

The Information Commissioner's response to the European Commission's Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

About the ICO

1. 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.
2. 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.

Introduction

3. The Information Commissioner's Office (ICO) welcomes this opportunity to provide comments on the European Commission's Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts¹ (the 'AIA') on behalf of the Commissioner.
4. The ICO recognises the significant benefits that Artificial Intelligence (AI) can bring to people and businesses, from helping tackle global health challenges to creating new products and services. However, AI allows the use of high volumes of personal, sometimes highly sensitive data about individuals that can be difficult for them to understand, and which can have

¹ EU Commission (2021). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. COM(2021) 206 final, 21 April 2021. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements_en

significant effects on their lives. This means that some uses of AI have the potential to create high risks to individuals' rights and freedoms.

5. Effective and proportionate regulation is therefore important to ensure individuals are protected. It is also important to unlocking those wider social and economic benefits, because it builds public trust and confidence in the development of these technologies. This is why we at the ICO have made enabling good practice in AI one of our top priorities.²
6. Machine-learning, algorithmic processing and profiling models have come to the ICO's attention in the context of political campaigning,³ the deployment of data analytics by police forces,⁴ and data brokers' business models,⁵ amongst other areas.
7. As part of our focus on AI, we co-authored the Explaining Decisions Made with AI⁶ guidance with the Alan Turing Institute, we published the Guidance on AI and Data Protection⁷ and the latest test version of our AI and Data Protection Risk Mitigation and Management Toolkit.⁸ In 2017 our Big Data, AI, Machine Learning and Data Protection report received a Global Privacy and Data Protection award.⁹
8. We believe the expertise of data protection authorities (DPAs) is a crucial element in developing AI policy that leads to good outcomes for the public and businesses. That is why the ICO has been engaged in AI policy debates at the international level, providing comments on relevant work at the Council of Europe, UNSRP, UNESCO and the Global Privacy Assembly.
9. The ICO is also a co-founder of the UK's Digital Regulation Cooperation Forum (DRCF) that includes the UK's Financial Conduct Authority, the Competition and Markets Authority and the Office of Communications (Ofcom). Algorithmic Processing is one of the priority areas for our strategic joint work with the DRCF.¹⁰
10. The ICO acknowledges that UK businesses are leading developers of AI tools and there is increasing demand for these products and services around the world, including the EU. Therefore, we believe it is important to retain a constructive dialogue between the UK, the EU and international partners to enable global trade in goods and services, while ensuring UK and citizens around the world are protected.

² <https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf>

³ <https://ico.org.uk/for-organisations/guidance-for-the-use-of-personal-data-in-political-campaigning/profiling-in-political-campaigning/>

⁴ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/12/ico-launches-tool-to-help-police-forces-using-data-analytics/>

⁵ <https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf>

⁶ ICO and the Alan Turing Institute (2020). *Explaining decisions made with AI*. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/>.

⁷ ICO (2020). *Guidance on AI and data protection*. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection>.

⁸ Blog: New toolkit launched to help organisations using AI to process personal data understand the associated risks and ways of complying with data protection law | ICO

⁹ [big-data-ai-ml-and-data-protection.pdf \(ico.org.uk\)](https://ico.org.uk/big-data-ai-ml-and-data-protection.pdf)

¹⁰ <https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022>

11. The following comments set out some of the ICO's thoughts on the European Commission ('the Commission') proposed AIA. Our analysis centres around the implications of the AIA for data protection law as this is our remit and area of expertise.

An important step towards regulating AI

12. We welcome the AIA's ambition to regulate the use of AI so that it is safe and respects existing law, fundamental rights and EU values. We agree with the proposal's view that legal certainty is paramount in facilitating innovation and investment in this emerging technology. We believe such a far-reaching regulatory framework should first and foremost serve the public interest by creating an ecosystem that provides consistency and certainty for the good players and enforces against the bad players in the marketplace.
13. The ICO appreciates and supports the innovation and opportunities to society that AI can bring. To build the trust that is necessary to realise that potential value, we must be mindful of the fact that the standard practices for developing and deploying AI may create data protection risks such as non-compliance with GDPR's data minimisation principle or individual information rights, as well as harms such as unfair discrimination.
14. Following the UK's exit from the EU, we remain committed to ensuring high standards of data protection that protect individual rights while also enabling data to be used responsibly to deliver social and economic benefits. Continuing to engage with our EU partners remains critical for the ICO and we support an approach to AI policy that respects and protects fundamental rights while boosting innovation by enabling personal data to be used responsibly and deliver social and economic benefits
15. Data protection law is already playing an important role in AI regulation and we commend the Commission's intention for the AIA to be consistent with existing legislation on data protection, consumer protection, non-discrimination and gender equality. We believe regulatory coherence between data protection law and the AIA will be vital for businesses to innovate free of the impediments that legal uncertainty creates.

