SLAUGHTER AND MAY/

DIGITAL
Part of the Horizon Scanning series

NEW ICO GUIDANCE ON AI: PRIVACY BY DESIGN SAVES RETRO-FITTING LATER

22 SEPTEMBER 2020

The Information Commissioner's Office (ICO) has published its long awaited guidance on "AI and Data Protection", which forms part of its AI auditing framework.

The need for guidance

Whether it is helping tackle COVID-19, or managing loan applications, the potential benefits of artificial intelligence (or AI) are clear. However, it has long been recognised that it can be difficult to balance the tensions that exist between some of the key characteristics of AI and data protection compliance, particularly under the GDPR (see our previous client briefing for more details).

Encouragingly, Elizabeth Denham's foreword to the ICO's new AI guidance confirms that "the underlying data protection questions for even the most complex AI project are much the same as with any new project. Is data being used fairly, lawfully and transparently? Do people understand how their data is being used and is it being kept secure?"

Opportunities and risks

"The innovation, opportunities and potential value to society of AI will not need emphasising to anyone reading this guidance. Nor is there a need to underline the range of risks involved in the use of technologies that shift processing of personal data to complex computer systems with often opaque approaches and algorithms" *(Opening statement of ICO guidance on AI and Data protection).*

That said, there is a recognition that AI presents particular challenges when answering these questions, and that some aspects of the law require "greater thought". Compliance with the data protection principles around data minimisation, for example, can seem particularly challenging given that many AI systems allow machine learning to decide what information is necessary from large data sets.

Scope of the guidance

The guidance forms part of the ICO's wider AI Auditing framework, which also includes auditing tools and procedures for the ICO to use in its audits and investigations and a (soon to be released) toolkit that is designed to provide further practical support for organisations auditing their own AI use.

It contains recommendations on good practice for organisational and technical measures to mitigate AI risks, whether an organisation is designing its own AI system or procuring one from a third party. It is aimed at those within an organisation who have a compliance focus (DPO's, legal, risk managers, senior management etc.) as well as technology specialists/developers and IT risk managers. The ICO's own auditors will also use it to inform their statutory audit functions.

It is not, however, a statutory code and there is no penalty for failure to adopt the good practice recommendations if an alternative route can be found to comply with the law. It also does not provide ethical or design principles – rather it corresponds to the data protection principles set out in the GDPR.

Structure of the guidance

The guidance is set out in four parts:

Part 1: This focusses on the AI-specific implications of accountability, namely responsibility for complying with data protection law and demonstrating that compliance. The guidance confirms that senior management cannot simply delegate issues to data scientists or engineers and are also responsible for understanding and addressing AI risks. It considers data protection impact assessments (which will be required in the majority of AI use cases involving personal data), setting a meaningful risk appetite, controller/processor responsibilities and striking the required balance between the right to data protection and other fundamental rights.

Part 2: This covers lawfulness, fairness and transparency in AI systems, although transparency is addressed in more detail in the ICO's recent guidance on 'Explaining decisions made with AI'. This section looks at selecting a lawful basis for the different types of processing (consent, performance of a contract etc.), automated decision making, statistical accuracy and how to mitigate potential discrimination to ensure fair processing.

Part 3: This focusses on security and data minimisation, and examines the new risks and challenges raised by AI in these areas. For example, AI can increase the potential for loss or misuse of the large amounts of personal data which are often required to train AI systems, or can introduce software vulnerabilities through new AI related code. The key message is that organisations should review their risk management practices to ensure personal data is secure in an AI context.

Part 4: This final part covers compliance with individual rights, including how individual rights apply to different stages of the AI lifecycle. It also looks at rights relating to solely automated decisions and how to ensure meaningful input, or (for solely automated decisions) meaningful review, by humans.

Headline takeaway

According to the Information Commissioner, the headline takeaway from the guidance is to consider data protection at an early stage. Mitigation of risk must come at the AI design stage as retro-fitting compliance ‘rarely leads to comfortable compliance or practical products’.

The guidance also acknowledges that, while it is designed to be integrated it into an organisation’s existing risk management processes, AI adoption may require organisations to re-assess their governance and risk management practices.

A landscape of guidance

AI is one of the ICO’s top three strategic priorities, and it has been working hard over the last few years to both increase its knowledge and auditing capabilities in this area, and to produce practical guidance for organisations.

To help develop this latest guidance, the ICO enlisted technical expertise (in the form of Doctor, now Professor, Reuben Binns, who joined the ICO as part of a fellowship scheme). It produced a series of ‘informal consultation’ blogs in 2019 focussed on eight AI-specific risk areas. This was followed by a formal consultation draft published in February, the structure of which this guidance largely follows. However, despite all of this preparatory work, this latest publication is still described as ‘foundational guidance’, as the ICO recognises that AI is still in its early stages and developing rapidly. It acknowledges that it will need to continue to offer new tools to promote privacy by design in AI and to continue to update this guidance to ensure it remains relevant.

From a user perspective, practical guidance is good news and this guidance is clear and easy to follow. Multiple layers of guidance can, however, become more difficult to manage. The ICO has already stated that this latest guidance has been developed to complement its existing resources, including its original Big Data, AI and Machine Learning report (last updated in 2017) and its more recent three part guidance on Explaining decisions made with AI. In addition, there is sector specific guidance being developed (for example the FCA’s AI collaboration with the Alan Turing Institute) and publications from bodies such as the Centre for Data Ethics and Innovation and the European Commission. As a result, organisations will need to start considering how to consolidate the different guidance, checklists and principles into their compliance processes.

This article was written by Duncan Blaikie (Partner) and Natalie Donovan (PSL) from Slaughter and May’s Emerging Tech Group. This article first appeared in PLC Magazine September 2020.