ForumEurope

MARCH 2026 / BRUSSELS / CONFERENCE REPORT

THE 15TH ANNUAL

European Data Protection & Privacy Conference

IN THIS ISSUE

17 March 2026 · Brussels · forum-europe.com

Policy Pulse

SIGNALS FROM THE 15TH EUROPEAN DATA PROTECTION & PRIVACY CONFERENCE

GDPR reform is targeted, not transformative

The Commission positioned its Digital Omnibus Package as simplification within existing principles, not deregulation. The EDPB and Parliament indicated they would resist any weakening of accountability or data subject rights.

The personal data definition remains contested

The proposed narrowing of what constitutes personal data through subjective reasonableness tests drew sharp opposition from consumer groups and some regulators, who warned it could hollow out protections while providing limited legal certainty.

Cross-border enforcement is accelerating

The GDPR Procedural Regulation's binding deadlines and harmonised admissibility standards were broadly welcomed. DPA representatives signalled readiness to operationalise the new framework.

AI legitimate interest faces a trust deficit

The proposal to recognise AI model training as a legitimate interest attracted support from industry but provoked concern from civil society and some MEPs about the absence of adequate safeguards for sensitive data processing.

Adequacy decisions are building a global network

With 18 adequacy decisions now in place, including mutual recognition with Brazil and South Korea, the Commission is constructing an adequacy network that may shift international data governance from bilateral to multilateral models.

Consent fatigue remains unresolved

Automated browser signals and one-click refusal mechanisms were proposed as solutions, but opinion was divided on whether simplification would genuinely empower users or merely obscure complex data processing.

Digital public services are maturing around trust-by-design

Estonia and Madrid demonstrated that privacy-by-design and interoperability-by-design, embedded from the outset, can deliver both convenience and citizen confidence at scale.

AI Act–EU data protection law guidance is imminent but untested

The European Commission confirmed joint guidelines with the EDPB are months away from public consultation, but their practical impact on dual compliance obligations remains an open question.

Momentum / consensus

Watch / emerging tension

SESSION ONE

Simplification Without Surrender: The Omnibus Debate

01

> *"Data protection and competitiveness are two sides of the one coin."*
>
> MICHAEL MCGRATH, EUROPEAN COMMISSIONER FOR DEMOCRACY, JUSTICE, THE RULE OF LAW AND CONSUMER PROTECTION

The conference's central tension was whether Europe can streamline its data protection framework without diluting the rights it was built to protect. This question animated every session and found expression across multiple debates, each revealing different facets of the broader concern that modernisation might inadvertently become deregulation.

Paul Adamson, Chairman of Forum Europe, opened proceedings by framing the day's central question: how Europe's data protection framework could evolve to maintain trust, support technological progress, and ensure coherent governance in a data-driven economy. Adamson moderated the keynote session that followed, in which three political figures set the terms of the debate. **Michael McGrath**, the European Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, opened the conference by positioning the Digital Omnibus Package as a recalibration of the GDPR rather than a retreat from its ambitions. The Commission, he argued, has designed the package to reduce unnecessary burdens while preserving the regulation's core principles and requirements and risk-based approach. The goal is not to rewrite the GDPR wholesale but to codify a decade's worth of case law from the Court of Justice and guidance from the European Data Protection Board, thereby reducing the legal uncertainty that businesses face.

This position found substantial backing from **Minister Jim O'Callaghan TD**, who spoke from the perspective of Ireland's assumption of the Council presidency in the second half of 2026. Ireland, he signalled, was committed to advancing the Omnibus package while maintaining the fundamental rights that underpin European data protection law. With Ireland taking the presidency at a critical juncture in the co-legislative process, his remarks amounted to a statement that a major member state intended to place the digital legislative agenda at the centre of its presidency, but only on the condition that the essence of the GDPR remained intact.

Vice-Minister of Justice Martynas Dobrovolskis, speaking on behalf of Lithuania as the incoming H1 2027 presidency, outlined a broadly similar position. Lithuania's priorities, he explained, would centre on advancing digital competitiveness, but always within a framework of rule of law and fundamental rights.

The sequencing was important: competitiveness is not the goal that would override rights protection, but rather an objective to be pursued in parallel, with rights as the non-negotiable baseline.

