The Information Commissioner's response to the European Commission's White Paper on Artificial Intelligence – a European approach to excellence and trust

About the ICO

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the General Data Protection Regulation (GDPR), the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003 (PECR), amongst 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 White Paper on "Artificial Intelligence – A European approach to excellence and trust" on behalf of the Commissioner. The paper presents interesting ideas and proposals, and we note that the European Commission is considering similar implications of artificial intelligence (AI) to those that the ICO has been looking at.

4. The ICO recognises that AI can bring distinct benefits for individuals and the wider society, but many uses of AI are likely to result in high risk to individuals' rights and freedoms and so, we have made enabling good practice in AI one of our top priorities.

5. As part of our focus on AI, we have co-authored the 'Explaining decisions made with AI' guidance with the Alan Turing Institute – the UK's national institute for AI. The guidance gives organisations practical advice to help explain the decisions delivered or assisted by AI, to the individuals affected by them. The guidance provides specific advice on interpreting and complying with the right to be informed (Articles 13 and 14 of the GDPR), the right of access (Article 15 and

Recital 71), the right to object (Article 21) and rights related to automated decision-making including profiling (Article 22 and Recital 71).

6. We are also producing an AI auditing framework (AIAF) that is being led by our first research fellow in AI. The AIAF is designed to provide the ICO with a solid methodology to assess AI applications and ensure:

    - they process personal data fairly, lawfully, and transparently; and

    - the necessary measures to assess and manage risks to individuals that arise from them are in place.

7. In February, we published draft guidance on the AIAF, which was designed to assist organisations that create and use AI systems to ensure their use complies with data protection law, as well as to provide practical advice to promote best practice. The final guidance will be published later in the summer.

Feedback

8. The following comments set out some of our thoughts on the European Commission's White Paper. We focus on section 5 of the paper, "An ecosystem of trust: regulatory framework for AI" and the implications it has for individual rights and freedoms. Analysis is limited to implications the framework may have for data protection as this is our remit and area of expertise.

9. We agree with the Commission that the "definition of AI will need to be sufficiently flexible to accommodate technical progress while being precise enough to provide the necessary legal certainty". In our work on AI, we have defined it as "an umbrella term for a range of algorithm-based technologies that solve complex tasks by carrying out functions that previously required human thinking."

10. We believe that there may be scope for clarifying transparency requirements. Whilst the GDPR has specific provisions for solely automated decision-making, transparency for data subjects in relation to AI-assisted decision-making depends on interpretation of the GDPR's general fairness requirements. The ICO has given guidance on

this but more clarity on legislative requirements would be helpful. In any case the GDPR standards for profiling and transparency should not be watered down.

11. We appreciate the Commission's proposals for which AI systems should be classified as 'high-risk', and we recognise the value of this in trying to avoid a disproportionate burden for small and medium size enterprises (SMEs). That said, it remains the case that AI use by SMEs may still often be 'high-risk' and it is important that any framework does not unintentionally remove oversight and safeguards for such risk. We also believe that the current proposal may need further elaboration over what is meant by 'significant risk'. Otherwise, the proposal risks becoming circular by saying that an AI application is high-risk if it is used in a high-risk sector.

12. There is no explicit definition of 'risk' in the GDPR, but the various provisions on data protection impact assessments (DPIAs) as they are foreseen in the GDPR make clear that this is about the risks to individuals' rights and freedoms. The concept of potential harm or damage to individuals links to risk. Examples of risks are where processing may lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. We believe that this could provide a basis for the Commission to decide on what basis AI applications should be considered high-risk.

13. The Commission's White Paper introduces the two criteria approach mainly defining 'high-risk' AI as follows: 'considering whether both the sector and the intended use involve significant risks, in particular from the viewpoint of protection of safety, consumer rights and fundamental rights'. We believe that it is helpful, when defining 'high-risk AI' within this two-criteria approach, to consider not only the broad sector, but within that also the specific context in which AI is being applied. Not all applications of AI in a high-risk sector will be high-risk – as the Commission reflects in the second criteria – suggesting that the context in which the AI is used is also significant. For example, AI is high-risk if it is being used for medical diagnosis, decisions made by law enforcement about prosecutions, or for employment purposes because these purposes are likely to have a significant impact on individuals. We believe that by adopting a

context-sensitive approach in this way, the exceptional instances the Commission talks about will be captured in the two criteria set out.

14. We welcome the discussion on human oversight and the proposed manifestations of this. We would highlight that any human intervention must be meaningful to reduce the chances of adverse effects. Non-meaningful human intervention could arise where there is automation bias or where there is a lack of interpretability. We discuss 'what is the role of human oversight' in our draft guidance on the AIAF.

15. We appreciate the Commission looking at the addressees of the legal requirements, as this is an issue that we too are considering. We recognise that in many cases, the various processing operations involved in AI may be undertaken by different organisations. It is therefore crucial that organisations determine what legal requirements they have. The accountability principle in the GDPR makes controllers responsible for complying with data protection law and says that they must be able to demonstrate their compliance.

16. We also welcome the recognition in the White Paper of the role and responsibilities of providers of AI systems. Where they are not processing personal data, they fall outside GDPR, but the features of the products they provide are a key determinant of how fairly and transparently AI is used in practice. A conformity assessment scheme for producers could help to identify likely risks to individual rights and freedoms. For example, a conformity assessment could assess how easy it is to interpret how an AI system made a decision. At the same time, we accept that this only provides assurance at a point in time and does not cover the application of the AI system in practice.

17. Our initial thoughts on a voluntary labelling for AI applications that are not classed as high-risk are that this may provide organisations with some assurance that their AI systems have obtained a minimum requirement of trustworthiness. However, organisations will still have responsibilities and a duty to ensure their AI application is compliant with the law.

Conclusion

18. We welcome the EU Commission's White Paper on AI and its proposals. We recognise the need for a risk-based approach that does

not stifle innovation or prevent the benefits of AI being realised. We also recognise that the challenges created or exacerbated by AI apply across different regulatory regimes. The ICO has taken steps to address this challenge by working with other UK regulators on AI issues. Underpinning many of these challenges for different regulatory regimes is data protection. It is important that any new AI legal framework should either reinforce or bolster data protection law's regulation of AI.

19. We will monitor any further developments from the EU Commission regarding this White Paper and will contribute when appropriate.