The Information Commissioner's response to the UN Special Rapporteur (UNSR) draft Data Privacy Guidelines for the development and operation of Artificial Intelligence solutions

About the Information Commissioner

The Information Commissioner has responsibility in the UK for promoting and enforcing the General Data Protection Regulation (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, amongst others.

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

We welcome the aim of setting guidelines for the development of AI at an international level. Organisations deploying AI are often doing so globally (for example via internet platforms) as well as at national level, while data protection regulators operate for the most part within national jurisdictions. These guidelines can therefore supplement their work. It has also been suggested that we are seeing the development of differing regional approaches to the use of AI, but human rights are universal and so this UN initiative can support a consistent respect for these rights.

We have previously commented on an earlier draft of these guidelines, and we note that some of the suggestions we made were accepted by the UNSR. We thank the UNSR for this. However, we still have some further comments about the latest version of the draft guidance.

Please find these comments below.

A.1 General remarks

The Introduction notes that:

> the concrete verification of the decision logic of highly complex AI systems on the basis of disclosed algorithms is likely to be difficult in practice

This is certainly an issue, and we would observe that there are a number of approaches which have been developed that query highly complex AI systems in order to provide a form of explanation (eg LIME and SHAP). This is sometimes called 'a model to explain the model'.

We suggest that a line could be added to the guidelines, to the effect that there are some tools available to help organisations understand and explain the decisions made by AI systems and some organisations are already adopting these methods.

B.2 Lawful basis and purpose limitation

The factors listed in the 'lawful basis and purpose limitation' section generally reflect those in the GDPR. However, the issue of data minimisation was not addressed. This is a challenging principle in relation to AI systems, considering that big data and AI solutions often require the accumulation of vast amounts of data. However, there should be a reasonable limit on the amount of data collected and processed, depending on the particular purpose. Also, data should not be kept indefinitely once it is no longer required for that purpose. We recommend that reference could be made to this.

B.3 Accountability

We agree that the accountability of organisations for data processing in their AI systems is key. A number of human actors within an organisation have a role to play in this. Demonstrating how an organisation has been responsible should not be delegated to just the data protection officer. Senior management, data scientists and engineering teams are also accountable for understanding and addressing issues appropriately and promptly.

Governance and risk management capabilities should be proportionate to the use of AI. This is particularly true now while AI adoption is still in its initial stages, and the technology itself, as well as the associated laws, regulations, governance and risk management best practices are still developing quickly.

B.4 Control

In this section we think it would also be helpful for the guidelines to comment on situations where an organisation procures an AI system from a third party. The organisation that procures the system should expect evidence and assurances from the organisation that built it that it has been created in line with data protection principles, and there should be provision for this in contracts between vendors and procurers.

B.6 Rights of the data subject

We recommend that as well as the more specific rights the UN provide in this section, there could also be reference to fundamental rights such as the right to privacy and the right to non-discrimination.

C.2 Test and correction phase

We feel that the suggestion of a 'black box in the internet' is an interesting one, but perhaps not practicable in all cases. It might be helpful, while emphasising the need for testing, to recognise that this can be done in various ways, for example a regulatory 'sandbox' in a jurisdiction where this is available, and also through user testing.

Conclusion

We hope that these comments are useful, and we look forward to the next version of the Guidelines.

Information Commissioner's Office

2 November 2020