ForumEurope

The 14th Annual European Data Protection & Privacy Conference

26 March 2025, Sofitel Europe, Brussels

08:30 - 09:00 Registration

09:00 - 09:30 Keynote speeches
Liisa-Ly Pakosta, Minister of Justice and Digital Affairs, Estonia (tbc)
Anu Talus, Chair, EDPB **(confirmed)**

09:30 – 10:40 Panel 1: The GDPR and the broader EU Digital Rulebook: What does the next chapter hold for innovation and privacy?

As the EU has embarked on a new legislative cycle with a renewed focus on digital transformation, innovation and competitiveness, the future of GDPR remains a topic of intense discussions. Nearly seven years after its adoption, the regulation continues to serve as a cornerstone of individuals' protection in the digital age, but its implementation has revealed certain challenges. At the same time, Europe's expanding "digital rulebook" has introduced both new complexities and opportunities for organisations operating within the bloc.

Following the European Commission's review of the GDPR in June 2024 and with the proposed procedural regulation aiming to harmonise cross-border enforcement under consideration, this panel will discuss the successes of the GDPR and address areas for improvement amidst a rapidly changing digital and regulatory landscape. With a wave of recent regulations shaping Europe's digital strategy,, the session will also explore the implications of the evolving EU "digital rulebook", how these new laws interact with GDPR principles, and the impact on data governance, consumer trust, and innovation. Finally, the panel will examine the evolving priorities of the EU Commission and Parliament to balance robust data protection rules with Europe's ambitions for a thriving and competitive digital economy.

Possible questions include:

- How can the proposed regulation on improving GDPR cross-border consistency and cooperation mechanisms enhance the effectiveness of enforcement? Is a more centralised GDPR enforcement mechanism needed?
- What further action is required from DPAs, particularly for SMEs, to provide clearer, more consistent guidance to ensure better compliance with an increasingly complex regulatory matrix?

- How can the tensions between GDPR enforcement and other new regulations be addressed to ensure a coherent digital regulatory framework? How can cooperation between EU data protection regulators and other supervisory authorities be enhanced to improve regulatory consistency and compliance efforts?
- How can organisations effectively align GDPR compliance with the obligations of new EU digital rules? What governance strategies can help businesses navigate potential legal inconsistencies between these frameworks? What role can technology play in facilitating compliance and enforcement?
- How can policymakers strike a balance between safeguarding citizens' rights and fostering technological innovation at scale and to what extent will the upcoming European Data Union Strategy address this?

Hielke Hijmans, President of the Litigation Chamber - Member of the Executive Committee, Belgian Data Protection Authority **(confirmed)**
Olivier Micol, Head of Unit for Data Protection, DG JUSTICE, European Commission **(confirmed)**
Markéta Gregorová, Member, European Parliament **(confirmed)**
Ilias Chantzos, Global Privacy Officer and Head of EMEA Government Affairs, Broadcom **(confirmed)**
Maryant Fernández Pérez, Head of Digital Policy, BEUC - The European Consumer Organisation **(confirmed)**

10:40 – 11:10 Coffee Break

11:10 – 12:20 Panel 2: Balancing Privacy, Security and Public Safety: Law Enforcement Access to Personal Data in a Digital Era

The growing volume of data, coupled with the rapid evolution of technology, has transformed the landscape of criminal investigations. While these advancements offer unprecedented opportunities for law enforcement to combat crime, they also raise significant concerns about privacy, surveillance, and the erosion of fundamental rights. As the forthcoming e-Evidence Package, set to apply in 2026, reshapes the landscape for cross-border data access in the EU, stakeholders are confronted with issues regarding adherence to democratic values, privacy, the rule of law, and human rights protections.

This session will discuss the legal, technological, and ethical dimensions of data retention and law enforcement access to data, with exchanges on the evolving legal framework governing such access, including but not limited to the implications of the e-Evidence Package, the LED, the Europol Regulation, and the work of the High-Level Group on access to data for effective law enforcement. It will also highlight what can be expected in the roadmap for the implementation of concrete measures

to guarantee access to data for effective law enforcement due to be released by the European Commission in the first half of 2025?
The discussion will also explore how emerging technologies such as AI are influencing law enforcement operations and whether current data protection frameworks and oversight mechanisms adequately protect individual rights.