Points of the AIA proposal the ICO supports

16. We believe responsible development, testing, deployment and oversight of AI can accelerate economic growth, build public trust in the technology itself and lead to technological progress and human flourishing more broadly.
17. As the UK data protection regulator, the ICO has been playing its part in helping businesses responsibly develop AI in ways that protect fundamental rights, including privacy and the right to non-discrimination. We agree that ensuring the public and consumers are protected while innovative businesses are supported is better accomplished by putting in place both

ex-ante and ex-post measures of control and oversight.¹¹ Going forward, we believe it is important for the efficacy of the measures the AIA envisions – both ex-ante (technical documentation, conformity assessment procedures,¹² etc) and ex-post (AI providers’ risk management systems and post-market monitoring) – to be evaluated in ways that are actionable.

18. We support the Commission’s risk-based approach to AI regulation, acknowledging that certain applications or contexts will not pose risks to fundamental rights and freedoms.
19. We agree with the proposal’s view that the risk management system for high-risk AI should be a continuous iterative process requiring regular systematic updates and that due consideration should be given to the environment/context¹³ in which the system is intended to be used. The ICO has been working to support businesses on how to manage AI risks effectively through our AI and Data Protection Risk toolkit.
20. The principle of identifying and taking action to mitigate risks in advance is an important one for all high-standard data protection regimes, ensuring harm is prevented before it occurs. We note that GDPR already includes ex-ante tools to mitigate high risks to individual rights and freedoms posed by AI such as Data Protection Impact Assessments (DPIAs). In our guidance and reports we have stated that a DPIA will likely be legally required for most big data applications such as AI systems.¹⁴ It would be helpful to understand how the Commission envisions DPIAs’ interaction with the AIA framework; we note that requiring a fundamental rights or algorithmic impact assessment within the AIA was discarded on the basis that ‘users of high-risk AI systems would normally be obliged to do a Data Protection Impact Assessment’.¹⁵
21. The ICO supports the proposal’s enhanced transparency provisions such as the establishment of a public registry for high-risk AI systems – in particular for systems deployed in the public sector – or the measures ensuring individuals tasked with oversight fully understand AI systems’ capacities and limitations. Such measures will assist AI businesses to comply with their transparency and accountability obligations under data protection law. We believe the data governance requirements the Commission envisions will also assist in that regard.

¹¹ As the EU proposal itself notes more than 50% of stakeholders from business associations that were consulted were in favour of such an ex-ante and ex-post approach.

¹² EU Commission (2021). *Commission Staff Working Document: Impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. 21 April 2021, SWD(2021) 84 final, page 77. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:0694be88-a373-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF. Page 77 of the impact assessment notes that “conformity assessment through independent third party notified bodies would be more effective than ex ante conformity assessment through internal checks as an enforcement mechanism in this respect to ensure the effective protection of the fundamental rights”.

¹³ OECD’s proposed classification framework also sets out context as one of AI systems’ four key dimensions. <https://oecd.ai/classification>

¹⁴ ICO (2017). *Big data, artificial intelligence, machine learning and data protection*, page 99. Available at: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

¹⁵ SWD(2021) 84 final, pp. 58-9.

