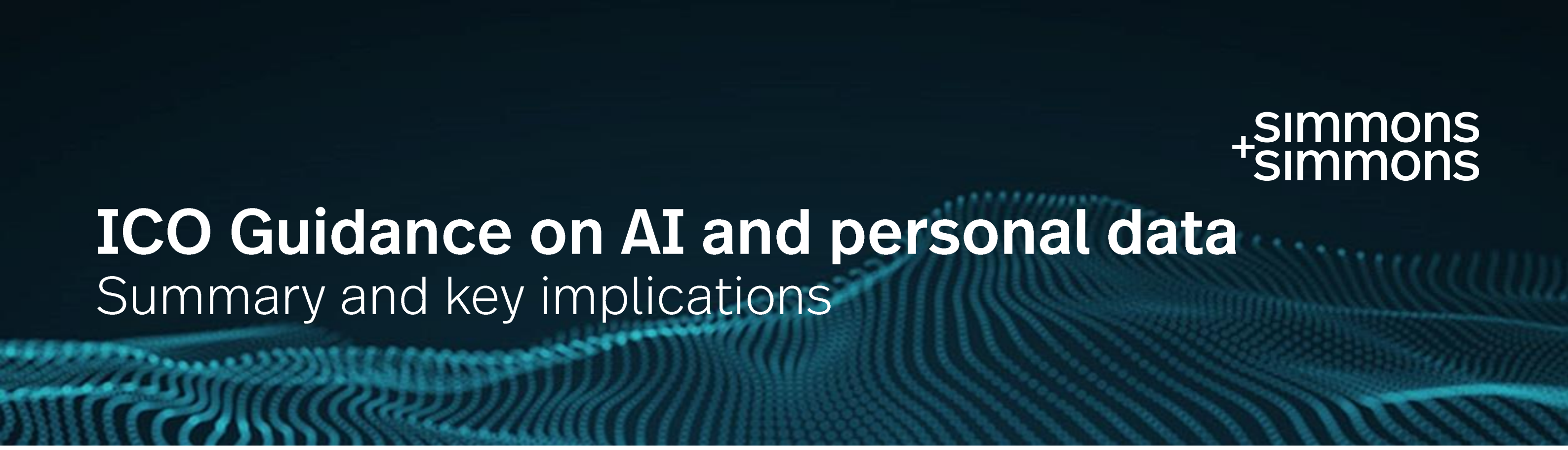

ICO Guidance on AI and personal data

Summary and key implications

As the use of Artificial Intelligence becomes more prevalent, organisations and regulators need to develop a strong understanding of the appropriate and lawful use of personal data in the context of AI. The deployment of AI can bring transformative benefits to organisations, but may also raise privacy concerns.

The ICO has recently issued guidance addressing a number of these concerns and provides an insight into the application of personal data protection law in the context of AI.

The ICO Guidance provides practical tips to improve how AI and the personal information associated with it are handled. Key takeaways from the guidance are:

01

Adopting a risk-based approach in the development and deployment of AI

AI is considered a **high-risk technology** and both the development and deployment of AI carries **significant risks to the rights and freedoms of individuals** along with compliance considerations. Before using an AI system, a risk assessment should be carried out and risk mitigation measures put in place.

To identify and minimise the risk of non-compliance with data protection legislation, the ICO recommends carrying out a **Data Protection Impact Assessment ("DPIA")**. A DPIA is legally required for high-risk data processing and should be performed prior to implementing the AI system. DPIAs should not be viewed as a compliance ticking exercise but rather as an opportunity for firms **to demonstrate their accountability** with regards to the design and deployment of AI systems. The ICO also suggests that firms consult with those affected by their AI systems in order to better understand the potential risks.

The ICO is clear that if an organisation decides not to carry out a DPIA for use of AI it should document why this decision was made

02

Explaining decisions made by AI to individuals affected

Although explaining the decision-making process of AI systems is not easy, individuals have a right to an explanation. The ICO encourages organisations to be **clear, transparent and honest** about the processing of individuals' personal data as they will need to consider how to handle subsequent individual rights requests.

In particular, the ICO is clear that **explanations of AI decision-making should be contextualised** with regards to the specific AI solution – i.e. varying levels of detail or types of explanation may be needed depending on the AI solution.

03

Minimising data collection

In order to have a positive impact, the use of AI may require large amounts of data while at the same time, data protection law and principles promote the **minimisation of the collection and use of personal data**. There is an apparent conflict in this, but the ICO is clear that this does not mean that AI cannot be used or that large amounts of data cannot be used where appropriate.

The ICO Guidance focuses on the fact that **the data minimisation principle should be applied contextually** to the AI and ensuring that the organisation ensures the data used is "**accurate, adequate, relevant and limited**" and privacy preserving techniques are used where appropriate.

04

Reducing the risk of bias and discrimination

Imbalanced datasets can produce outputs with **discriminatory effects** based on gender, race, age, religion, disability, health and sexual orientation etc.

The ICO Guidance is clear that, in order to address the risks of bias and discrimination, organisations should assess whether the data being collected is **accurate, reliable, up to date and not misleading** (and take action to resolve any issues). Organisations should **assess the likely effects of AI-based decisions** for different groups and consider whether the outcomes are acceptable.

05

Preparing data appropriately by dedicating time and resources

An AI system will produce different results depending on the quality of its input data. Firms should therefore ensure that proper time and resources are taken in collecting **accurate, up-to-date and relevant data**.

