04 September 2024

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

"Annual Privacy Forum 2024"

Keynote talk

Wojciech Wiewiórowski
European Data Protection Supervisor

Ladies and gentlemen, allow me to begin by thanking the organisers for the opportunity to speak once again at the Annual Privacy Forum.

The year 2024 holds significant importance for the European Data Protection Supervisor (EDPS). On one hand, we are celebrating two decades since our establishment as an independent supervisory authority for data protection. On the other hand, with the entry into force of the AI Act on August 2, 2024, we have assumed the responsibility as the competent authority for AI systems provided and deployed by EU Institutions, Bodies, Offices, and Agencies, with the duty to ensure a high level of protection against the potential harmful effects of AI systems.

2024, also marks the tenth anniversary of the EDPS Internet Privacy Engineering Network (IPEN) initiative. As some of you may have already noticed, even our IPEN event has not escaped the influence of AI. In last year's edition, we focused on explainable artificial intelligence, examining the relationship between humans and technology and its effect on fundamental rights. Yesterday, the IPEN event focused on "Human Oversight of Automated Decision-Making," bringing together experts from various fields to discuss the importance of human oversight in AI decision-making. This event highlighted the need for ongoing collaboration and knowledge-sharing among privacy engineers, psychologists, and other experts to ensure that AI systems are designed and implemented in a way that allows effective human oversight.

While we can celebrate the benefits of AI, we must also acknowledge the challenges it poses to individuals' privacy and safety. Given my dual role as the European Data Protection Supervisor (EDPS), I have a unique perspective on this issue. From a data protection perspective, I observe the increasing use of AI systems to analyse and make decisions based on personal data, which presents new challenges for data protection. On one hand, AI can be used to improve data protection and enhance privacy. On the other hand, it can also erode privacy by analysing and exploiting personal data in ways previously unimaginable. As the AI Act supervisor, I see systems that may or may not process personal data, such as critical infrastructure control systems or autonomous vehicles.

As we gather here today in Karlstad, Sweden, I am reminded of some of the many ongoing AI projects in Sweden. Among them, the AI model used in Vetlanda to identify patients at risk, AI-driven assessment within the social services in municipalities like Lunds or Värmdö. At national level, I recall Trafikverket's (the Swedish Transport Administration) project to help optimise the country's road infrastructure management using computer vision and machine learning and Karolinska Institute's project that leverages AI to identify patients that need early preventive treatment.

Also, I would like to take a moment to refer to a recent development in our host country. Just last June, the Swedish government announced plans to introduce real-

time facial recognition technology, leveraging public surveillance cameras to identify suspects in potential crimes. The European Union's regulation on artificial intelligence generally bans real-time facial recognition in public spaces, although exceptions are allowed for law enforcement in certain cases.

As you probably know, the EDPS and the EDPB have already highlighted in our joint opinion our concerns about the use of AI for automated recognition of human features in public spaces. A thorough risk assessment is crucial to identify and address potential threats to individual privacy. Once identified, strong safeguards must be put in place to comply with the GDPR and the new AI Regulation. I am convinced that the implementation of this system in practice will be an early test of the recently adopted AI Act Regulation and will probably act as a key reference not only in Sweden but also for other Member States.

Reflecting on the need to assess risks and apply mitigation measures, I would like to return to the core of this year's Annual Privacy Forum. In this context, I commend the efforts of some AI developers and researchers who are working on addressing the concerns around AI and fundamental rights. It is crucial to develop technologies that allow for the deployment of new services without compromising fundamental rights. Later today, we will hear about the use of AI Cards as a tool to promote transparency and accountability. Differential privacy, which is on tomorrow's program, is another tool that can enhance individuals' privacy when building training datasets. Beyond the topics covered in this APF edition, I also find it important to consider safeguards such as AI alignment, which aims to ensure that AI systems are designed to align with human values and respect fundamental rights. Additionally, the development of techniques such as machine un-learning, which allows AI systems to "forget" certain data or patterns, is a promising approach to mitigate the risks of AI systems retaining and processing sensitive personal data. As in other contexts, I sometimes feel that we are too often trying to solve problems that we should not have created in the first place.

AI is a powerful new technology, but the need to assess the impact on privacy of new applications is technology-agnostic; the same concerns could apply to big data, cloud computing, and many other innovations. The challenges of new technologies enabling unprecedented data processing are not new. The GDPR principle of "privacy by design and by default" and the requirement of conducting Data Protection Impact Assessments are two of the tools that help us in addressing those challenges. These challenges are also reflected in the AI Act, which emphasises the importance of integrating risk management and transparency throughout the lifecycle of AI systems, particularly in high-risk applications like facial recognition.

These principles require that data protection measures be integrated into the development of processes and technologies from the outset, ensuring that personal data is handled with the highest levels of security and privacy by default. By adopting a privacy-by-design approach, using privacy-enhancing technologies,

conducting privacy impact assessments, and engaging with stakeholders from a wide range of backgrounds and disciplines, we can ensure that AI systems are designed and implemented in a way that prioritises individual privacy.

We should not halt technological progress, but we must influence it to ensure that this progress is positive and aligned with our fundamental values.

If adequate investment is done in Privacy-Enhancing Technologies (PETs), they can become increasingly important in balancing the rapid advancements in technology with the need to protect individual privacy. By developing these technologies alongside innovations in data processing, we can create systems that not only drive progress but also safeguard the privacy and rights of individuals. This dual approach ensures that technological advancements do not come at the expense of the fundamental freedoms that underpin our societies.

PETs could play a crucial role in the responsible and secure development of AI, particularly in addressing privacy concerns related to the collection, storage, and processing of large volumes of personal data. Techniques such as differential privacy, homomorphic encryption, and secure multi-party computation enable data analysis and machine learning while minimizing privacy risks. However, this is not an easy path. For PETs to truly benefit AI development, however, they must be mature, widely adopted, and integrated into AI systems' lifecycle. Achieving this will require overcoming challenges such as standardisation, increasing education and awareness, investing in research and development, and improving the accessibility of these technologies to developers.

The acknowledgment that new technologies bring new risks, which are multifaceted and far-reaching, is the initial step; the second step is to invest and develop mitigation measures such PETs. I firmly believe that no single entity, whether in the public or private sector, can do this alone. That is why I strongly advocate for a collaborative approach. By working together, we can drive the development of privacy-enhancing technologies to new heights, making them more robust, more reliable, and more widely available to all.

Let me conclude by emphasising once more that we must work together to develop and implement AI systems that prioritise privacy, transparency, and accountability. Only by doing so can we ensure that the benefits of AI are realised, while protecting the fundamental right to privacy.

Thank you.