GIBSON DUNN

Ahmed Baladi is a partner and Thomas Baculard is an associate at Gibson, Dunn & Crutcher LLP. Mr Baladi can be contacted on +33 (1) 5643 1350 or by email: abaladi@gibsondunn.com.

EXPERT BRIEFING ARTICLE REPRINT April 2024

Artificial intelligence and the GDPR

BY AHMED BALADI AND THOMAS BACULARD

One of many definitions of artificial intelligence (AI) describes the technology as machines or systems performing tasks that would ordinarily require human brainpower.

Given the strong benefits AI can generate in all industry sectors, as well as the risks of some of its applications, the European Union (EU) launched a large project to regulate AI to ensure the best conditions for the safe development and use of this technology. This has resulted in a proposal for a regulation laying down harmonised rules on artificial intelligence: the AI Act.

At the time of writing, the AI Act is still a proposal and is awaiting formal adoption by the European Parliament and endorsement by the Council. This regulation will apply to certain providers, deployers, distributors, affected persons and authorised representatives of providers of 'AI systems'.

As to how AI systems operate, the draft AI Act indicates that such systems infer, from the input they receive, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Therefore, in order to be developed, AI systems need to be trained on large amounts of data and they may also, once deployed, continue to be improved based on the data received when in operation.

The General Data Protection Regulation (GDPR) is a technologically neutral regulation that applies to the processing of personal data (provided it is subject to the material and territorial scope of application of the GDPR). Therefore, when processing personal data in the context of AI, be it for the development and training phase and or during the use of an AI system, the GDPR will apply and AI providers and deployers will need to comply with GDPR requirements in addition to AI Act requirements.

In this regard, article 2.5.a and recital 5aa of the draft AI Act clearly indicate that the AI Act will apply without prejudice of the requirements set by the GDPR. Therefore, these two sets of obligations will apply at the same time.

This article touches upon some of the main challenges in complying with the principles laid down by the GDPR when developing and using AI systems. Such challenges are due to various factors, including the amount of data processed, the source of the data or the opacity of AI systems' functioning.

We have highlighted some of the most salient GDPR compliance challenges organisations will face, including: (i) complying with some of the core principles of the GDPR; (ii) complying with transparency obligations; (iii) ensuring effective data subject rights; and (iv) identifying the legal basis for processing.

Article 5 principles

Compliance with the following core principles of the GDPR can prove challenging for providers or deployers of AI systems but is all the more important because data protection supervisory authorities will need to pay close attention to this aspect of data processing.

Accuracy. A very popular method for developing AI systems, outside of reusing specific training data sets, is through scraping of publicly available data including personal data. However, the data made available to AI systems will not always match factual circumstances, so personal data may not always be processed

accurately, and data subjects could be tempted to request that such data is updated in the context of its processing by an AI system. This first GDPR requirement illustrates the practical challenge faced by AI providers seeking to satisfy it.

Data minimisation. Complying with this principle can be challenging due to the fact that AI systems are usually built on a large amount of structured or unstructured data, including personal data. During the 45th Global Privacy Assembly in October 2023, a resolution was adopted on generative AI (GenAI) systems and, as to data minimisation, the resolution noted that personal data must be used as training data only if required to achieve the intended purposes of the GenAI system and only after a data protection impact assessment has been carried out.

In addition, the French Data Protection Authority (CNIL) issued guidance on practical measures ensuring data minimisation. The CNIL also specified in relation to the reuse of publicly accessible data that the scraping tools used must be configured to allow compliance with the minimisation principle (e.g., define specific criteria for collection, only collect relevant data and immediately delete irrelevant data).

Transparency

The application of the GDPR triggers the obligation to inform data subjects of the processing of their personal data in a concise, transparent, intelligible and easily accessible way.

However, some exceptions to this obligation are provided by article 14.5 of the GDPR, such as when the provision of the required information proves impossible or would involve a disproportionate effort. We note that there is a risk that a data protection authority would consider this exception as not applicable. For instance, the Italian data protection supervisory authorities and those of the UK have ruled that Clearview AI failed to adequately inform data subjects of the processing of their personal data and imposed heavy fines on the organisation.

Finally, in the case of automated decision making (including profiling), the principle of transparency also involves the provision of meaningful information about the logic involved and of the significance and envisaged consequences of such processing for the data subject.

Such decisions may be based on complex AI models which are difficult to explain and whose outcomes are difficult to interpret due to the sophisticated nature of their architecture. Therefore, it will be technically challenging and costly to retrieve such information and provide it in a clear, understandable form.

Data subject rights

Under the GDPR, data subjects whose personal data is processed by AI systems will be able to exercise their various rights (e.g., access, erasure, rectification and objection).

In this regard, the resolution adopted by the 45th Global Privacy Assembly highlights that developers, providers and deployers of GenAI systems will implement appropriate technical and organisational measures in order to ensure that affected data subjects are able to exercise their rights.

Organisations can face various challenges to enable data subjects to exercise their rights. Most importantly, organisations can struggle to retrieve the personal data in question that can be embedded within the system, making it difficult to link it to a specific data subject. To mitigate these difficulties, organisations should implement data labelling and data mapping measures, adopt 'privacy by design' concepts when building the AI system, and make use of privacy enhancing technologies.

Legal basis

Under the GDPR, organisations are required to only process personal data if such processing is lawful and relies on an appropriate legal basis. Therefore, choosing the right legal basis for the processing of personal data in the context of an AI system is crucial. In this respect, consent and legitimate interest are the two legal bases that stand out as the most suitable despite presenting a number of challenges.

Consent. This would be an adequate legal basis only if it is freely given, specific, informed and unambiguous. Since consent may need to be given on a case by case basis depending on the intended purpose of the processing, it can prove very challenging for organisations to precisely define the purposes of the processing and allow users to provide their consent for each of them. In addition, organisations would also have to grapple with the possibility of data subjects withdrawing their consent, which would deprive them of the future use of their personal data in the context of the operation of the AI system.

Legitimate interest. Considering the inherent difficulty of relying on the consent legal basis, legitimate interest may be more appropriate to rely on when processing personal data for AI purposes. However, this is subject to demonstrating the existence of an actual legitimate interest and to completing a legitimate interest assessment. Based on the G29 Opinion 06/2014 on the notion of legitimate interest, the CNIL, in its 2022 Clearview AI decision, considered that even if "the fact that personal data is publicly available may be considered as a factor in the assessment" of the existence of a legitimate interest, such legitimate interest would only exist "if the publication was carried out with a reasonable expectation of further use of the data for certain purposes".

Conclusion

Ensuring compliance with GDPR obligations when processing personal data for developing or using AI systems is paramount. Data protection supervisory authorities will strongly enforce these principles and have started to do so. However, navigating the application of GDPR concepts to AI remains challenging and will require organisations to incorporate even more the concept of privacy by design when building their AI systems. ■

This article first appeared as exclusive online content for April 2024 on www.financierworldwide.com.