Possible questions include:

- To what extent will the e-Evidence Regulation and Directive concretely help streamline cross-border access to data? What should the roadmap for the implementation of concrete measures to guarantee access to data for effective law enforcement expected from the European Commission in the first half of 2025 include?
- What are the operational implications for service providers, and how are they preparing to comply with evidence requests under strict time limits?
- How can the principles of legitimacy, necessity, transparency, and proportionality guide data retention practices for law enforcement purposes? Are current oversight mechanisms sufficient to ensure accountability and protect individual rights, including access to effective remedies?
- How are access to data at rest in a provider's system, real-time access to data in transit, and access to data at rest on a user's device addressed by the policy framework?
- How can AI and other emerging technologies be leveraged to improve law enforcement activities without compromising privacy or exacerbating discrimination?
- How can collaboration between law enforcement agencies, policymakers, and the tech industry foster solutions that balance security needs with the protection of fundamental rights?
- What are the challenges and opportunities in balancing national interests, public safety, and fundamental rights in the context of international data access, considering the current geopolitical context?

Ignacio Gómez Navarro, Team Leader, E-evidence and Cybercrime, Security in the Digital Age Unit, European Commission **(confirmed)**
Jürgen Ebner, Deputy Executive Director, Governance Directorate, Europol (tbc)
Chloé Berthélémy, Senior Policy Advisor, EDRi **(confirmed)**
Lorelien Hoet, Director of EU Government Affairs, Microsoft **(confirmed)**
Catherine Van De Heyning, Professor, Protection of Fundamental Rights and Law & Technology, University of Antwerp **(confirmed)**

Moderated by: Júlia Tar, Data Privacy and Security Reporter, MLex **(confirmed)**

12:20 – 12:45 Fireside discussion: Privacy, Advertising and Competition in Digital Markets

As the digital economy continues to grow, privacy, competition, and advertising technology (AdTech) intersect in complex ways, shaped by evolving regulations, technological advancements, and shifting consumer expectations. Businesses and policymakers face pivotal questions about achieving regulatory coherence and maintaining trust while fostering innovation in a highly competitive and data-driven market.

This session will examine strategies for leveraging first-party data, contextual advertising, and consent-based models. It will also explore the implications of regulatory frameworks like the DMA, DSA, GDPR, and the ePrivacy Directive on business models, advertising practices, and consumer trust. Additionally, this discussion will address critical issues surrounding the interplay of privacy and competition, drawing insights from real-world examples, recent decisions on the "pay-or-consent" model, and lessons learned from implementing GDPR and DMA provisions.

Representative, Apple (confirmed - name of speaker tbc)

12:45 – 13:45 Lunch

13:45 – 14:00 Keynote Speech
Michael McGrath, Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, European Commission **(confirmed)**

14:00 – 15:20 Panel 3: Aligning Data Privacy and AI Governance

AI technologies are now rapidly deployed across the public and private sectors, ushering in new opportunities for transformative innovation. Since data is at the heart of AI – with large amounts of (sometimes personal and sensitive) diverse data required to train AI models - these advancements also bring challenges around privacy, the protection and fundamental rights and adherence to various regulatory frameworks.

This panel will explore how AI innovation can co-exist with robust privacy standards, ensuring compliance and trust in AI-driven systems. It will examine the intricate relationship between AI and data privacy, including the interaction, and overlap, between AI governance and privacy frameworks like GDPR and the EU AI Act. It will also address the recent EDPB's opinion on the use of personal data in AI model training and its implications. Speakers will discuss how public and private organisations can be empowered to innovate responsibly and uphold data protection rights by embedding privacy into

AI systems, as well as the need for a collaborative regulatory and enforcement environment. This session will further consider how AI technologies themselves can support privacy practices and improve data protection compliance.