22. We believe there is value in industry-led governance tools, such as codes of conduct, that can help raise the bar and enable resources to be focused on areas of greatest risk. Sectoral expertise will be key in their development. We support the view of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) that any codes of conduct should not conflict with codes of conduct developed in the context of data protection.¹⁶
23. We welcome provisions that will help providers and users of high-risk AI systems comply with the accountability principle of data protection, such as the suggestion of automatic recordings of events ('logs'). We also note the Commission's intention to give public authorities access to confidential information or source code of AI systems to examine compliance, as an important accountability and transparency tool.
24. The ICO supports the Commission's decision to highlight the need to address bias and discrimination in the context of AI systems to ensure data processing complies with the fairness principle. We believe useful gateways can be clarified that enable AI developers to tackle this challenge. We also plan to produce clarificatory guidance on fairness in AI and anti-discriminatory design.
25. We are particularly interested in the proposed regulatory sandboxes established by competent authorities. The ICO's engagement with AI-driven companies in the context of our own Regulatory Sandbox¹⁷ has demonstrated that by bringing innovators into the controlled environment of a regulator, risks can be identified and tackled early enough for consumers to be protected and business development to progress faster. We would welcome the opportunity to share our experience with the Commission.
26. We support the AIA's view that remote biometric identification for non-law enforcement purposes constitutes a high-risk deployment and as the Opinion recently published by the Commissioner states, there is a high bar for its use to be lawful.¹⁸
27. We support the Commission's decision not to propose the automatic creation of additional bodies to oversee the regulation, suggesting members states can appoint existing sectorial authorities to do so. We believe that in the UK, the DRCF's work on building common capacity and enhancing knowledge-sharing provides a useful template for how to harness existing expertise to approach AI regulation.

Additional areas of interest

28. We recognise the AIA seeks to tackle the difficult challenge of regulating the application of a complex technology in a way that does not conflict with

¹⁶ https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

¹⁷ Onfido was one of the AI-driven companies that was accepted in ICO's sandbox.

<https://ico.org.uk/media/for-organisations/documents/2618551/onfido-sandbox-report.pdf>

¹⁸ <https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf>

existing legal frameworks such as data protection, impede innovation or result in harm. We believe this consultation process provides an opportunity for different stakeholders to constructively engage with the proposal and make the AIA more robust and efficient. With that in mind, the ICO is particularly interested in the Commissions' thinking in regard to two main aspects of AI regulation:

- the rights individuals and groups have in relation to AI systems and how they can exercise them; and
 - the efficacy of the suggested control and oversight measures and the scope for auditing.
29. The proposal states that effective redress for affected persons will be made possible by the transparency and traceability of AI systems coupled with ex-post controls. It is also our understanding that the Commission plans to propose a liability framework in the context of AI systems in Q4 of 2021.¹⁹ Existing frameworks such as data protection law contain provisions individuals can use to contest certain AI-driven decisions, or to seek an explanation of those decisions, but it would be useful to have more clarity in terms of how these existing provisions interact with the AIA.
30. A substantial portion of the proposed ex-ante and ex-post measures for high-risk AI systems, including risk reporting, rely on self-reporting and internal controls. We look forward to learning about the results of this approach. We believe in providing industry with guidance and tools that help them comply with the law and in this context, we have developed our public-facing AI and Data Protection Risk Mitigation and Management Toolkit. We also believe in building regulators' auditing capability and the ICO has been developing its internal AI auditing toolkit. We are open to sharing lessons learned with the Commission if deemed useful.
31. We reiterate a point we raised in our response to the consultation on the EU Commission's White Paper on AI, to highlight the importance that any new AI legal framework reinforces or bolsters data protection law's regulation on AI, to avoid legal ambiguity and protect citizens. In that context, setting out how the roles of AIA's user/provider map onto the processor/controller responsibilities of the GDPR would be also useful as AI supply chain issues constitute an area of increasing interest for data protection regulators.
32. We also look forward to seeing how the development of harmonised standards that would enable AI providers to report compliance with the AIA progresses. We agree with EDPB and EDPS that DPAs should be involved in the preparation and establishment of such standards.²⁰

Conclusion

33. We welcome the European Commission's ambition to regulate the use of AI technologies so that it is safe and respects existing law on fundamental

¹⁹ SWD(2021) [84 final](#), p. 88.

²⁰ [edpb-edps joint opinion ai regulation en.pdf \(europa.eu\)](#)

rights, facilitates the development of lawful, safe and trustworthy AI and ensures legal certainty for businesses.

34. We support the Commission's broader view that it is important to balance the flow and wide use of data, while preserving high privacy, security, safety and ethical standards.²¹
35. We will monitor any further developments from the EU Commission regarding this proposal and related frameworks and will contribute when appropriate.

²¹ EU Commission (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data. COM(2020) 66 final, 19 February 2020. Available at: https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf