The Information Commissioner's response to the Lords Communications and Digital Committee's call for evidence on Large Language Models

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 suitable action where the law is broken.

3. The Information Commissioner's Office (ICO) has set out its strategic vision in the ICO25 plan[1], which highlights promoting regulatory certainty, empowering responsible innovation and safeguarding the public as key priorities.

Introduction

4. The ICO welcomes the opportunity to respond to The Lords Communications and Digital Committee's ('the Committee') call for evidence on large language models (LLMs).[2] We support the Prime Minister's Office's interest in making the UK a world-leading centre for AI safety.

The ICO's role in regulating AI

5. Personal information is often used to train, test or deploy an AI system and where it does, it will fall under the remit of the ICO as the UK's data

[1] https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan/
[2] https://www.parliament.uk/business/lords/media-centre/house-of-lords-media-notices/2023/july-2023/how-will-ai-large-language-models-shape-the-future-and-what-is-the-right-regulatory-approach

protection regulator. We believe data protection can help organisations to safely build or use AI in a way that mitigates risks to people's rights and freedoms.

6. AI is a priority for the ICO. The ICO25 strategic plan highlights our current work in relation to AI, including actions to tackle urgent and complex issues such as AI-driven discrimination. This builds on our existing work on AI, including:

- our landmark Guidance on AI and Data Protection[3], which is regularly updated to address emerging risks and opportunities;
- our accompanying AI and Data Protection risk toolkit[4], which won a Global Privacy and Data Protection Award in 2022;
- our supplementary guidance on Explaining Decisions Made with AI[5], co-badged with The Alan Turing Institute;
- our support for AI innovators through our Regulatory Sandbox, Innovation Advice and Innovation Hub[6];
- our advice to regulators on how to use AI and personal data appropriately and lawfully, following a recommendation by the House of Lords.
- our contribution to standard-setting initiatives as a member of the AI Committee of the British Standard Institution (BSI); and
- our supervision of organisations using AI, including through both proactive audits and investigations.

Data Protection and LLMs

7. Large language models (LLMs) are a type of generative AI (GenAI), with the ability to produce human-like text, code and translations. Where they process personal information, data protection law will apply.

8. Data protection law is principles-based and technology-neutral, and the ICO's existing guidance and support for organisations on AI applies equally to the narrower contexts of GenAI and LLMs. While in some domains (e.g. intellectual property, online safety) the emergence of LLMs has exposed risks that may be difficult to mitigate using existing legislation, this is less true in the context of data protection.

[3] Guidance on AI and data protection | ICO
[4] AI and data protection risk toolkit | ICO
[5] Explaining decisions made with AI | ICO
[6] ICO Innovation Services | ICO

9. As such, the ICO's focus is on driving compliance across the GenAI value chain using its existing powers. Our work programme includes:

- Targeted communications to remind organisations of their responsibilities, such as our April 2023 blog "Generative AI: eight questions that developers and users need to ask",[7] which outlines some key areas developers and users of GenAI need to consider when processing personal data.

- Scrutinising how developers and deployers of GenAI have tackled privacy risks before introducing new products and services utilising GenAI and initiating investigations where necessary.

- Joining forces with international data protection and privacy authorities regarding GenAI, including a joint statement with G7 authorities on GenAI[8].

10. What primarily differentiates GenAI and LLMs from other forms of AI is the increase in scale of the data that is being processed, and the increase in the complexity of the techniques used to develop the models. From a data protection perspective, these differences mostly exacerbate existing risks.

11. While these risks need to be considered across the entire AI lifecycle, we consider the greatest opportunity to embed effective safeguards may arise during the initial development stages of an AI system. For example:

- Problem formulation choices directly shape a model's purpose and impacts. Engaging diverse views at this phase can help surface potential harms.

- Data protection impact assessments (DPIA) and other forms of risk assessment and planning early on allows data protection by design, rather than a retrospective approach.

- Choices around data sourcing and pre-processing are key to mitigating risks of bias being encoded into models.

- The selection of the techniques to train models may also have inherent trade-offs around accuracy, security, transparency etc. that are hard to change post-development.

12. The ICO recognises that AI systems like LLMs may result in unintended outcomes that infringe data protection principles or cause broader societal harms. We believe a multi-faceted approach is needed to proactively identify and mitigate such risks, including:

[7] Generative AI: eight questions that developers and users need to ask.
[8] Roundtable of G7 Data Protection and Privacy Authorities Statement on Generative AI -Personal Information Protection Commission- (ppc.go.jp)

- Conducting and regularly updating DPIAs both for the underlying model but also for the applications that embed it. These should look beyond immediate use cases to plausible downstream impacts, with input from diverse perspectives.

