Belgian Data Protection Authority Publishes Guidance on the Interplay between the GDPR and the AI Act

September 25, 2024 By Wim Nauwelaerts and Alice Portnoy

On 19 September 2024, the Belgian Data Protection Authority (DPA) issued new Guidance on the interplay between the recently adopted EU Regulation on Artificial Intelligence (the AI Act) and the General Data Protection Regulation (the GDPR), which aims to provide further insight into the use of artificial intelligence (AI) systems that process personal data.

The DPA's key take-aways can be summarized as follows:

1. Data Protection Officers play an essential role in ensuring a company's compliance with the GDPR, including when the company provides or uses AI systems – as this concept is defined in the AI Act – that rely on personal data to generate outputs.

2. AI systems should be understood as systems specifically designed to analyze data (incl. personal data), identify patterns, and use such data knowledge to make informed decisions or predictions. AI systems can also learn from data and improve their performance to generate more accurate or nuanced outcomes. The Guidance provides some examples of technologies that should be viewed as AI systems, such as spam filters that help determine

if emails are legitimate, streaming recommendation systems that assess users' viewing preferences and suggest content, or virtual assistants that respond to users' commands and complete selected tasks.

3. The AI Act does not contain explicit references to fair use of AI systems, whereas fairness of personal data processing is one of the key principles of the GDPR. However, the AI Act only allows for the development and use of trustworthy AI systems that do not leave room for bias and discrimination.

4. The riskier the AI system, the greater the need to provide users with clear and precise information on how personal data is used, how decisions are made, and how potential biases are mitigated.

5. The AI Act does not provide for specific personal data retention rules. Businesses that deploy AI systems which process personal data will, however, not be exempted from establishing clear retention policies or schedules that will need to meet GDPR requirements.

6. The GDPR and the AI Act have different approaches regarding automated decision-making (ADM). The GDPR offers individuals the right not to be subject to ADM based on the processing of their personal data and to challenge decisions they consider unfair or inaccurate. The AI Act requires businesses deploying high-risk AI systems to ensure human oversight throughout the whole lifecycle of the AI system. This means that businesses subject to the AI Act must design and implement significant governance measures that allow for humans to be involved in all steps of the use of AI systems (and not only when individuals wish to challenge certain outcomes).

7. The GDPR requires companies to protect personal data via the implementation of technical and organizational measures such as encryption or pseudonymization. The AI Act imposes higher security standards on providers and deployers of high-risk AI systems, especially where there are risks of bias or data or system manipulation. By way of example, the AI Act requires businesses to run upstream risk assessments, ensure continuous monitoring and testing, and guarantee human oversight throughout the lifecycle of a high-risk AI system to ensure the security of the processing.

8. The GDPR grants individuals specific rights regarding the processing of their personal data (e.g., the right to access, rectify, or delete their data). The AI Act complements the GDPR in that it imposes important transparency obligations on businesses deploying AI systems that process individuals' personal data. Moreover, the AI Act will allow individuals affected by certain high-risk AI systems to obtain from deployers clear and meaningful explanations about the outputs generated by such systems and to file complaints about potential infringements of the AI Act with the relevant market surveillance authorities.

9. The GDPR's accountability principle expressly requires businesses to take responsibility for what they do with personal data and to demonstrate their compliance with the regulation (e.g., by drafting policies and procedures, keeping records of processing activities, personal data breaches, or individuals' consent, or by performing data protection impact

assessments). Under the AI Act, businesses providing or deploying AI systems will still have to carry out certain activities to prove their compliance with applicable AI Act requirements. For instance, the AI Act requires businesses to classify their AI systems to identity the level of risks that can be posed to users, or to report and document security incidents suffered due to a high-risk AI system's malfunction.

The DPA's Guidance stresses the importance for companies designing or using AI systems that process personal data of individuals to ensure compliance not only with the AI Act, but with the GDPR as well. Companies would be well-advised to assess to what extent these EU regulations apply to them, and to design, if necessary, a suitable compliance plan.

Filed Under: AI, Artificial Intelligence, Belgium, GDPR

Wim Nauwelaerts is a partner in the Brussels office, leading Alston & Bird's European Privacy, Cyber & Data Strategy Team. Wim has over 20 years of experience working with global companies on their data protection, privacy, and cybersecurity needs, including General Data Protection Regulation (GDPR) readiness, data transfer, data security and breach requirements, and compliance training.

Alice Portnoy is an associate in Alston & Bird's Brussels office and a member of the Privacy, Cyber & Data Strategy Team. Alice focuses her practice on technology and data privacy matters with experience counseling national and international companies across the media and entertainment, pharma, scientific research, education, nonprofit, and food and retail sectors.