The Commission's defence of its proposals fell to **Karolina Mojzesowicz** of DG JUSTICE, who, as part of the first panel discussion, offered detailed explanations of two particularly contested proposals. On the personal data definition, she maintained that the Commission's suggested refinements simply codified existing Court of Justice jurisprudence around the concept of reasonableness and the practical identifiability test. The GDPR's definition had always been understood to exclude data that could not reasonably be linked to a person; the Omnibus merely makes this explicit. On the AI-related provisions, particularly the proposed legitimate interest basis for AI model training and the incidental-processing exemption for sensitive data, she argued these too reflected existing case law and did not represent a new favour toward artificial intelligence systems.

> *"Simplification must not compromise the consistency mechanism or the independence of national DPAs."*
>
> ZDRAVKO VUKIĆ, DEPUTY CHAIR, EUROPEAN DATA PROTECTION BOARD

The European Data Protection Board, speaking through its Deputy Chair **Zdravko Vukić**, accepted the broad direction of travel but issued a carefully calibrated warning. Simplification is necessary and appropriate, Vukić cautioned, but it must not be allowed to compromise either the consistency mechanism through which the EDPB ensures harmonised interpretation across member states, or the organisational independence of national data protection authorities. Any legislative change that weakened these safeguards would undermine the very consistency that modernisation was intended to serve.

Marina Kaljurand MEP, a Member of the European Parliament from the S&D group and co-rapporteur for the Omnibus from the LIBE committee, offered a candid assessment of the legislative terrain. The Parliament's internal working methods were still being established — two co-rapporteurs from different committees, two opinion-giving committees, and a complex shadow structure that made consensus-building unusually difficult. Speaking in a personal capacity, Kaljurand expressed growing concern that the proposed changes to the personal data definition are not, in fact, clarifying. Placing controllers in a subjective role — where they must assess identifiability based on their own means and knowledge — introduced more confusion, not less. She noted that many member states in the Council share this view and did not exclude the possibility that the Council would propose deleting the Commission's definition changes entirely. More broadly, she urged the co-legislators to focus the Omnibus on areas where simplification was genuinely needed — eIDAS, the ePrivacy framework, operational resilience — rather than reopening the GDPR's foundational provisions through what was supposed to be a fast-track process.

Jörn Wittmann, Group Privacy Ambassador at Volkswagen Group, brought the perspective of a major industrial manufacturer operating under long development cycles and thin profit margins. He expressed frustration that the Commission's original proposals — which he considered well-targeted and proportionate — were being progressively stripped back in the legislative process. From the automotive sector's standpoint, the implementing act power proposed under Article 41a is critical: product development cycles of three to five years meant that regulatory clarity needed to come in advance, not through retrospective court decisions that could render products unprofitable after launch. Wittmann also pressed the case for addressing Article 9 limitations on processing special categories of data, and for resolving the outdated ePrivacy framework, which he described as a genuine bottleneck for technology development in the public interest.

Lorelien Hoet, Director of EU Government Affairs at Microsoft, argued that legal clarity around the definition of personal data was essential for industry. The question of when pseudonymised data became anonymous was not merely academic — it determines the scope of regulatory obligations for every controller. Hoet emphasised that the Court of Justice's SRB ruling had confirmed that identifiability is not absolute, and called for practical, non-academic guidance that would allow companies to determine with confidence whether their processing activities fell within or outside GDPR scope. She also addressed the AI-related provisions, arguing that the legitimate interest basis for AI training was a proportionate recognition of how innovation actually worked, provided existing GDPR safeguards — including data protection impact assessments and the right to object — remained fully in place.

Itxaso Domínguez de Olazábal, Policy Advisor at the European Digital Rights organisation (EDRi), pushed back on the proposed narrowing of the personal data definition. The Commission's reliance on a subjective reasonableness test, she argued, risked excluding from GDPR protection categories of data that in practice remained linkable to identifiable individuals. The effect would be to shrink the regulation's scope precisely where civil society groups had been working to extend it, and to do so under the guise of clarification. She cautioned that framing the change as mere codification of SRB-line case law understated the substantive consequences for data subjects, particularly in contexts — AI training datasets, behavioural advertising pipelines — where re-identification risk was demonstrably high.

On ePrivacy, Domínguez de Olazábal defended the directive's continued relevance and argued that automated, machine-readable signals expressed through browsers and devices were a necessary complement to the GDPR rather than a threat to it. Far from being gatekeeper-enabling, such privacy signals offered users a genuine means of exercising their rights at scale, provided they were implemented in ways that reflected user intent rather than platform preference. Abandoning ePrivacy, or allowing it to be absorbed into a weaker horizontal framework, would remove one of the few remaining mechanisms through which individuals could exercise meaningful control over the processing of their data.

A question from the floor, posed by a representative of the City of London Corporation, brought the debate to ground level by asking about the practical implications of the proposed changes for financial services compliance. The response, drawing on points made by Mojzesowicz, was that the Omnibus was designed to clarify, not contradict, existing obligations — but the questioner's persistence suggested that the City's constituency remained unconvinced that simplification at the EU level would translate into reduced complexity in the supply chain. **Sara Brandstätter**, Data Privacy and Security Reporter at MLex, moderated the opening panel, steering the discussion between those who saw the Omnibus as necessary pragmatism and those who regarded it as a Trojan horse for deregulation.

SESSION TWO

02 Placing Individuals at the Centre: Consent, Dark Patterns, and the Digital Fairness Agenda

Alongside the Omnibus debate, a second, equally important conversation emerged on digital fairness and the mechanisms through which individuals exercise meaningful control over their personal data. This conversation moved beyond the regulatory architecture of the GDPR to address the behavioural and design practices that erode consent into a formality.

Anne Debet, Vice-President of France's CNIL and a member of the European Data Protection Board, welcomed the ePrivacy provisions within the Omnibus, particularly the clarifications around cookie consent and the simplified disclosure rules. However, she cautioned that the dual-authority structure — with data protection authorities and telecom regulators both having jurisdiction — created practical enforcement challenges. A processor might find itself defending the same activity against both a GDPR investigation and an ePrivacy investigation, with different legal standards applying. Harmonising this landscape remains an unfinished task.

> *"Centralised browser consent creates new gatekeepers and undermines direct user–service relationships."*
>
> VICTORIA DE POSSON, SECRETARY GENERAL, EUROPEAN TECH ALLIANCE (EUTA)

Sachiko Scheuing, Chairwoman of FEDMA (the Federation of European Data and Marketing), approached the consent question from the business perspective. She argued for proportionate transparency obligations that would allow organisations of different sizes and sectors to comply meaningfully. The risk, in her view, was that prescriptive requirements designed for large platforms would prove technically unfeasible or economically irrational for smaller operators, leading to either non-compliance or compliance through form-filling that satisfied legal obligations without communicating anything useful to consumers.

Victoria de Posson, Secretary General of the European Tech Alliance (EUTA), pressed the innovation-friendly case, arguing that consent mechanisms themselves could be modernised using new technologies. She warned that automated browser signals and one-click refusal mechanisms risk consolidating the market position of incumbents — ultimately limiting consumer choice in Europe. The goal, she argued, should be to fix consent fatigue through a risk-based approach that reduces unnecessary requests, rather than introducing new technical intermediaries.

> *"Opening multiple legislative instruments simultaneously risks creating a Pandora's box."*
>
> ALEX AGIUS SALIBA, MEMBER OF THE EUROPEAN PARLIAMENT, S&D GROUP

Cláudio Teixeira, Head of Digital Policy at the European Consumer Organisation (BEUC), delivered the sharpest critique of the simplification agenda. BEUC, he noted, represented 44 consumer organisations across 31 countries, and from their vantage point the proposals amounted to deep-cutting deregulation rather than genuine simplification. Teixeira cited survey data showing that 60 per cent of consumers considered personalisation based on their data to be unfair and only 16 per cent considered it fair, while a 2024 survey conducted for the digital fairness fitness check found 74 per cent believed businesses were misusing their personal data to personalise commercial offers. On the personal data definition, he argued that the Commission's reliance on the SRB judgment was "an extremely subjective and restrictive way of viewing personal data," noting that both the EDPS and the EDPB have said the Commission had misrepresented the decision itself. Combined with the proposed AI legitimate interest basis and the possibility of processing sensitive categories of data, an exceptional volume of consumer data would be opened to processing that was previously protected. When set alongside the AI Omnibus, which was proceeding on a faster track, the cumulative rollback of consumer protections, should it all come to fruition, would be "extremely extensive."

