FUTURE OF PRIVACY FORUM

VUB BRUSSELS PRIVACY HUB

Brussels Privacy Symposium 2025

A Data Protection (R)evolution?

Symposium Report

Authors: Andreea Şerban, Margherita Corrado
Editor: Bianca-Ioana Marcu

December 2025

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum

In Europe, the Future of Privacy Forum (FPF) is an independent voice, maintaining neutrality in any discourse. FPF is optimistic that social and economic good can be achieved through innovation in data and technology while also respecting privacy and data protection rights. FPF has built strong partnerships across Europe through its convenings and trainings for policymakers and regulators. FPF's transatlantic engagement helps regulators, policymakers, and staff at European Union data protection authorities better understand the technologies at the forefront of data protection law.

FPF explains EU data protection and privacy law to make them easily understandable for stakeholders in the U.S. and around the world. FPF hopes to bridge the gap between European and U.S. privacy cultures and build a common data protection language.

A space for debate and dialogue: FPF is a non-profit organization providing a space for debate and dialogue by:

- Sharing knowledge of European privacy and data protection law with its members
- Connecting a network of key players from corporations, NGOs, academics, civil society, and regulators
- Engaging with EU regulatory bodies and policymakers
- Being a respected voice in the media
- Advising corporations and policymakers regarding technological, privacy and data protection issues
- Offering regular peer-to-peer gatherings, workshop, and training interventions in selected hotspots across Europe

Brussels Privacy Hub

At the Brussels Privacy Hub (BPH), we believe strongly in the relevance and importance of data protection and privacy law, particularly in light of the challenges posed by the rapid development of technology and globalization. We also believe that fresh and innovative thinking based on multidisciplinary research is necessary to meet these challenges. The BPH thus brings together scholars from a wide array of disciplines who collaborate with the private sector, policymakers, and NGOs to produce cutting-edge research. We believe in network-building and have built a strong network of contacts with leading privacy researchers both in and outside the EU. The BPH's main goals are to produce privacy research of the highest quality, bring together leading thinkers from around the world, and foster an interchange of ideas among privacy stakeholders in a climate of intellectual openness.

TABLE OF CONTENTS

Executive Summary: Key Takeaways

Opening Keynote: Reinforcing the GDPR's Role in an Evolving Digital Framework

- The GDPR remains the cornerstone of privacy and data protection across the EU.
- The Commission has proposed targeted amendments to the GDPR as part of its simplification agenda, particularly concerning reporting obligations for SMEs, and confirms that further simplification measures are being considered.
- Further simplification efforts regarding the implementation of the GDPR are being considered following stakeholder feedback from the GDPR Implementation Dialogue.
- The core principles of the GDPR will remain unchanged.
- In the Commission's view, other legislative instruments, such as the DSA, DGA, and AI Act, are not overlapping but rather complementary to the GDPR.

A Data Protection (R)evolution?

- The discussion highlighted a shift from calls to overhaul the GDPR toward improving its implementation through targeted, evidence-based adjustments and stronger cooperation between regulators.

- Two specific issues related to the GDPR and its application on the radar of the European Commission are: using legitimate interests for AI training, and the clarifications brought recently by the CJEU to pseudonymization and the definition of personal data.
- Several interventions stressed that the GDPR's enduring strength lies in its balance between clear principles and flexible application, urging that reforms refine rather than rewrite the existing framework.
- The AI Act's risk-based model was seen as creating uneven regulatory coverage and poor incentives, pointing to the need for proportionate safeguards across all AI systems.
- The global success of the GDPR as a regulatory model was explained by the fact that it was built on internationally developed principles. The new digital laws, including the AI Act, have been developed too rapidly, without the same foundation of global consensus.
- Overall, the panel agreed that the EU's data protection framework should continue evolving to meet new technological realities without eroding the core values that make it a global benchmark.

Lightning Talk: Are LLM-Based Systems Pushing Rights to the Breaking Point and Can We Govern Them?

- LLMs present distinct data security and protection risks across their lifecycle.
- Understanding data flows is essential to tracing how information moves within AI systems.
- An iterative, lifecycle-based risk management framework is needed to address AI-specific challenges.
- *Ex ante* risk assessment remains crucial, though not consistently implemented in practice.

Between a Rock (AI Act) and A Hard Place (GDPR)?

- The EDPB Opinion on AI models was praised for constructively clarifying this relationship and avoiding legal overlap or conflict.
- Harmonization remains a challenge, as national DPAs take divergent approaches, some pragmatic, others restrictive.
- Dialogue between DPAs and industry has improved, fostering more openness, mutual understanding, and early engagement on AI compliance.
- Data protection cannot be an afterthought. Compliance must precede processing, and technical impossibility is not a valid excuse for noncompliance.
- AI pushes for shifts in how classic data protection principles, like data minimization, are interpreted.
- Innovation and compliance are compatible, but pragmatic, evidence-based, and harmonized approaches are needed to balance both effectively.
- The GDPR's rights-based and the AI Act's risk-based frameworks were described as complementary, together forming the foundation for trustworthy and accountable AI governance in Europe.

Honored Guest Speaker Talk: Prof. Norman Sadeh

- AI agents are becoming more complex, requiring a deeper and broader understanding of users and access to personal data.
- Research is moving towards AGI, enabling agents to communicate across different apps and contexts.
- To reduce user burden, privacy assistants can inform people about data practices, provide support to manage data subject rights, and provide personalized recommendations based on interactions.
- Privacy preferences are complex and context-dependent. The GDPR and CCPA are useful, but they are not sufficient to manage this diversity. As such, standards, taxonomies, and protocols are necessary to ensure that privacy is respected as AI continues to develop.

Lightning Talk: Investigating Automated Decision-Making

- Methods such as blind review reduce bias, while empirical tests measure whether humans independently assess algorithmic outputs.
- Effective oversight depends on giving reviewers the time, information, and authority to make real decisions.