Possible questions include:

- How do the GDPR and EU AI Act intersect, and what opportunities and challenges does this bring to organizations and individuals?
- What lessons can the privacy and AI communities learn from each other to create synergistic frameworks that include key concepts such as fairness, transparency and explainability?
- How can privacy principles be systematically integrated into the entire AI lifecycle, from development to deployment? What should a robust risk management approach to AI system lifecycle phases look like to successfully address privacy, security and bias? What practical measures can mitigate AI bias, and how can transparency and accountability be ensured around the use of input and output data?
- How can organizations strike the balance between collecting diverse, high-quality datasets—sometimes involving sensitive data—and adhering to GDPR's strict data minimisation requirements? What are the key considerations around the legal basis for the use of publicly available data, the purpose limitation and right-to-be-forgotten principles, and data retention in the context of AI? To what extent does the EDPB's recent opinion go far enough to address this? How can organizations ensure transparency and facilitate the exercise of data subject rights—including access, rectification, and erasure—in AI-driven data processing systems?
- What role will collaboration between MSAs, DPAs, other authorities with AI-related competencies and the EU AI Office play in fostering innovation while enforcing compliance?
- How can DPOs adapt to the challenges posed by AI, and what specific Michaelskills and knowledge are required to effectively oversee AI-related data protection?
- How can AI technology be used to protect personal data and ensure compliance with privacy rules?
- What measures can be taken to empower users in understanding and asserting their rights regarding AI-driven data processing under the GDPR and AI Act?

Yordanka Ivanova, Head of Sector, Legal Oversight of the AI Act Implementation, AI Regulation and Compliance, EU AI Office, DG CNECT, European Commission **(confirmed)**
Michael McNamara, Member, European Parliament **(confirmed)**
Juraj Čorba, Co-Chair of The Global Partnership on AI and acting Chair of OECD Working Party on Governance of AI (AIGO OECD) **(confirmed)**
Nicolas de Bouville, Privacy Policy Manager, Meta **(confirmed)**
Representative, Mastercard **(provisionally confirmed)**

Moderated by: Natascha Gerlach, Director of Privacy Policy, CIPL (tbc)

15:20 – 15:40 Coffee Break

15:40 – 16:45 Panel 4: The Role of Technology in Fostering the Power of Personal Data: Privacy, Trust, and Innovation

In today's data-driven world, unlocking the full potential of personal data for innovation, research, and societal benefit depends on striking a delicate balance: enabling data utility while preserving privacy and building public trust. How can technology be part of the solution? How do privacy-preserving data sharing mechanisms work?

This session will focus on the power of personal data in the delivery of data-enabled innovation for the interest of society as a whole and the challenges involved. It will discuss what is required at regulatory and technological levels so that effective, privacy-preserving, and trustworthy data-sharing mechanisms can be put in place to maximise the social and economic benefits of data. Speakers will explore the potential of PETs and PPTs - including tools such as synthetic data, federated learning, confidential computing and homomorphic encryption - to complement robust data privacy management programmes and drive positive change around the collection, processing, analysis, and sharing of data by safeguarding data confidentiality and privacy, and ultimately fostering equitable participation in the digital economy and fuelling economic growth

Possible questions include:

- How can public confidence be built and citizens more empowered to access and share their data, especially in sensitive sectors like healthcare, finance and education? How do provisions included in the EU Data Act address this? What can be learnt from the Data Spaces that have been created at EU level? What role can data intermediaries play in governing the use of personal data, and how can they provide individuals with centralized control over their data sharing while ensuring regulatory compliance? What will be needed in the upcoming European Data Union Strategy to further promote responsible personal data sharing and access?
- From differential privacy, K-anonymisation, Fully Homomorphic encryption, zero-knowledge proof, decoupling, federated learning and multiparty computation, what capabilities do PETs offer? How can they uphold equity, transparency, and accountability in data use? How are privacy-preserving techniques complementing each other?
- How can synthetic data be leveraged to drive innovation while mitigating privacy concerns? What are the ethical considerations and regulatory implications of using synthetic data?