Alex Agius Saliba MEP, a Member of the European Parliament from the S&D group, sounded a note of procedural alarm. Opening multiple legislative instruments simultaneously — the Omnibus, the AI Omnibus, the Digital Fairness Act framework, the consumer protection regulation — risk creating a Pandora's box from which unintended consequences could scatter. The current Parliament, he suggested, is more fractious than its predecessors, which meant that negotiating a complex, multi-layered digital legislative agenda demands more skill and political capital than recent co-legislative exercises.

Karolina Mojzesowicz returned to defend the ePrivacy consolidation in the Omnibus. The Commission, she noted, had sought to remove redundancy: where GDPR and ePrivacy rules addressed the same activity, harmonising them is a logical step. The result would be fewer, but no less protective, obligations. **Lara Natale**, Senior Director of Public Affairs at the Centre for Future Generations, moderated this session, maintaining pressure on the panel to move beyond abstractions and into the practical consequences for consumers and businesses.

SESSION THREE

03 Breaking Regulatory Silos: Competition Meets Data Protection

As markets become increasingly digital, data protection and competition law have begun to overlap and sometimes to pull in different directions. A fireside chat moderated by **Matthew Newman**, Global Chief Correspondent at MLex, brought together **Michael König** from DG Competition, **Siún O'Keeffe** from the Dutch Data Protection Authority, and **Maria Goikoetxea** from ACT | The App Association to explore how these two regimes could coexist without creating impossible compliance burdens or perverse incentives.

König outlined the Digital Markets Act's three principal data-related obligations, each with its own architecture. The first, conflict of interest prevention, requires designated gatekeepers not to use data in competition with business users on their platform. The second, data sharing with business users, obligates gatekeepers to grant SMEs and other ecosystem participants access to data necessary for them to compete. The third, ecosystem advantage prevention, targets the use of data obtained from one context to gain unfair advantage in another. Critically, König emphasised, the DMA does not mandate gatekeepers to collect more data. It obliges them to share what they already hold, and it does so within a framework of safeguards: user consent, authentication, encryption, and periodic reporting.

> *"Competitiveness is not a human right."*
>
> SIÚN O'KEEFFE, ACTING HEAD OF STRATEGY, DUTCH DATA PROTECTION AUTHORITY

Siún O'Keeffe, Acting Head of Strategy at the Dutch Data Protection Authority, challenged the tendency to treat competitiveness as a right on par with data protection: competitiveness, she cautioned, is not a human right. On the specific question of consent under Article 5(2) of the DMA, O'Keeffe argued that the provision's rigour reflected existing GDPR principles rather than creating a "GDPR plus." The DMA's requirement that gatekeepers obtain consent for cross-service data combination was a response to markets where users had no meaningful choice — the very conditions the DMA was designed to address. On data portability, O'Keeffe warned that the right must not be misused as a mechanism for bulk data extraction divorced from individual choice. She also pointed to the practical necessity of granular cooperation between competition and data protection authorities, citing the protocols between the Netherlands' ACM and its data protection authority as a model.

Maria Goikoetxea from ACT | The App Association brought the perspective of startups and smaller technology firms. These companies, she argued, differ fundamentally from established brands: they lack consumer recognition, operate with minimal teams, and build privacy into their products from the outset out of necessity, not just principle. On the question of legal basis, her members favoured just-in-time consent — obtaining permission at the precise moment of data use — because it gave end users the context to understand what their information would be used for and why. Goikoetxea maintained that companies should compete on privacy, and that the regulatory framework should reward those that develop privacy-enhancing technologies and features. At the same time, she cautioned against naivete about the risks of interoperability: when new parties gained access to data that gatekeepers previously held exclusively, the privacy implications could be significant.