Data Protection Authorities in the Spotlight: Pathways for Harmonization

- DPAs are becoming central to AI governance, ensuring the GDPR guides responsible AI development while shaping harmonization under the AI Act.
- The CNIL's guidance confirmed that purpose limitation and data minimization can apply effectively to AI training, reinforcing trust and responsible innovation.
- The Dutch and Italian DPAs foresee a continued, central role for DPAs in AI oversight, emphasizing cross-authority cooperation and consistency across the EU's digital framework.

Closing Reflections: In Dialogue Wojciech Wiewiorowski and Gianclaudio Malgieri

- Each crisis tests the principles of necessity and proportionality, requiring a balance between State and individual rights.
- Any simplification of the GDPR should not compromise fundamental rights, and core principles should remain untouched.
- There are still weaknesses, including uneven enforcement, slow development of codes of conduct, and procedural differences across Member States.
- GDPR and generative AI do not conflict, but there is just a continued need for balance and coherent judicial interpretation.
- The DFA has a promising consumer-oriented approach, but the fairness concept is unclear and varies across languages.

1. Introduction

The ninth edition of the Brussels Privacy Symposium, jointly co-organized by the Future of Privacy Forum and the Brussels Privacy Hub of the Vrije Universiteit Brussel (VUB), took place on Tuesday 14 October 2025 at Les Ateliers des Tanneurs. The Symposium is a multidisciplinary, global convening bringing with it an opportunity to discuss some of the most pressing issues for Europe's digital society today and in the years to come. This year's panels, talks, and workshop sessions were united by an overarching theme, asking the question: are we seeing **"A Data Protection (R)evolution?"**

The programming of the Symposium has drawn attention over the past two editions to the complexity, overlap and often incongruence of the various new European Union (EU) legislative acts in the digital realm, on top of the General Data Protection Regulation (GDPR). This complexity is now at the heart of an effort by the European Commission, with support from the EU Council, to simplify the digital regulation acquis. At the same time, **the push for competitiveness in the age of AI and the unpredictable geopolitical landscape might lead to a full data protection (r)evolution, with increased appetite to reopen the GDPR or, at least, to clarify its interplay with the AI Act.** These were the pressing questions and debates at the heart of this year's program.

The Symposium opened with a keynote by Ana Gallego, Director-General of DG JUST at the European Commission, who reiterated that the GDPR remains the cornerstone for privacy and data protection across the EU. During a fireside chat with Dr. Gabriela Zanfir-Fortuna, Gallego confirmed that **the Commission is considering further GDPR simplification efforts**, noting that any such changes must be evidence-based.

Alongside three expert panels throughout the day, the program of the Symposium also included two lightning talks and three breakout workshop sessions, providing plenty of opportunities for active exchange among participants. Topics covered range from addressing the privacy risks of LLMs to investigating automated decision-making systems, and from operationalizing the GDPR and AI Act's right to an explanation to addressing complex privacy preferences using agentic AI.

This report captures some of the most prominent outcomes of the day's discussions and debates, providing notes and summaries of the day's proceedings.

2. Opening Keynote: Reinforcing the GDPR's Role in an Evolving Digital Framework

In the opening of the ninth Brussels Privacy Symposium, Ana Gallego, Director-General of the European Commission's Directorate-General for Justice and Consumers, delivered a keynote reflecting on the European Commission's efforts to simplify and adapt the General Data Protection Regulation (GDPR) within the broader digital and AI regulatory framework. Her remarks focused on easing compliance for SMEs while preserving fundamental rights and consistent enforcement across the EU.

She began with the observation that the **evolution of AI and the EU digital ruleset** makes the Symposium's questions particularly timely. The Commission's competitiveness and simplification agenda is already impacting digital regulation, including data protection. The focus is on addressing evolving needs within Europe's broader digital transformation while ensuring that the **GDPR remains the cornerstone of privacy and data protection in the EU**, balancing innovation with fundamental rights.

The Commission has proposed targeted amendments to the GDPR as part of its simplification agenda and the fourth omnibus package adopted on 21 May 2025. In response to concerns raised by SMEs during stakeholder consultations, the Commission proposed to exempt companies or organizations with fewer than 750 employees from the obligation to maintain records when those processing activities do not entail a high risk to individuals' data. Gallego clarified that the proposal does not affect the obligations of data controllers and the rights of data subjects, but grants SMEs greater flexibility without jeopardizing GDPR compliance.

Further simplification efforts regarding the implementation of the GDPR are being considered following stakeholder feedback collected during the GDPR Implementation Dialogue held on 16 July, hosted by EU Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, Michael McGrath. While stakeholders generally opposed reopening the GDPR, they nevertheless suggested targeted amendments to simplify specific obligations of data controllers.

The broader EU digital framework, including the Artificial Intelligence Act (AI Act)**,** the Digital Services Act (DSA), and the Data Governance Act (DGA), complements the GDPR, though it adds to overall regulatory complexity. The European Data Protection Board (EDPB) has adopted guidelines on the interplay between the DSA and GDPR, and is working closely with the AI Office to draft guidance on the AI Act-GDPR interface to ensure consistent enforcement across the EU.

Gallego further emphasized that **any simplification must be evidence-based**, addressing practical concerns in GDPR implementation and enforcement rather than altering the Regulation itself. Initiatives such as the Helsinki Statement are particularly welcomed, as they facilitate compliance for small operators and strengthen cross-regulatory cooperation in a complex digital landscape. Gallego highlights that the Commission looks forward to the practical steps that the EDPB will take to follow up on the statement. In addition, negotiations on the Commission's proposal for GDPR procedural rules were finalized last summer during the Polish Presidency (a political agreement between the Council of the European Union and the European Parliament was reached in June 2025).

During the fireside chat with Dr. Gabriela Zanfir-Fortuna following the keynote, Gallego reiterated that **the GDPR is the cornerstone of EU privacy law and a horizontal framework for all personal data processing**. **Legislative instruments such as the AI Act, DSA, and DGA are designed to be complementary and not overlapping**, addressing gaps and clarifying rules for emerging technologies.