Data labelling criteria should be clear and there should be **lines of accountability** where data involving protected characteristics or special data categories are involved. Bias in the labelling or measurement of variables could be mitigated by holding **consultations with members of protected groups** and **involvement of multiple human labellers.**

06

Security of the AI systems

The **use of AI to process personal data** adds an **extra layer of risk** to the usual data security risks. Organisations will need to manage and assess this carefully.

Whilst the security measures to be adopted will depend on the type of risks, technical and organisational measures are legally required in order to ensure that an **appropriate level of security** is maintained. Such measures include, but are not limited to, **security risk assessments**, regular **model debugging** by internal or external security auditors and **pro-active monitoring and investigation** of anomalies.

07

Human review of decisions

AI systems can be used to **support human decision-making** or make **solely automated decisions**. If the latter is the case, then individuals have the right to not be subject to such a decision and request a human review.

To ensure the integrity of the human review, reviewers will need to:

i. be provided with **adequate training** to analyse and challenge AI decisions,

ii. have the **authority to override** AI automated decisions, and

iii. take into account **additional factors** which are distinct from any of the input data.

The ICO is clear that solely automated decision-making means if **there is no meaningful input by a human in the final decision being made about a person**. Organisations must be careful and should be aware that a decision does not fall outside this scope just because a human has **'rubber-stamped'** it.

08

Engaging with external suppliers

It is becoming increasingly common to procure an AI system from a third party. However, organisations need to keep in mind that they are still subject to data protection legislation as the party responsible for deploying the AI system and therefore the data controller.

Firms should undertake **careful due diligence** before a supplier is contracted and it is recommended that a DPIA is carried out. The **roles and responsibilities** for tasks such as security testing, monitoring, compliance, and handling of rights requests should be **agreed and documented between the parties**. The organisation will need to ensure that it has a reasonable level of understanding of how the AI system works to comply with data protection principles.

Firms should ensure that third parties provide documentation demonstrating a **data protection by design approach**. Where international transfers of personal data will take place, firms should ensure that information rights are protected or whether an exception is applicable.

ICO FAQs

The ICO also provides some answers to FAQs. Where the FAQS are covered in the key points, see the summaries above. For additional topics, see below:

Accuracy Principle – the ICO also states that the **accuracy principle applies to all data** but that this doesn't mean that an AI System needs to be '100% statistically accurate' to comply with this principle. They key is to ensure that the data is not **incorrect or misleading as to any matter of fact** and is sufficiently statistically accurate for your purposes. This does not mean that every inference has to be correct.

Legality of AI – the ICO is clear that no part of data protection legislation explicitly regulates or prohibits use of AI.

Lawful basis – the ICO is clear that there are multiple lawful bases potentially available, they key is to choose the most appropriate one. It particularly notes that although consent may be appropriate, it may be difficult to collect the consent and may be difficult to manage withdrawal of consent when using complex AI systems.

Policies and fair processing information – organisations should provide fair processing notices to individuals (other than in the unusual circumstances where not required by law). A specific AI policy is not needed if the information provided clearly gives individuals what they need to know about the data processing.

What does this mean for organisations using AI?

- Organisations need AI governance, not least to understand if and how AI is being used, whether this use amounts to “solely automated decision-making” and the legal risks associated with this, particularly data privacy risks.
- Organisations using AI should consider producing AI Explainability Statements (given the ICO’s comments around explainability) and/or DPIAs. We advised on the first AI Explainability Statement which was reviewed by the ICO and would be happy to advise further on this.
- Organisations should maintain robust policies and practices around data collection, retention and processing, including for AI use.
- Where there is a risk of discriminatory output from AI systems, organisations should take effective measures to reduce these risks.

AI GROUP KEY CONTACTS

Please get in touch if you have any queries or would like to arrange a discussion or training session with our AI Group

Sophie Sheldon
Managing Associate
Digital Business
E sophie.sheldon@simmons-simmons.com
LinkedIn

Minesh Tanna
Partner and AI Lead
Disputes & Investigations
E minesh.tanna@simmons-simmons.com
LinkedIn

Jonathan Chan
Trainee Solicitor
Simmons Wavelength
E jonathan.chan@simmons-simmons.com
LinkedIn

Salihah Shabir
Paralegal
Digital Business
E salihah.shabir@simmons-simmons.com

How we can help you

We have a dedicated AI Group, comprising lawyers across various practice areas and jurisdictions, which regularly advises clients on AI legal, regulatory and ethical issues. Our recent experience includes:

- Advising one of the world’s largest developers of biometric technology on a response to the European Commission’s draft EU AI Regulation.
- Advising a developer of AI technology on its standard form contractual documents.
- Advising a financial institution on a dispute arising out of the allocation of proprietary rights to an AI system.

We are one of the leading law firms in AI:

- We are regularly invited to speak to national governments (including the UK and UAE governments).
- Our AI Lead, Minesh, is Chair of the Society for Computers and Law (SCL) AI Group (and a former member of the CBI’s Working Group on AI).

We are at the forefront of developments in AI law and involved in cutting-edge projects. For example, in collaboration with Best Practice AI (comprising a member of the World Economic Forum’s Global AI Council), we recently advised on the world’s first AI explainability statement, working alongside the UK Information Commissioner’s Office.

Through Simmons Wavelength, we have numerous in-house data scientists who have day-to-day experience of developing AI models. We are therefore able to offer both legal advice and a practical insight into AI-related legal issues.