König acknowledged that coordination mechanisms between DG Competition and national data protection authorities existed and were improving, but distinguished between the high-level group's role in policy coordination and the direct bilateral cooperation required on individual cases. The Meta case, in which competition and data protection concerns were both at issue, served as a worked example of how jurisdiction could be divided and coordination achieved. Companies can support the coordination process by sharing the same level of information with all regulators concerned so that all authorities can consider the same facts. All three panellists converged on a practical conclusion: the DMA and GDPR can be reconciled, but only through sustained, granular engagement between regulators at every level, and solutions that work on the ground rather than only in legislative text.

The session underscored a broader truth about the current regulatory moment: as data becomes the common currency of both competition and privacy enforcement, the institutional architecture must evolve to match. The protocols between the Dutch ACM and its data protection authority offer a working model, but scaling that cooperation across twenty-seven member states and multiple EU-level bodies remains a formidable challenge. What emerged most clearly was that neither regime can afford to operate in isolation. Competition authorities that ignore privacy risk enabling market structures built on surveillance, while data protection authorities that ignore market dynamics risk entrenching the dominance of incumbents who can absorb compliance costs that smaller rivals cannot. The path forward, as all three speakers acknowledged, lies in structured, case-level cooperation that treats regulatory overlap not as a jurisdictional problem but as an opportunity for more complete enforcement.

SESSION FOUR

04 Building Bridges in a Fragmented Regulatory Landscape

The international dimension of data protection governance has grown steadily more complex as jurisdictions multiply their regulatory ambitions. A dedicated panel examined how the EU might construct a coherent approach to international data flows while respecting the sovereignty of trading partners and maintaining the security of sensitive data.

> *"The challenge is not flowing data but materialising trust."*
>
> MAIKO MEGURO, LEAD COORDINATOR ON DATA-FREE FLOW OF TRUSTED DATA, OECD

Louisa Klingvall from DG JUSTICE's International Affairs unit provided a comprehensive overview of the adequacy framework's expansion. As of March 2026, eighteen adequacy decisions were in place, covering populations that spanned from the UK to Japan, from South Korea to Brazil. Two of these were particularly significant as mutual recognitions: the EU–Brazil mutual adequacy, negotiated over three years and adopted in January 2026, and the EU–South Korea reciprocal framework, which represent a shift from unilateral EU decision-making to a more negotiated, bilateral form of recognition. These mutual arrangements, Klingvall suggested, signalled a transition in international data governance from bilateral deals to the beginnings of a multilateral adequacy network.

Klingvall also noted that work was proceeding on new Standard Contractual Clauses to cover transfer scenarios not contemplated when the current clauses were approved. The regulatory uncertainty that had followed the Schrems II judgment — which invalidated the Privacy Shield and raised questions about the sufficiency of SCCs without supplementary safeguards — is gradually being addressed through a combination of improved clauses and country-specific adequacy decisions.

Yoon Jeong Choi, Head of the International Cooperation Division at South Korea's Personal Information Protection Commission (PIPC), highlighted Korea's efforts to facilitate secure cross-border data flows. She noted that the 2023 amendment to Korea's privacy law introduced new transfer mechanisms, including equivalency recognition, enabling mutual recognition with the EU in 2025 and reducing compliance burdens. While CBPR is not recognized as a legal basis for data transfers, she emphasized its value in promoting higher regional standards. She also noted that expanding mechanisms such as the EU–US Data Privacy Framework globally should be reviewed. She underscored the importance of interoperable data protection in the AI era and plans to expand mutual recognition frameworks and strengthen global cooperation.

Eduardo Gomes Salgado, General Coordinator of Brazil's ANPD, walked the conference through the negotiation of Brazil's mutual adequacy with the EU. Three years of work had gone into the arrangement, reflecting the complexity of reconciling different constitutional traditions and legal frameworks. The agreement, he emphasised, was predicated on the principle of interoperability — accepting that Brazil's data protection rules were not identical to the EU's, but sufficiently aligned that transfers could proceed safely. Salgado also noted that the ANPD was in discussions with the UK Information Commissioner's Office about a potential similar arrangement, suggesting that bilateral adequacy negotiations were becoming a standard feature of post-GDPR international relations.