TAKEAWAYS

- The GDPR remains the cornerstone of privacy and data protection across the EU.
- The Commission has proposed targeted amendments to the GDPR as part of its simplification agenda, particularly concerning reporting obligations for SMEs, and confirms that further simplification measures are being considered.
- Further simplification efforts regarding the implementation of the GDPR are being considered following stakeholder feedback from the GDPR Implementation Dialogue.
- The core principles of the GDPR will remain unchanged.
- In the Commission's view, other legislative instruments, such as the DSA, DGA, and AI Act, are not overlapping but rather complementary to the GDPR.

3. A Data Protection (R)evolution?

The opening panel explored the evolving role of data protection law within the broader EU digital regulatory landscape.

As debates around competitiveness and regulatory simplification gain momentum, the discussion turned to the future of the GDPR, its continued relevance, its interaction with other digital laws, and the growing pressure to adapt to emerging technologies such as AI.

The panel featured Olivier Micol (DG JUST, European Commission), Prof. Gloria González Fuster (Vrije Universiteit Brussel), Stephan Geering (Anthology), and Itxaso Domínguez de Olazábal (EDRi), and was moderated by Bianca-Ioana Marcu (Future of Privacy Forum).

3.1. BRIDGING THE GAP BETWEEN AI INNOVATION AND REGULATION

Speaking from the perspective of a global education technology company operating in over 90 countries, Stephan Geering noted the importance of legislation that fosters trust in technology while acknowledging that not all regulations add equal value. He underlined that crafting good laws is difficult, and the focus should be on ensuring they create the right incentives and avoid unintended consequences.

Geering cautioned that the pace of legislative and supervisory processes risks falling behind the rapid development of AI. He suggested improving how impact assessments and lawmaking are conducted to match technological speed and complexity better.

Turning to the AI Act, he described the **GDPR as a success but argued that the AI Act's risk-based structure has some gaps**. The narrow scope of the prohibited categories of AI practices means most companies fall either into the high-risk tier, with very stringent obligations, or the non-high-risk category, where requirements are minimal. This binary system creates bad incentives: firms will try to avoid the high-risk classification, while lower-risk applications may remain underregulated.

Geering noted the absence of a general clause requiring all AI developers to implement appropriate technical and organizational measures proportionate to their level of risk. Without such a principle, non–high-risk systems may lack sufficient safeguards. As an example, he pointed to the emerging phenomenon of AI companion bots, which raise serious ethical and societal concerns but are not adequately addressed under the current framework.

3.2. THE EUROPEAN COMMISSION'S PATH FORWARD FOR THE GDPR

With regard to the European Commission's ongoing response to the growing debate around the GDPR's future and its interaction with the AI Act, Olivier Micol mentioned that earlier this year the GDPR faced strong criticism, with calls for a complete overhaul among claims that it was no longer fit for purpose. However, following the Commission's full evaluation of the Regulation and the launch of the GDPR Implementation Dialogue, the tone of the debate shifted significantly.

Through this dialogue, which brought together industry, civil society, and the EDPB as an observer, the Commission moved past flashy headlines toward more concrete and evidence-based discussions about what truly needs improvement. Micol emphasized that **a change of narrative has taken place, now focusing less on rewriting the GDPR and more on improving its application and implementation.** He explained that the Commission distinguishes between two types of problems, implementation and legislation, each requiring a different type of solution. The priority is to preserve the risk-based approach of the GDPR while strengthening practical compliance support.

On the implementation side, Micol highlighted several initiatives: providing clearer, more accessible guidance; engaging in proactive dialogue with stakeholders before drafting guidelines; and fostering cross-regulatory cooperation among authorities. He pointed to joint initiatives between the Commission and the EDPB, such as the joint guidelines on the DMA and upcoming work with the AI Office and DG CONNECT on the interplay between the AI Act and the GDPR. He also underlined the importance of cybersecurity and the practical benefits often overlooked in GDPR discussions, such as reduced costs from avoiding data breaches.

Addressing the Commission's simplification agenda, Micol noted that work is already underway on several fronts, including simplification of records of processing activities, the GDPR Procedural Regulation, and other initiatives currently progressing in the Council and Parliament.

He added that both civil society and industry had provided strong input during consultations. Civil society continues to play its role in defending fundamental rights and keeping pressure on the Commission, while industry feedback has been more measured. Micol concluded that **the Commission's pragmatic, targeted approach aims to ensure that the GDPR remains effective, coherent, and future-proof.**

3.3. CIVIL SOCIETY CONCERNS OVER THE SIMPLIFICATION AGENDA

Itxaso Domínguez de Olazábal expressed concerns with regard to the Commission's *simplification* or *deregulation* agenda. She noted that simplification is often presented as neutral or positive, but it risks weakening fundamental rights protections. She argued that the

Commission is lacking an overarching strategy, where each Commission DG appears to be under pressure to simplify, often without evidence-based justification or proper fundamental rights impact assessments.

Domínguez de Olazábal pointed to Article 30(5) GDPR as an example: despite plans to simplify record-keeping obligations, many companies and DPOs still need to map data processing activities, illustrating thus how simplification can be misguided when the measures proposed do not reflect on-the-ground realities.

Domínguez de Olazábal also referred to the omnibus packages, which put together amendments to multiple laws into single deals. This approach limits democratic scrutiny and pressures lawmakers to accept problematic revisions to avoid reopening broader legislative frameworks like the GDPR. Rules and safeguards should not be dismissed as bureaucratic burdens but understood as necessary tools that protect people.