- What are the practical challenges and limitations of implementing PETs? What strategies can be used to overcome obstacles to the adoption of PETs and data-sharing frameworks? What can policymakers and regulators do to incentivise innovation and accelerate the adoption of PETs?
- What steps are needed to establish global standards for PETs to ensure interoperability across jurisdictions?

Raluca Stefanuc, Deputy Head of Unit, Cybersecurity and Digital Privacy Policy, DG CONNECT, European Commission **(confirmed)**
Maria Rautavirta, Head of Data Policy, Ministry of Transport and Communications, Finland **(confirmed)**
Michel Combot, Director of Technology and Innovation, CNIL **(confirmed)**
Monica Suarez, Data Governance & Protection Counsel, ING Belgium (tbc)

Moderated by: Resham Kotecha, Global Head of Policy, Open Data Institute (tbc)

16:45 – 18:00 Panel 5: Bridging Borders: Towards the Interoperability and Convergence of Data Privacy Rules Worldwide?

In today's data-driven world, cross-border data flows underpin international trade, economic growth, innovation, and societal progress. However, aligning diverse privacy frameworks, addressing data sovereignty concerns, and navigating the complexities of data transfer requirements—while also responding to the demands of emerging technologies such as AI—pose significant challenges for policymakers, businesses, and individuals alike.

This session will examine the evolving international efforts to strengthen global data protection and streamline data transfer mechanisms. Topics will include the EU's expanding web of adequacy decisions, updates to standard contractual clauses (SCCs), and global initiatives such as those under the Data Free Flow with Trust (DFFT) initiative or frameworks like the Cross-Border Privacy Rules (CBPR). The discussion will explore how interoperability and regulatory convergence can be advanced to protect privacy, foster trust, and support economic growth while safeguarding individuals' rights. It will also examine how policymakers and regulators can work together to reconcile data sovereignty with seamless global data flows.

Possible questions include:

- What are the key barriers to achieving global interoperability or convergence in data protection and privacy frameworks, and how can these be addressed?

- What has been achieved through initiatives such as DG JUSTICE's "Enhanced Data Protection and Data Flows" programme or the EU-US Data Privacy Framework (DPF)?
- What steps can be taken to improve adequacy decisions and promote the standardisation or mutual recognition of SCCs? Could the development of "Global SCCs" offer a scalable solution?
- What role can international initiatives, such as the DFFT, play in promoting regulatory convergence? What actions are needed to operationalise the principles outlined in such frameworks?
- What challenges do international cooperation on data privacy and interoperability face in the context of the AI boom, considering the need for diverse and representative data sets for AI training? How can these challenges be addressed?
- How can cross-border data transfer solutions be made more accessible and cost-effective for start-ups and SMEs?
- How can enforcement cooperation between Data Protection Authorities (DPAs) across jurisdictions be strengthened to address global privacy challenges?
- How can trust and confidence in cross-border data flows be bolstered, particularly amidst geopolitical tensions and shifting regulatory landscapes?

16:45 – 17:15 Part 1: International Perspective - Speeches

Irena Moozova, Deputy Director-General, DG Justice, European Commission (tbc)

Katherine M. Harman-Stokes, Acting Director, Office of Privacy and Civil Liberties, United States Department of Justice (tbc)

17:15 – 18:00 Part 2: Reactions and discussion

Birgit Sippel, Member, European Parliament (tbc)

Irena Moozova, Deputy Director-General, DG Justice, European Commission (tbc)

Monika Tomczak-Górlikowska, Group Head of Privacy, Digital & Regulatory, Prosus **(confirmed)**

Marco Moragón, Senior Public Policy Manager, Workday **(confirmed)**

Chris Taylor, Director Regulatory Strategy – International, Information Commissioner's Office (ICO) **(confirmed)**

Moderated by: Bianca-Ioana Marcu, Deputy Director for Global Privacy, Future of Privacy Forum **(confirmed)**