BCLP. Client Intelligent

Insights

COMPUTER SAYS YES? WHAT DO THE UK'S PROPOSED DATA PROTECTION REFORMS MEAN FOR AI?

May 26, 2023

SUMMARY

How should artificial intelligence ("AI") be governed? This conundrum is rightly receiving considerable attention from governments, businesses and civil society. Should controls be principles-based, as proposed in the UK's AI White Paper? Or would it be better to implement granular regulation, prohibiting some applications and requiring high-risk systems to undergo prior certification, like the EU's draft AI Act?

Whatever the result of the debate surrounding new AI regulation, in the UK and EU, AI is already regulated to some extent through the General Data Protection Regulation ("GDPR"). This includes restrictions on use of personal data for automated decision-making ("ADM") including profiling.[1] The UK is currently reforming its GDPR-originated data protection laws, so this briefing shifts the spotlight onto the impact of the UK's proposed reforms on AI systems.

AT A GLANCE

We see three main areas where the UK's proposed data protection reforms look set to facilitate the development and use of AI systems:

1. Greater clarity around anonymisation – anonymised "personal data" could be freed up to use for machine learning
2. Making "robot" decision making easier by reducing the restrictions around significant ADM
3. Clarifying permitted re-purposing of personal data - potentially making it easier for use in connection with AI systems.

Together with the UK's high level, principles-based approach to AI regulation, these proposed reforms are in stark contrast to the controls proposed in the EU's draft AI Act. This is sure to provide

another factor to be weighed by the European Commission when it comes to re-visit the UK's adequacy status (due to expire in 2025).

On a more positive note, the amendments highlighted below are AI-permissive and appear aligned with the UK's light touch approach towards the regulation of AI. In particular, the proposed reforms could help ease the burden of UK GDPR compliance for organisations using "anonymised" personal data for AI training purposes. This may help to make the UK an attractive destination for cutting-edge AI R&D operations.

THE UK'S DATA PROTECTION REFORM AGENDA

On 8 March 2023, the Department for Science, Innovation and Technology ("**DSIT**") introduced the UK government's updated proposals for data protection reform in the shape of the Data Protection and Digital Information (No.2) Bill (the "Revised Bill"). The introduction of the Revised Bill resumes the legislative process abruptly halted in 2021, although it does not depart significantly from proposals set out in the initial bill.

Compared with some of the radical ideas in the original 2021 public consultation exercise (Data: A new direction), the Revised Bill resembles more of a "light trim" than fundamental post-Brexit pruning. Nevertheless, Technology Secretary Michelle Donelan has described it as providing a "*new common-sense led UK version of the EU's GDPR [that] will reduce costs and burdens to British businesses*", with the government predicting savings of more than £4 billion for the UK economy over the next 10 years.

DO I KNOW YOU? CLEARER BOUNDARIES AROUND ANONYMISED DATA

Some changes are proposed to the definition of "personal data", centred on when an individual is "identifiable" or not. These adjustments appear somewhat technical but could have a more profound impact, by bolstering the robustness and legal certainty of "anonymisation" processes. Information that cannot be linked to an identified or identifiable living individual is out of scope of the UK GDPR, meaning that "anonymised" information derived from personal data would be available to use for research and analysis without needing to take further steps to comply with the UK's data protection legal framework.

According to the amendments, there would be two circumstances in which information (relating to an individual who is not clearly *identified*) is considered to relate to an *identifiable* individual (and therefore amounts to personal data):

1. Where the controller or processor can themselves identify a living individual from the information they are processing, by using reasonable means; or

2. Where the controller or processor knows or ought reasonably to know that (i) as a result of their processing, another person is likely to obtain the information **and** (ii) that other person could identify a living individual using reasonable means at the time of the processing.

For the purposes of (2) above, an organisation that failed to implement appropriate security measures would be deemed to "know" another person was likely to obtain the information.