Finally, Domínguez de Olazábal highlighted more constructive ways to achieve simplification, such as strengthening resources for Data Protection Authorities (DPAs), supporting SMEs and mid-caps facing disproportionate compliance burdens, and ensuring fair enforcement so that large tech companies are held equally accountable. **Simplification should serve all stakeholders without compromising the fundamental rights that form the foundation of the EU's digital framework.**

3.4. A CALL FOR RESTRAINT AND PERSPECTIVE IN THE GDPR DEBATE

Prof. Gloria González Fuster (Vrije Universiteit Brussel) reflected on the pressure to amend the GDPR, offering an analogy to Michelangelo's David. She suggested that, like the sculptor making only cosmetic adjustments to appease critics, perhaps the **EU should pretend to change the GDPR without altering its core, preserving thus a framework that has taken time to build and continues to serve as a cornerstone of rights protection.**

González Fuster cautioned against unnecessary reforms made merely to satisfy political pressure, arguing that the GDPR works and embodies values fought for over half a century. In her view, it would be a mistake to "break the sculpture" in the name of simplification.

Turning to the AI Act, González Fuster acknowledged the existence of **real overlaps and tensions, but warned that attempts to clarify them often create more confusion**. To this point, she referred to the example of the right to explanation, where efforts to define its relationship to the GDPR in the text of the AI Act have made it more complex rather than clearer. Similarly, duplicative obligations between the data protection impact assessment and the fundamental rights impact assessment risk making compliance unnecessarily cumbersome.

Finally, González Fuster noted that institutions like the EDPB continue to promise consistent application of the GDPR but have yet to fully deliver on this goal. She urged regulators and policymakers to focus on better implementation rather than endless reinterpretation.

3.5. TARGETED ADJUSTMENTS WITHOUT WEAKENING ITS FOUNDATIONS

In the final part of the discussion, Geering reflected on the UK's post-Brexit data reform as an example of targeted simplification. He said the UK legislation may bring benefits for domestic, consumer-facing businesses, particularly around legitimate interests and automated decision-making. However, for global service providers like his, the reform has little impact. Most companies serving EU clients must still comply with the EU GDPR, and large international organizations prefer maintaining a consistent, high standard of data protection worldwide. Geering described the **GDPR as a global success built on internationally developed principles**. He suggested that newer EU digital laws, in contrast, have been developed too rapidly, without the same foundation of global consensus or practical experience.

Responding to a question on potential narrow amendments to the GDPR, Micol said the Commission's approach remains targeted and pragmatic. **Simplification is meant to provide breathing space without affecting fundamental rights or the risk-based approach.** He noted that these proposals are about concrete, practical problems raised by stakeholders. Micol also pointed to recent CJEU case law clarifying that pseudonymized data is not always personal data, and to EDPB guidance confirming that legitimate interest can serve as a legal basis for AI training. These developments, he said, are helping to make the GDPR easier to apply in practice.

Domínguez de Olazábal **compared the GDPR to a Jenga tower, a structure built of interdependent rights and principles.** Removing or changing even one block risks destabilizing the framework. She argued that while simplification may seem minor, it could affect other provisions related to transparency and accountability. She underscored that the real weaknesses lie not in the text of the GDPR but in its enforcement. Civil society organizations have waited years for decisions under the one-stop-shop mechanism, while large companies can afford to delay or absorb fines.

González Fuster added that data protection law has always evolved through a balance of principles and flexibility. She said **the endurance of the GDPR and its predecessors stems from the ability to preserve fundamental principles while allowing for nuanced interpretation**, like compatible further processing.

She proposed that rather than breaking the system, Europe should continue refining it through such subtle adjustments, ensuring that it remains alive and adaptable. González Fuster likened the current debate to a game of Tetris, with shifting legislative pieces such as the GDPR and AI Act that must fit together coherently.

TAKEAWAYS

- The discussion highlighted a shift from calls to overhaul the GDPR toward improving its implementation through targeted, evidence-based adjustments and stronger cooperation between regulators.
- Two specific issues related to the GDPR and its application on the radar of the European Commission are: using legitimate interests for AI training, and the clarifications brought recently by the CJEU to pseudonymization and the definition of personal data.
- Several interventions stressed that the GDPR's enduring strength lies in its balance between clear principles and flexible application, urging that reforms refine rather than rewrite the existing framework.
- The AI Act's risk-based model was seen as creating uneven regulatory coverage and poor incentives, pointing to the need for proportionate safeguards across all AI systems.
- The global success of the GDPR as a regulatory model was explained by the fact that it was built on internationally developed principles. The new digital laws, including the AI Act, have been developed too rapidly, without the same foundation of global consensus.
- Overall, the panel agreed that the EU's data protection framework should continue evolving to meet new technological realities without eroding the core values that make it a global benchmark.

4. Lightning Talk: Are LLM-Based Systems Pushing Rights to the Breaking Point and Can We Govern Them?

During the first lightning talk of the Symposium, Isabel Barberà explored **emerging systemic risks posed by autonomous LLM systems and the importance of iterative lifecycle risk management**, including its limits in preventing systemic harm.

Barberà shared some insights from the report "*AI Privacy Risks & Mitigations Large Language Models (LLMs)*", commissioned by the EDPB, and from ongoing work for the Council. The report is based on Article 32 of the GDPR, focusing on data security and data protection risks.

The report elaborates on important concepts such as data flows, which are essential for understanding how data moves through AI systems from beginning to end. It also explores the different categories of data encountered throughout the lifecycle of an AI system, noting that each stage involves processing specific types of data. Additionally, it discusses the evolution of LLMs and how they interact with the internet and knowledge bases.

A key contribution of the report is the lifecycle-based risk management framework. While the concept aligns with Privacy by Design, its application to AI systems is more complex, as it requires assessing risks from the perspective of the model system. Examples include agentic AI and potential data leaks. Risk management forms a foundation for governance, but it is not sufficient to address all risks in LLM systems, and much research remains to be done. The report also emphasizes awareness of rights, highlighting the importance of understanding one's own rights and the effects of actions on the rights of others.

During the Q&A session, Barberà **stressed the importance of conducting *ex ante* risk assessments, noting that in practice companies do not always embrace this.** *Ex post* risk acceptance remains part of risk management, but its appropriateness depends on the size of the risk and the company's capacity to mitigate it.