> *"Comply once, comply many."*
>
> JOHN KAVANAGH, PUBLIC POLICY, TIKTOK EUROPE

Maiko Meguro, Lead Coordinator on Data-Free Flow of Trusted Data (DFFT) at the OECD, offered a multilateral perspective. The challenge of international data governance, she contended, was not flowing data but materialising trust. The question was not 'can data move?' but 'can organisations in one jurisdiction trust organisations in another to handle data according to acceptable standards?' Multilateral dialogue hosted by neutral organisations like the OECD was more likely to build that trust by ensuring that no single regional tradition set the terms of discussion, grounded in evidence rather than in any particular regulatory practice as a reference point.

John Kavanagh, representing TikTok's public policy function in Europe, introduced the concept of 'comply once, comply many' — the idea that a company certified for compliance in one jurisdiction should be able to benefit from at least some starting recognition when carrying that certification into other jurisdictions. He described Project Clover, an initiative representing €12 billion of investment in data localisation and infrastructure for European users, as a practical response to the regulatory fragmentation created by divergent national requirements. Kavanagh called for an ambitious international transfer strategy, developed alongside the Digital Omnibus, to reduce the compliance burden that fragmentation created. He also advocated for privacy-enhancing technologies and demonstrated accountability as mechanisms through which compliance could be shown without requiring data to be physically located in specific territories.

Gabriela Mercuri, Managing Director of SCOPE Europe, raised the underutilisation of codes of conduct and certification mechanisms under Articles 40–41 of the GDPR. These instruments, she argued, were well-designed but rarely used, because the process for developing and approving them was slow and required DPA engagement at different levels across member states. If certification and codes of conduct could be streamlined, they might become meaningful tools for facilitating international transfers and demonstrating compliance without requiring transaction-specific assessments.

Natascha Gerlach, Director of Privacy & Data Policy at the Centre for Information Policy Leadership (CIPL), moderated this panel and drew out the tension between the Commission's stated goal of building a global adequacy network and the practical reality that each new jurisdiction demanded a fresh assessment. The process of establishing adequacy is iterative and painstaking; the result is a patchwork that served some trade routes well and left others in uncertainty.

SESSION FIVE

Sovereignty, Security, and the Digital Transformation of Public Services

05

Moving from commerce to citizenship, a panel on digital public services explored how governments could deliver citizen-facing digital services while maintaining data security and respecting privacy throughout the process. The emphasis fell on the concept of trust-by-design — the principle that privacy and security must be embedded from the outset, not retrofitted.

> *"There is no absolute sovereignty."*
>
> ILIAS CHANTZOS, GLOBAL PRIVACY OFFICER AND HEAD OF EMEA GOVERNMENT AFFAIRS, BROADCOM

Cristina Cosma from DG DIGIT outlined the Commission's framework for sovereign digital infrastructure. The EU Digital Identity Wallet, expected to roll out by November 2026, is designed to allow citizens to share only the minimum attributes necessary to prove their identity or transact with government and private service providers. The architecture embodies the principle that interoperability does not require data minimisation to be sacrificed; on the contrary, it demanded it. The European Digital Infrastructure Consortium, launched in Greece the previous week, represents a practical instantiation of the Commission's commitment to building critical digital capabilities within the EU.

Fernando de Pablo Martín, Director General of the Digital Office of the City of Madrid, brought a municipal perspective. Madrid's digital services reach 3.5 million residents, with 83 per cent digital service uptake — among the highest in the EU. He reported that Madrid had quadrupled its cybersecurity investment over four years, a reflection of the escalating threat landscape and the critical role that digital public services now played. Notably, de Pablo Martín spoke of 'autonomy' rather than 'sovereignty' — a deliberate choice of language suggesting that the goal was not for Madrid to be isolated or self-sufficient in digital systems, but rather to have meaningful agency and control within an interconnected environment.

Pille Lehis, Director General of the Estonian Data Protection Inspectorate, presented Estonia's quarter-century journey toward a fully digitised state. The X-Road system, Estonia's backbone for government digital services, operates on a principle of distributed databases — no central repository exists, but all systems are linked through encrypted, authenticated connections. Every database has to have a documented legal basis; citizens have the right to access logs showing who queried data about them. This architecture, Lehis suggested, has enabled Estonia to deliver convenience and citizen confidence at scale.