- Adopting from the beginning data protection principles like data minimisation, purpose limitation and storage limitation to limit unnecessary processing.

- Ensuring strong transparency and meaningful human oversight, enabling unintended effects to be detected and addressed.

- Monitoring systems in real-world contexts for emerging issues, and empowering rapid response to problems.

- Making explainability a priority, so anomalies indicating unintended consequences can be investigated.

- Implementing effective security practices to reduce vulnerabilities like model inversion and membership inference.

- Training and information sharing involving senior decision-makers in an organisation but also front-line staff using the applications powered by LLMs so they understand the associated data protection risks in their context.

13. While not exhaustive, these measures reflect the ICO's risk-based approach to AI regulation, ensuring unintended consequences can be minimised through responsible design, transparency, and iterative improvement when deployed.

14. The context within which a LLM is deployed also plays a critical role. A model considered safe in one domain could have unintended consequences in another. For example, using a chatbot to write a poem carries different risks compared to a medical professional using it as part of the process of diagnosing a patient's condition.

15. Organisations adopting LLMs to solve a business or consumer need are still accountable for the processing of their customers' personal data by those LLMs and have to be confident they comply with all their data protection obligations including rules around solely automated decision-making, security of personal data and responding to data subjects' information rights requests.

16. Organisations should also take steps to guard against the unauthorised use of LLMs for processing of their customers' personal data by their staff. This is particularly important given the time-saving nature of many of these applications and their wide availability.

17. Our existing initiatives such as our Regulatory Sandbox and our Innovation Advice service can provide tailored guidance to organisations that is specific to the technologies and use cases concerned. The ICO is ready to provide advice and assistance to innovators across all industries, and is already answering queries from organisations on GenAI[9].

Domestic regulation

18. The ICO has responded to the UK government's AI White Paper[10]. We support the government's vision to make the UK the best place in the world to found and grow an AI business and translate AI's potential into growth and societal benefits[11]. We welcome proposals that support responsible innovation while protecting people and their rights. At the same time it is important to note that AI and LLMs are already regulated by a variety of UK regulators, including the ICO.

19. We believe that non-regulatory and regulatory measures can be mutually reinforcing and should be pursued in tandem. On the non-regulatory side, we welcome industry best practices, voluntary codes of conduct, and standards relating to how personal information is processed. We believe that these can help organisations demonstrate accountability and compliance with data protection law.

20. The ICO also plays a central role in initiatives to foster greater regulatory coherence and certainty for organisations developing and using AI. We are a founder member of the Digital Regulation Cooperation Forum (DRCF) through which we are examining common risks across the regulatory landscape in relation to GenAI and opportunities for joint research and interventions[12]. We are also piloting a Multi-Agency Advice Service[13] for digital innovators needing joined up advice from multiple regulators with our DRCF partners.

International context

21. The ICO is committed to making the international flow of data as frictionless as possible to support economic growth.[14] We actively cooperate with international partners on AI governance and regulation. As a member of the Global Privacy Assembly (GPA), we work with the GPA's permanent working group on Ethics and Data Protection in AI, promoting international alignment. The ICO shaped the G7 Data Protection Authorities' "Statement on Generative AI" and continues to work with

[9] Previously asked questions | ICO
[10] ico-response-ai-white-paper-20230304.pdf
[11] We have also responded to the House of Commons inquiry on AI governance: UK Parliament consultation: Governance of artificial intelligence | ICO
[12] Maximising the benefits of Generative AI for the digital economy | DRCF
[13] Projects selected for the Regulators' Pioneer Fund (2022) - GOV.UK (www.gov.uk)
[14] Empower responsible innovation and sustainable economic growth | ICO

counterparts on the privacy implications of GenAI through the G7 Emerging Technologies Working Group and Enforcement Cooperation Working Group.[15] We also work with international colleagues on a bilateral basis. Through these initiatives, the ICO aims to foster coordinated oversight of AI across borders.

Conclusion

22. Data protection provides a risk-based, context-specific framework for the governance of LLMs. Risks should be evaluated holistically across the AI lifecycle based on the intended purposes and potential impacts, not the specific technology itself used. The ICO sees the data protection principles, as a robust foundation but emphasises practical support tailored to particular applications will better support responsible innovation. Providing this support may require additional resources to supplement existing in-house expertise. As AI continues to rapidly evolve, sustained investment in UK regulators' oversight capabilities is needed.

23. The ICO welcomes further engagement and discussion with the Committee on translating its ambitions into effective, proportionate governance that unlocks the benefits of LLMs while safeguarding the public.

[15] Roundtable of G7 Data Protection and Privacy Authorities Statement on Generative AI -Personal Information Protection Commission- (ppc.go.jp)