TAKEAWAYS

- LLMs present distinct data security and protection risks across their lifecycle.
- Understanding data flows is essential to tracing how information moves within AI systems.
- An iterative, lifecycle-based risk management framework is needed to address AI-specific challenges.
- *Ex ante* risk assessment remains crucial, though not consistently implemented in practice.

5. Between a Rock (AI Act) and A Hard Place (GDPR)?

The second panel of the day examined one of the most critical points of friction in Europe's digital rulebook: the interaction between the AI Act and the GDPR. The discussion focused on how to untangle overlapping obligations, understand pathways for convergence and harmonization, and address persistent questions surrounding legal bases for AI training.

The panel featured Prof. Theodore Christakis (Université Grenoble Alpes), Rafaela Nicolazzi (OpenAI), Lorelien Hoet (Microsoft), and Laura Lázaro Cabrera (CDT Europe), and was moderated by Prof. Sophie Stalla-Bourdillon (Brussels Privacy Hub).

5.1. THE EDPB'S APPROACH TO HARMONIZING AI AND DATA PROTECTION RULES

Prof. Theodore Christakis noted that the EDPB Opinion on AI models dealt with the AI Act in a very satisfactory way, as it explicitly acknowledged the Act in several places, but always in a constructive way that aims to avoid conflict by clarifying definitions and ensuring that each instrument plays its respective role.

He found it very positive that the Opinion does not use the AI Act as an excuse to subject AI developers to harsher data protection rules or to conflate data protection compliance with new AI Act obligations. Christakis noted that the AI Act creates its own rules for risk levels such as high risk and systemic risk, with targeted obligations including transparency, human oversight, and safety assessments, while the GDPR deals with data processing risks. Merging the two, he warned, would entirely blur the links between data protection criteria and other forms of risk management and be extremely harmful for innovation in Europe.

As a second point, Christakis noted that even after the EDPB Opinion, fragmentation continues, with national DPAs still issuing their own guidelines. He said the CNIL tried to adopt a pragmatic approach, consistent with the view that the GDPR wants to promote innovation, not hinder it, but in a responsible way. In contrast, he said the Dutch DPA maintains a very restricted reading of the Opinion, for instance, by requiring model retraining for every erasure request instead of considering that an output filter could also work well in practice.

5.2. INDUSTRY REFLECTIONS ON ENGAGEMENT WITH DPAS AND EVOLVING GDPR-AI ACT PRACTICES

Laureline Hoet was asked what she had learned from recent interactions with supervisory authorities and what they hoped to see next. She began on a positive note, stating that there has been increased dialogue with DPAs, particularly with the Irish DPC, but also with others. She said there is a clear willingness from authorities to engage, understand, and ask questions, which the industry values greatly. While disagreements remain, this constructive engagement marks an important change.

Reflecting on recent developments, Hoet noted that the EDPB Opinion on AI models brought a key clarification: the recognition that legitimate interest is a valid legal basis, on the same hierarchical level as other legal bases. She added that there now seems to be emerging commonality around certain mitigating measures considered acceptable when training AI systems, such as notice and opt-out mechanisms, reasonable deadlines, data scrubbing, output filters, and red team testing. These measures, while not officially endorsed, are being discussed and used in practice with regulators.

On data minimization, Hoet observed a shift in understanding. While the concept was previously associated with less data, in the context of AI, accurate, complete, and representative data are needed. She said this reflects the AI Act's logic, where data minimization is interpreted more in line with purpose limitation, the idea that data may be reused or supplemented over time, provided the purpose remains compatible.

Hoet concluded that further guidance and clarity are needed on several points, especially regarding the roles of controllers and processors, and how these notions link to the different roles established by the AI Act, as well as on the use of sensitive data.

5.3. CONTINUOUS LEARNING IN APPLYING THE GDPR TO AI

Rafaela Nicolazzi was asked whether there is enough clarity regarding the effects of the GDPR on AI practices. She began by noting that AI development is moving at an unprecedented pace, with new paradigm shifts and new capabilities every week, creating both excitement and uncertainty. Drawing from her experience engaging with regulators across the globe, she identified three key expectations that AI companies like hers are seeing from supervisory authorities.

First, she said, is openness and communication. Regulators consistently emphasize the importance of proactive engagement before or during product adjustments. Nicolazzi stressed that being humble and forthcoming about how systems work, regularly sharing information on practices and safeguards, has directly influenced how companies design privacy protections from pre-training to deployment.

Second, she said, while transparency matters, explainability is gold. DPAs expect not just clear and accessible disclosures but meaningful explanations of how systems process data, such as layered notices and detailed explanations of data use for training. She also mentioned publishing research papers, system cards, and using different formats to communicate, since people learn in different ways. As an example, she referred to the Privacy Angel, a chatbot co-developed with the Italian Institute of Privacy to help individuals navigate privacy policies through natural, human-like conversation.

Third, Nicolazzi emphasized the need to ground regulatory expectations in the technology itself. Many authorities are bringing technical expertise to the table, which she welcomed, since guiding informed decisions by the technology is more likely to protect rights than unintentionally stifle innovation.

She concluded that building clarity around the GDPR's application to AI requires a mindset of openness, continuous improvement, and evidence-based regulation.

5.4. NATIONAL DPAS AS DRIVERS OF AI ACCOUNTABILITY AND PROTECTION OF RIGHTS

Laura Lázaro Cabrera was asked whether current AI training practices and safeguards show that the industry is going in the right direction. She began by acknowledging the important role of DPAs, noting that they were the first regulators to enforce AI accountability, even when it was still debated whether AI models process personal data at all. She highlighted that the Italian DPA's (Garante) decision on OpenAI came at a time when discussions within the EDPB were still ongoing, and many voices claimed that AI models could not process personal data because of the way such models worked. As a fundamental rights advocate, she said her organization was pleased to see that assumption debunked.