Ilias Chantzos, Global Privacy Officer and Head of EMEA Government Affairs at Broadcom, offered a technology industry perspective. There is no absolute sovereignty, he argued, because global supply chains mean that digital systems inevitably depend on components and services from other jurisdictions. The practical approach is not to seek isolation but to manage risk through appropriate safeguards. He called for regulatory approaches that emphasise risk management rather than the illusion of risk avoidance, and for further simplification of compliance obligations.

Marianna Mattera, Principal Analyst at Cullen International, moderated this session, drawing out the contrast between the aspirational goal of 'European digital sovereignty' and the practical reality that digital systems are inherently globalised. The speakers' consensus seemed to be that the appropriate frame was not sovereignty but resilience and appropriate governance — systems that can be relied upon precisely because their operations are transparent, auditable, and subject to meaningful oversight.

SESSION SIX

Data, Privacy, and AI: Building Trustworthy Innovation

06

> *"AI has not created these problems; it has merely highlighted that the law and its interpretation have failed to solve them."*
>
> CECILIA ÁLVAREZ RIGAUDIAS, DIRECTOR OF DATA AND PRIVACY POLICY, META EUROPE

The final substantive panel brought together the two regulatory frameworks that will shape the digital economy of the coming decade: data protection and artificial intelligence governance. The tension between these regimes — GDPR's emphasis on individual control and AI Act's emphasis on system-level risk — demands practical reconciliation.

Joanna Jużak, Legal Officer at the AI Office in DG CNECT, provided the most detailed public preview to date of joint guidelines being developed with the EDPB on the interface between the AI Act and EU data protection law. These guidelines, she indicated, will be ready for public consultation within a matter of months. The work addresses questions that have bedevilled practitioners since the AI Act entered force: what processing activities trigger dual compliance obligations? How does the concept of legal basis under the GDPR map onto the legitimate interests and special categories handling under the AI framework? Are privacy-enhancing technologies a sufficient safeguard, or do additional organisational controls need to be in place?

She also described the regulatory sandboxes envisioned under the AI Act as a crucial mechanism for testing innovative approaches in a controlled environment before they were scaled. Sandboxes will allow companies to test federated learning architectures, retrieval-augmented generation systems, and other approaches that attempt to deliver AI capability while minimising personal data exposure.

Kari Laumann, Head of Section at the Norwegian DPA, shared the results of a recent Norwegian survey on public attitudes toward AI in different contexts. Citizens were most positive about AI in healthcare, where it promised to improve diagnosis and treatment. They were least positive about workplace monitoring and behavioural advertising. The survey also revealed a striking shift: where AI governance had previously been the concern of large technology companies, it was rapidly becoming an issue requiring guidance across all sectors. The Norwegian DPA was receiving enquiries from manufacturers, retailers, and public sector organisations, all seeking to understand their obligations.

Cecilia Álvarez Rigaudias, Director of Data and Privacy Policy for Meta Europe, addressed the concept of legitimate interest for training GenAI models. She contended that the problems now attributed to AI — the tensions around claimed processing of sensitive personal data, the questions about what constitutes personal data in the context of model training — were long-standing problems in data protection that predated the AI Act. AI has not created these problems; it has merely highlighted that the law and its interpretation have failed to solve them. She called for innovation mindsets at the regulatory level, suggesting that regulators need to think about how they can contribute to competitiveness and also how AI might enable better outcomes, including but not limited to compliance. In this regard, they should be prepared to assess and accept trade-offs. This is the case for example of privacy-enhancing technologies (PET) that inevitably involve trade-offs: they reduce the scientific value of the data, might require addressing computational dependencies and ecosystem lock-in, and require sustained investment to maintain. With these trade-offs in mind, for PETs to thrive, we cannot continue working with an absolute concept of personal data, an overemphasis on consent or a co-controllership concept divorced from the actual scope of risk control.

> *"Privacy is not a compliance checkbox but a design constraint that shapes technical choices."*
>
> NAZANIN GIFANI, DATA PROTECTION OFFICER, ALLIANZ TECHNOLOGY FRANCE AND BENELUX

Nazanin Gifani, DPO at Allianz Technology France and Benelux, offered the perspective of a large multinational organisation navigating dual compliance. Data Protection Officers, she argued, were the natural trust officers for AI systems, given their experience at the intersection of law and technology. She described privacy integration across the full AI lifecycle: from the scoping of business use cases through training data selection, model development, ongoing monitoring, and eventual decommissioning. Privacy, in this framework, is not a compliance checkbox but a design constraint that shaped technical choices. However, she noted that privacy-enhancing technologies, whilst promising, remain immature and expensive. The ecosystem of tools and techniques is still developing and they cannot always be used to entirely circumvent the obligations under the data protection law; nonetheless, when combined with other technical, organisational or contractual measures they can provide substantial opportunities for leveraging personal data.