"REASONABLE MEANS" TO IDENTIFY

The Revised Bill confirms that an individual will be identifiable via "reasonable means" if the individual "is identifiable by the person by any means that the person is "*reasonably likely to use*". Whether a person is reasonably likely to use a given means of identification will depend on factors including (i) the time, effort and costs involved in identifying the individual by that means, and (ii) the technology and other resources available to that person. The explanatory notes accompanying the Revised Bill state that this is not an exhaustive list and other factors could be relevant, such as whether re-identification would be lawful. Regulatory guidance will be important in this area, if the intended certainty is to be achieved.

IMPACT ON AI

These changes should benefit AI labs and other organisations subject to the UK GDPR which are seeking to train AI models. The "training" process in machine learning requires the processing of huge volumes of data, in order to produce meaningful and reliable outputs. At present, even if training data has undergone a technical process of "anonymisation" by a third party before being used, the UK GDPR's broad concept of "personal data" means that training data could be considered personal data if individuals could possibly be identified directly or indirectly, i.e. without establishing any degree of probability.

The proposed changes would mean that when using large volumes of "anonymised" data to train AI models, organisations will not necessarily be treated as processing personal data simply because individuals *could* (theoretically) be re-identified. As a result, these organisations may be able to avoid the significant UK GDPR compliance burdens that would otherwise apply to that processing.

LET THE ROBOTS DECIDE!

A WIDER RANGE OF SIGNIFICANT DECISIONS COULD BE TAKEN WITHOUT HUMAN INTERVENTION

Decisions that (i) are wholly automated (i.e. without meaningful human involvement) and (ii) have a "significant" impact on an individual, could be taken provided that safeguards for individuals' legitimate interests, rights and freedoms are in place. A decision is considered "significant" where it produces legal or similarly significant effects for the individual. ADM could readily be a feature of some AI systems that make use of personal data. Under the EU's draft AI Act, both ADM and

profiling are likely to be linked to "higher risk" AI systems (e.g. biometric identification and categorisation of natural persons) or "prohibited" AI systems (e.g. those used for government "social scoring").

BUT SAFEGUARDS MUST BE PUT IN PLACE

Currently, ADM that produces legal or other significant effects for individuals can only take place in three situations: (i) where the ADM is necessary for entering into/performing a contract with the individual, (ii) where the ADM is authorised by law or (iii) with the individual's explicit consent (which can be revoked) (Article 22, UK GDPR). The Revised Bill removes these limits for "non-special category" personal data but adds an obligation to ensure that safeguards are in place for the individuals' rights, including providing information about the decision making and providing details about how to contest the decision and seek human intervention. The details are expected to be set out in future regulations. Tighter controls would remain in place regarding ADM involving special category personal data (e.g. relating to health).

USING PERSONAL DATA FOR NEW PURPOSES

The reforms also broaden the ability of a controller to undertake further processing of personal data in certain circumstances, where this further processing is compatible with the original purpose. The purpose-compatibility principle is well established in data protection law (Article 5(1)(b) UK GDPR). The change proposed here is the addition of a new Article 8A UK GDPR, setting out various conditions for determining whether a new purpose is compatible with the original purpose. In addition, the Revised Bill introduces a new annex to the UK GDPR which sets out conditions where such compatibility can be deemed to arise and personal data may thus be further processed. These measures could make it easier for personal data collected for one application to be re-purposed for use in training AI systems.

NEXT STEPS

The speed of progress of data protection reform is difficult to gauge. At the time of writing, the Revised Bill is at the third reading stage in the House of Commons – i.e. an early stage.

The proposed amendments are consistent with the UK government's policy focus on fostering innovation and sustaining the UK as a global AI powerhouse. According to the National AI Strategy, the UK ranked behind only the USA and China for private investment into AI companies in 2020. Both the Revised Bill and the AI regulation White Paper (open for public consultation until 21 June 2023) reflect a desire to capitalise on this position.

RELATED INSIGHTS

- Our UK and EU AI regulatory tracker

- Our insight on the impact of the Revised Bill for “business as usual” activities

---

[1] “Profiling” is defined in the GDPR as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483