Lázaro Cabrera underlined that, while harmonization across Europe is important, the individual role of national DPAs in shaping the debate and paving the way for legal certainty at the EU level cannot be underestimated. She pointed to strong synergies between the Garante's approach and the EDPB Opinion on AI models, describing the Garante's decision as having set the tone for the kind of discussion needed on AI and data protection.

Lázaro Cabrera thought that the main takeaway from the Garante's investigation is that data protection cannot be an afterthought. The decision made clear that developers must identify a legal basis *before* processing personal data. She also welcomed the transparency measures introduced, including mechanisms enabling the public and users to request erasure or corrections of inaccuracies, which she described as a positive milestone demonstrating what good faith efforts can look like.

With regard to data subject rights, Lázaro Cabrera noted that it is still uncertain whether rights such as erasure can be fully exercised in practice. AI models cannot always guarantee deletion or accuracy, and companies frequently invoke technical impossibility. Technical complexity or impossibility should never serve as a justification for non-compliance.

Lázaro Cabrera also warned against the growing idea that data protection could be seen as an "obligation of means" rather than of results. She underlined that the GDPR gives concrete effect to a fundamental right, not a flexible or optional standard. Concluding her remarks, she stressed that regulators and companies must avoid lowering compliance expectations under the pretext of innovation, affirming that data protection must remain a fully enforceable individual right—no matter how complex or advanced the technology becomes.

5.5. TOWARDS PRAGMATIC AND HARMONIZED APPROACHES TO AI AND PRIVACY

In the final exchange of the panel, speakers reflected on the relationship between GDPR compliance, AI innovation, and the need for pragmatic solutions to persistent legal and technical challenges.

Hoet noted that the CNIL recognizes both the benefits and weaknesses of open-source AI models. While open source promotes transparency, verification, and vulnerability reporting, it can also expose systems to manipulation or exploitation and make it harder to protect data confidentiality.

Nicolazzi emphasized that OpenAI has been investing in privacy-preserving techniques across the model lifecycle, from pretraining to post-deployment, and recently published its multi-layered privacy approach during the Global Privacy Assembly in Seoul. Referring to tools such as filtering, synthetic data, and output privacy features, Nicolazzi announced an in-house innovation, the "privacy filter", which will be made publicly available for the developer community to test and improve.

Christakis reiterated the importance of harmonization, stressing that the 27 DPAs across the EU should unite in their positions. In this context, he welcomed the EDPB Opinion on AI models for promoting harmonization and reaffirming that the GDPR encourages responsible innovation.

Lázaro Cabrera agreed that AI is here to stay and that regulators must continue to refine enforcement practices. She highlighted that DPAs can play a powerful role by focusing on risk mitigations as part of the legitimate interest assessment, emphasizing guarantees and safeguards rather than rigid obligations like model retraining. She also noted that the GDPR and AI Act set standards unthinkable elsewhere, concluding that the **GDPR's rights-based framework and the AI Act's risk-based approach are complementary, together enabling effective remedies and rights protection through mechanisms that could also strengthen DPAs' new roles as AI regulators.**

TAKEAWAYS

- The EDPB Opinion on AI models was praised for constructively clarifying this relationship and avoiding legal overlap or conflict.
- Harmonization remains a challenge, as national DPAs take divergent approaches, some pragmatic, others restrictive.
- Dialogue between DPAs and industry has improved, fostering more openness, mutual understanding, and early engagement on AI compliance.
- Data protection cannot be an afterthought. Compliance must precede processing, and technical impossibility is not a valid excuse for noncompliance.
- AI pushes for shifts in how classic data protection principles, like data minimization, are interpreted.
- Innovation and compliance are compatible, but pragmatic, evidence-based, and harmonized approaches are needed to balance both effectively.
- The GDPR's rights-based and the AI Act's risk-based frameworks were described as complementary, together forming the foundation for trustworthy and accountable AI governance in Europe.

6. Workshop Sessions Diving into the Main Themes of the Day

Three workshop sessions were facilitated by Gianclaudio Malgieri (Leiden University & Brussels Privacy Hub) on **"The Right to an Explanation: From the GDPR to the AI Act,"** Bárbara Lazarotto (VUB) and Pablo Trigo Kramcsák (VUB) on **"From Theory to Practice: How Would You Change the GDPR?"**, and Vincenzo Tiani (FPF) and Monika Tomczak-Gorlikowska (Prosus Group) on **"Agentic AI under the GDPR and the EU AI Act."** The main highlights from these workshops were presented in the plenary.

6.1. THE RIGHT TO AN EXPLANATION: FROM THE GDPR TO THE AI ACT

Facilitator: Professor Gianclaudio Malgieri (Leiden University & Brussels Privacy Hub)

The discussion focused on how the right to explanation in the AI Act overlaps with similar provisions under the GDPR. Participants noted that the scope of this right remains highly complex and nuanced. Determining its applicability depends not only on whether a system is high-risk but also on the presence of adverse effects and the absence of other overlapping explanatory rights. Reference was made to the CJEU *Dun & Bradstreet* case, which recognized an explicit right to explanation in the GDPR. It was also observed that AI outputs not directly influencing decisions are exempted from the high-risk category under Annex III of the AI Act. The group concluded that the right to explanation is a dynamic, evolving rule, whose interpretation will depend on future case law, updates to the high-risk list by the Commission, and the interaction with other rights. Article 86 was described as the only individual right in the AI Act, yet not really connected to the right to contestation and therefore potentially a "powerful but powerless" tool. The placement of Articles 26 (obligations of deployers of high-risk AI systems) and 86 of the AI Act was discussed as an illustration of how EU law can be shaped by the timing and political context of trilogue negotiations.

