbot; we are considering their representations before taking a final decision.

Part 4: Upcoming developments

44. Artificial intelligence – and its application in biometric technologies – is one of the ICO's three focus areas in 2024/25, along with children's privacy and online tracking.

45. In this section, we set out some of the key developments that organisations can expect over the coming months, complementing the ongoing work of our advice services and our supervision of firms using personal data to develop or deploy AI.

Our policy and guidance

46. We continue to ensure our advice and guidance keeps pace with the rate of development and adoption of AI technologies as well as legislative changes.

Consultation series on generative AI

47. In January, we launched a consultation series on generative AI, examining how aspects of data protection law should apply to the development and use of the technology. So far, the series has examined:

- the lawful basis for web scraping to train generative AI models;
- purpose limitation in the generative AI lifecycle; and
- the accuracy of training data and model outputs.

48. Further calls for evidence will focus on individual rights and controllership. The ICO is seeking views from a range of stakeholders, including developers and users of generative AI, civil society groups and other public bodies with an interest in the technology.

Consultation on biometric classification

49. In spring 2024, we will seek views on how biometric classification technologies, such as those used to draw inferences about people's

[52] UK Information Commissioner issues preliminary enforcement notice against Snap | ICO

[53] The findings in the preliminary enforcement notice are provisional. No conclusion should be drawn at this stage that there has, in fact, been any breach of data protection law or that an enforcement notice will ultimately be issued. The ICO will carefully consider any representations from Snap before taking a final decision.

emotions or characteristics, should be developed and deployed. This follows publication of our guidance on biometric recognition[54] earlier this year.

Updated guidance on AI and data protection

50. In spring 2025, we expect to consult on updates to our Guidance on AI and Data Protection[55] and Automated Decision-Making and Profiling,[56] to reflect changes to data protection law following the passage of the Data Protection and Digital Information Bill.

Our advice and support

51. We will continue to provide support to organisations seeking to develop and deploy AI in novel ways, including through our Regulatory Sandbox, our Innovation Advice service, our Innovation Hub partnerships and the DRCF AI and Digital Hub.

New Regulatory Sandbox projects

52. In the coming months, the ICO's Regulatory Sandbox[57] will support a number of AI-related projects, including: a system to help prevent falls in the elderly; personalised AI for those affected by cancer; AI to help identify individuals who may be at risk of domestic violence; and AI used to remove personal data from drone images.

Ongoing Innovation Hub projects

53. In the coming months, the ICO's Innovation Hub will continue to support AI innovators through partnerships with:
    - DSIT, the Home Office and GCHQ on the SafetyTech Innovation Challenges;[58]
    - DSIT, Innovate UK and the EHRC on the Fairness Innovation Challenge[59]; and
    - the Digital Catapult Bridge AI[60] cohorts.

Our assurance projects

54. We continue to undertake consensual and compulsory audits in order to drive best practice. Later this year, we will report detailing our findings following a series of engagements with providers of AI recruitment

[54] Biometric data guidance: Biometric recognition | ICO
[55] Guidance on AI and data protection | ICO
[56] Automated decision-making and profiling | ICO
[57] Current projects | ICO
[58] Safety Tech Challenge
[59] Fairness Innovation Challenge
[60] BridgeAI | Digital Catapult

solutions. We will also examine AI practice as part of future audits looking at technology in education and youth prison services.

Our regulatory action

55. We continue to actively scrutinise the development and deployment of AI across the economy to safeguard people from harm. This includes scrutiny of how biometric technologies, such as those used for biometric recognition or behaviour classification, are developed and used. We will continue to communicate the outcomes of regulatory action to the market to drive improvements overall.

Part 5: Working together

Working with other regulators

56. As a whole-economy regulator, supervising the processing of personal data in both the private and the public sector, we work closely with a wide range of regulators to safeguard people from harm and ensure coherent regulation for organisations.

The Digital Regulation Cooperation Forum

57. We are proud to be a founding member of the Digital Regulation Cooperation Forum (DRCF), through which we work with the Competition and Markets Authority, Ofcom and the Financial Conduct Authority to deliver a coherent approach to digital regulation for the benefit of people and businesses.

58. AI is a priority for the DRCF. With our fellow regulators, we have:

- published a paper setting out our shared perspective on the benefits and harms of AI;[61]
- shared our views on technologies such as generative AI[62] and issues such as fairness and AI[63];
- undertaken research into the third-party auditing market[64] and engaged with participants in this market; and

[61] The benefits and harms of algorithms: a shared perspective from the four digital regulators | DRCF
[62] Maximising the benefits of Generative AI for the digital economy | DRCF
[63] Fairness in AI: A View from the DRCF | DRCF
[64] Auditing algorithms: the existing landscape, role of regulators and future outlook | DRCF

- established the AI and Digital Hub, enabling innovators to obtain answers to complex queries which span the regulatory remits of DRCF member regulators.