Katherine Quezada Tavárez, Group Deputy DPO and AI Compliance Advisor at bnode, defined trustworthiness as reliance: the extent to which organisations could trust AI systems to perform reliably in critical workflows. This framing shifted the conversation from abstract principles to operational risk. She noted that enforcement actions from national DPAs — the CNIL in France, the Belgian DPA, the Spanish DPA, and the UK Information Commissioner's Office — are beginning to establish expectations about what adequate AI governance looked like in practice. These decisions are helping to shape day-to-day compliance obligations.

Axel Voss, a Member of the European Parliament, offered a perspective focused on the relationship between the GDPR and the AI Act. He called for clearer interaction rules that would remove ambiguity about which regime applied to which processing activities. Anonymised and pseudonymised data, he argued, were essential for innovation and should be definitively excluded from GDPR scope, allowing businesses to iterate without regulatory impediment. Voss pressed for a pragmatic approach: rather than layering additional obligations, the co-legislators should clarify existing ones so that companies could invest in AI development with confidence about the legal framework they were operating within.

Bianca-Ioana Marcu, Managing Director for Europe at the Future of Privacy Forum, moderated this panel. The theme that emerged was that the GDPR and AI Act, rather than pulling in opposite directions, could be understood as complementary regimes — one focused on individual agency and control, the other on system-level risk management. The challenge was practical reconciliation, which the joint guidelines would attempt to provide.

LOOKING AHEAD

What Comes Next

The conference concluded with a forward-looking session addressing the timeline and sequencing of the regulatory work ahead. Several key milestones emerged as critical.

European Commission & EDPB Joint Guidance

The joint guidance from the European Commission and EDPB on the AI Act–EU data protection law interface is expected for public consultation within months, signalling that this foundational work is nearing completion.

Ireland's Council Presidency

Ireland's assumption of the Council presidency in the second half of 2026 marks the beginning of the critical co-legislative phase for the Digital Omnibus and the broader digital legislative agenda. Lithuania's H1 2027 presidency will continue this work, with two consecutive presidencies committed to advancing digital competitiveness within the rule of law.

New Standard Contractual Clauses

New Standard Contractual Clauses from the Commission will be issued in the coming months, addressing transfer scenarios not covered by the current clauses. This work is particularly critical for SMEs and for sectors — such as research and development — that depend on international data flows.

EDPB Guidance on Anonymisation

The EDPB's updated guidance on anonymisation and pseudonymisation is pending, and will provide crucial clarity on what processing activities fall outside GDPR scope.

Codes of Conduct & Certification

Codes of conduct and certification mechanisms remain significantly underexploited tools for demonstrating compliance and facilitating international transfers; streamlining the process for their approval should be a priority.

EU Digital Identity Wallet

The EU Digital Identity Wallet rollout is scheduled for November 2026, representing a practical test of whether digital systems can deliver convenience and security in tandem.

AI Act Regulatory Sandboxes

Regulatory sandboxes under the AI Act are opening for business, providing controlled environments in which innovative compliance approaches can be tested before scaling.

The immediate challenge before the co-legislators is to convert the broad political consensus on the direction of travel — simplify the GDPR, modernise the regulatory framework for AI, address digital fairness, and build trustworthy international data governance — into legislative text that preserves fundamental rights whilst enabling innovation. That consensus is real but fragile. The question that will define European data protection policy over the next eighteen months is whether the political will to act quickly can survive the technical complexity and internal disagreement that co-legislation inevitably entails.

ForumEurope

This report was prepared by Forum Europe following the 15th Annual European Data Protection & Privacy Conference held in Brussels on 17 March 2026. Forum Europe's editorial content is produced independently of conference sponsors and speakers. The views reported herein are those expressed during the conference and do not represent the position of Forum Europe.

FORUM-EUROPE.COM