6.2. AGENTIC AI UNDER THE GDPR AND THE EU AI ACT

Facilitators:

- *Vincenzo Tiani (Future of Privacy Forum)*
- *Monika Tomczak-Gorlikowska (Prosus Group)*

The workshop explored two practical use cases of agentic AI: one in the e-commerce domain, where digital agents act on behalf of users to complete transactions and make recommendations, and another in the context of recruitment and employment. The discussions highlighted how varying degrees of autonomy and spectrum of tasks influence explainability. There was a broad consensus that explainability is essential to build user trust, particularly in high-impact applications such as employment. Participants also discussed the need for standards to ensure assurance and transparency, including bias detection, discrimination prevention, and cybersecurity. Privacy-by-design and privacy-enhancing technologies were identified as key to protecting sensitive data, such as voice or biometric data. It was noted that users should remain aware and in control when sharing personal data with AI agents, especially during initial setup phases.

6.3. FROM THEORY TO PRACTICE: HOW WOULD YOU CHANGE THE GDPR?

Facilitators:

- *Bárbara Lazarotto (Vrije Universiteit Brussel)*
- *Pablo Trigo Kramcsák (Vrije Universiteit Brussel)*

The workshop invited the participants to reflect on possible reforms to the GDPR. Enforcement emerged as the first priority, with support for stronger coordination among DPAs rather than the creation of a centralized body. The second priority was to clarify the definition and interpretation of legal bases, with many noting inconsistencies across Member States and calling for greater guidance at both EU and national levels. The group also discussed the need to refine principles, particularly fairness, and debated whether clarification, merging or expansion of these principles would be appropriate. Participants considered broadening research-related exceptions. The group concluded that the GDPR should not be "simplified" but rather “sharpened” to enhance precision and coherence. The final reflection pointed to the broader issue of regulatory fragmentation in the digital domain, suggesting that effective governance requires coordination across the wider EU legislative framework rather than amendments to the GDPR alone.

7. Honored Guest Speaker Talk: Prof. Norman Sadeh

This year, the Brussels Privacy Symposium welcomed Prof. Norman Sadeh of Carnegie Mellon University, who delivered a speech on agency in the age of AI.

The talk explored the growing complexity of AI agents and the implications this evolution has for privacy and security. AI agents can be viewed as "mobile apps on steroids", tools that must understand users' preferences and behaviors far more deeply than traditional applications. Over the past decade, AI research has moved toward the broader goal of Artificial General Intelligence (AGI), with agents acting as an intelligent "glue" that can communicate across different apps and contexts. As we move toward these more general agents, they must have a broader and deeper knowledge of their users, which greatly expands the challenges around privacy and control of personal data.

As people begin interacting with a growing number of agents across a wide range of scenarios, their ability to keep track of data flows and understand the consequences of data sharing will become increasingly limited. Research has shown that **privacy preferences are extremely complex and context-dependent**, e.g., someone might allow only team members to see their location and only when they are in the same building. To support such nuanced preferences, **we will need standardization, protocols, and authentication mechanisms capable of handling this complexity in a uniform way**.

Studies involving hundreds of participants have confirmed that privacy attitudes are diverse and situational. While regulations such as the GDPR or the California Consumer Privacy Act (CCPA) are helpful, they are not sufficient to manage this diversity. To reduce user burden, privacy assistants have been developed to inform users about data practices, provide support to manage data subject rights, and make personalized recommendations based on short interactions. Some of these systems, initially developed in academic settings, have been implemented by companies like Google and Apple, showing that such approaches can work effectively in real-world contexts. However, obstacles remain, including the lack of open permission APIs and inconsistent regulatory frameworks.

Sadeh's key message was that **as AI agents become more powerful and pervasive, the amount and complexity of personal data involved will increase dramatically.** To ensure that privacy is respected, we need standards, taxonomies, and protocols capable of capturing privacy preferences. These frameworks must also align with how users think about privacy, not just with how engineers describe technical permissions. Current regulations like GDPR and CCPA provide a strong foundation, but they will need refinement to encourage the development of richer ontologies and interoperable systems that allow agents to act responsibly on behalf of users, handling tasks such as opt-in, opt-out, or data deletion across different contexts and jurisdictions. Finally, Sadeh noted that the **adoption of these pragmatic steps is slowed by industry inertia.** Without regulatory encouragement, progress will be limited. Governments must play a supportive role, stimulating innovation while guiding the creation of standards and best practices.

TAKEAWAYS

- AI agents are becoming more complex, requiring a deeper and broader understanding of users and access to personal data.
- Research is moving towards AGI, enabling agents to communicate across different apps and contexts.
- To reduce user burden, privacy assistants can inform people about data practices, provide support to manage data subject rights, and provide personalized recommendations based on interactions.
- Privacy preferences are complex and context-dependent. The GDPR and CCPA are useful, but they are not sufficient to manage this diversity. As such, standards, taxonomies, and protocols are necessary to ensure that privacy is respected as AI continues to develop.

8. Lightning Talk: Investigating Automated Decision-Making

In the second lightning talk of the day, the program turned to automated decision-making and the role of human oversight. Ylja Remmits, Head of Projects at Algorithm Audit, shared insights from her work at the intersection of technology, law, and practice, particularly within the Dutch public sector.

Remmits discussed automated decision-making under Article 22 of the GDPR and presented **a five-step approach to prevent algorithmic decision support systems from falling under this prohibition**. The first steps regard *understanding the decision-making process*, identifying whether decisions produce legal or similarly significant effects, and ensuring meaningful human intervention. Two additional steps apply empirical and statistical methods to test whether human involvement influences outcomes.

Remmits used the example of the Dutch Tax Office's fraud signal system, where algorithmic risk scores were stored long-term without proper labeling. She further explained that **assessing compliance requires mapping transparency obligations and identifying points of human intervention**. Yet, determining what counts as a "similarly significant effect" remains a grey area. The decisions affecting fundamental rights should also be considered significantly impactful.