59. This year we will:

- conduct joint research into consumer use, understanding and trust of generative AI;
- conduct research to better understand cross-sector adoption of generative AI technology by organisations;
- share our approaches to conducting regulatory audits of AI systems, including challenges and learnings; and
- continue our research into the third-party auditing market, to help inform industry on how they can make best use of third-party auditors.

60. In relation to the AI Regulation White Paper, we will host joint workshops to explore how its principles interact across the four regulators, with a focus this year on AI transparency and accountability. We will continue to work with the government's new central AI function and consider potential joint regulator capability-building projects.

The Regulators and AI Working Group

61. The Regulators and AI Working Group – founded by the ICO in 2019 – ensures open dialogue with a wider set of AI regulators. The working group's membership includes over 47 regulators and public authorities, including DSIT. The group has facilitated connections with international AI regulators, with guest speakers including representatives from the US Federal Trade Commission and the European Commission.

Bilateral partnerships

62. Beyond these multilateral forums, we work closely with other regulators on a bilateral basis. For example, we continue to partner with EHRC and DSIT to support the Fairness Innovation Challenge to address bias and discrimination in AI systems, building on our earlier work together on fairness. Later this year we will publish a joint statement with the Competition and Markets Authority on foundation models, with the aim of supporting coherence for businesses and promoting behaviours that benefit consumers where our remits interact.

Working with government

63. We have worked closely with our sponsor department DSIT to inform the government's AI Regulation White Paper and look forward to working together on its implementation, including the establishment of central functions to promote regulatory coherence. We will continue to analyse and

review potential gaps in legislation and advise government on these matters as appropriate.

64. The government is well-placed to set an example of what responsible AI development and deployment looks like. We continue to shape approaches to AI deployment in different contexts, such as with the Department for Education on generative AI. We will continue to provide advice and scrutiny to ensure that the adoption of AI in public services is compliant with data protection law.

Working with standards bodies

65. We continue to inform standard-setting initiatives as a member of the AI Committee of the British Standard Institution (BSI). We monitor development at international standardisation bodies such as CEN CENELEC, ISO and ETSI and have already provided input into standards such as the ISO/IEC 4200 1:2023 AI Management System, published in December 2023 and the ISO/IEC 23894:2023 on AI Risk Management.

Working with international partners

66. We work closely with international counterparts, to safeguard people from harm and promote regulatory coherence across borders. This includes:

- bilateral cooperation with fellow data protection and privacy authorities, such as our joint investigation with the Office of the Australian Information Commissioner into Clearview AI;
- plurilateral cooperation through the G7 group of data protection and privacy authorities, with whom we issued a joint statement on generative AI[65], on which we will continue to build this year;
- multilateral cooperation through the Global Privacy Assembly, with whom we issued resolutions on generative AI and AI in employment last year;
- membership of the OECD AI Expert Group on AI, Data and Privacy, which is currently exploring the synergies between privacy, data protection and AI governance frameworks; and
- contribution to the International Working Group on Data Protection in Technology (the Berlin Group), on matters such as large language models.

[65] Roundtable of G7 Data Protection and Privacy Authorities Statement on Generative AI | Personal Information Protection Commission of Japan

Annex: Our capabilities

Our people

67. As AI transforms our economy, an increasing proportion of all regulatory roles at the ICO deal with AI – including staff working in communications, policy, advice, complaints, audits, investigations and litigation. We expect that in the future nearly all data protection roles at the ICO will involve AI to some degree.

68. At the core of our regulatory operations is our AI and Data Science team, which acts as a centre of excellence on AI, informing our policy, advisory and enforcement interventions alike. This unit comprises 10 professionals who are dedicated full-time to AI governance and is expected to grow in the coming years.

69. In tandem with growing our capacity to regulate AI, we are also investing in the technical capabilities of our staff. We will continue to develop our people, ensuring that we have the right mix of skills to be an effective regulator of AI.

Our technology

70. As AI presents new opportunities, we will role-model responsible use of AI here at the ICO as part of our Enterprise Data Strategy.[66]

71. The use of AI and machine learning will help the organisation become more data-led in its decision making, improving the services and support it can offer to customers. We currently use AI to support a customer service chatbot and an algorithmic tool for email triage and are developing an AI solution to help identify websites using non-compliant cookie banners.

72. We welcome the government's commitment to use of the algorithmic transparency recording standard[67] across government departments and, in due course, the wider public sector. This will support greater transparency and scrutiny of public sector AI adoption. We already employ the standard in our internal AI deployments and will continue to do so.

73. We will develop an internal data literacy initiative to empower data and analytics skills across the organisation. We will also develop a suite of AI training and resources to ensure AI adoption at the ICO aligns with our regulatory expectations of others.

---

[66] ICO Enterprise Data Strategy | ICO
[67] Algorithmic Transparency Recording Standard Hub | GOV.UK