Remmits also highlighted the importance of understanding the reviewer's context, what information they have, how much time they are given, and what training they receive. She discussed practical methods such as blind review, where some cases are presented without algorithmic flags to reduce bias. She also talked about empirical testing to measure human-algorithm agreement. **A high agreement rate could indicate bias rather than oversight, though disagreement provides stronger evidence of independent judgment.** Field experiments can further reveal whether humans rely on algorithmic outputs or exercise autonomous evaluation by randomizing the information presented to decision-makers.

In her concluding remarks, Remmits noted that **combining qualitative assessments of process design with empirical experiments provides a way to determine whether human intervention is meaningful or symbolic**.

TAKEAWAYS

- Methods such as blind review reduce bias, while empirical tests measure whether humans independently assess algorithmic outputs.
- Effective oversight depends on giving reviewers the time, information, and authority to make real decisions.

9. Data Protection Authorities in the Spotlight: Pathways for Harmonization

The final panel of the Symposium brought together representatives of some of the most active DPAs in the EU to discuss the evolving role of data protection enforcement in the age of AI. The moderator noted that throughout the day’s sessions, one theme had consistently emerged: the centrality of DPAs in interpreting and enforcing the GDPR as it applies to AI systems, and their potential to shape broader regulatory harmonisation across the EU.

The panel featured **Sarah Artola** (CNIL), **Guido Scorza** (Italian DPA, Garante), **Sven Stevenson** (Dutch DPA, **Paul McDonagh-Forde** (Data Protection Commission of Ireland), and was moderated by Dr. **Gabriela Zanfir-Fortuna** (Future of Privacy Forum).

9.1. THE IRISH DPC’S SUPERVISION FUNCTION AND ITS ROLE IN FACILITATING RESPONSIBLE AI INNOVATION

Paul McDonagh-Forde (Irish DPC) described how the DPC engages with major technology companies that develop and deploy AI systems within the EU. As the lead supervisory authority for many global tech firms headquartered in Ireland, the DPC plays a central role in ensuring that AI systems align with the GDPR before entering the EU market. McDonagh-Forde clarified that this engagement primarily takes place through what the DPC calls its “supervision function,” a voluntary, non-statutory process distinct from formal investigations or audits.

Under this supervision framework, companies contact the DPC proactively to discuss new AI products or services before launch. The DPC reviews proposals, offers recommendations, and promotes dialogue to foster responsible innovation consistent with fundamental rights, without issuing binding compliance determinations. McDonagh-Forde notes that this collaborative supervision approach, adapted to the specific AI models, aims to address potential compliance issues before products reach the market.

The DPC remains ready to use its statutory powers where necessary, including taking enforcement actions. Importantly, these supervisory engagements are without prejudice to the statutory side, ensuring that potential compliance issues can still be addressed later through regulatory channels. McDonagh-Forde concludes by noting that the DPC coordinates closely with other DPAs through the EDPB to ensure a common position throughout Europe.

9.2. ENFORCEMENT LESSONS AND THE EVOLVING ROLE OF REGULATION IN AI OVERSIGHT

Guide Scorza (Garante) offered insights into a more enforcement-oriented approach to AI governance. Reflecting on multiple cases involving AI systems such as chatbots and LLMs, Scorza focused on positive and negative lessons from recent enforcement actions.

On the positive side, these actions have sent a strong message to the market: **innovation cannot take place outside the regulatory framework.** Regulatory action can guide industry towards more sustainable practices that balance technological development, business objectives, and human dignity. Several cases have led to some improvements, such as the withdrawal of certain services from the market, more transparency from AI providers, the identification of legal bases for data processing, and the introduction of opt-out mechanisms.

Scorza also acknowledged two challenges: on the one hand, there are still limitations in achieving extra-European enforcement, making it challenging to ensure compliance or meaningful cooperation in cross-border contexts; on the other hand, the experience so far shows that conventional regulatory approaches are often insufficient to address the speed and complexity of AI innovation.

Scorza argued that regulators must now develop new enforcement models capable of ensuring both legal certainty for industry and robust protection of fundamental rights.

9.3. APPLYING THE GDPR TO AI SYSTEMS THROUGH PRACTICAL GUIDANCE

Sarah Artola (CNIL) explained that with the emergence of generative AI, the CNIL received many questions from stakeholders about the application of the GDPR to AI training. In response, the CNIL launched an AI Action Plan, which included the publication of fact sheets and other actions. The aim was to clarify the legal framework applicable to the training of AI systems and models and to give legal certainty to stakeholders.

The “factsheets” published by the CNIL were designed to address the toughest questions and friction points in applying the GDPR to AI models, focusing on the least solvable issues. According to Artola, this work showed that it is possible to reconcile the challenges of AI with the application of the GDPR.

For example, regarding the principle of purpose limitation, the CNIL stated that when a controller cannot completely foresee in advance all possible applications of an AI model, they may still define a sufficiently specific purpose by referring to the specificities of the model. On the principle of data minimization, the CNIL explained that this does not prevent the use of large training datasets but recommended carefully selecting the data to ensure that it is necessary for the pursued purpose.

As for the legal basis, the CNIL stated that consent is not always necessary and that legitimate interest can be a valid legal basis, provided that sufficient safeguards are implemented. These safeguards are of utmost importance to ensure that the development of AI systems and models does not disproportionately impact the fundamental rights of data subjects.

Artola emphasized that this work demonstrates that EU data protection law is still relevant and appropriate for AI regulation. It is not aimed at hindering innovation, but rather encourages responsible innovation, enabling the development of ethical AI systems that European citizens can trust and that are in line with European values. She concluded that the CNIL will continue to apply a pragmatic and comprehensive approach to ensure the effective application of the GDPR to AI systems.

9.4. COORDINATING AI AND DATA PROTECTION SUPERVISION UNDER AN EXPANDING DIGITAL FRAMEWORK

Sven Stevenson (Dutch DPA) explained that the role of DPAs today goes beyond being a linchpin between the GDPR and the AI Act. In many cases, including their own, authorities have joint responsibility not only for these two frameworks but also for the broader digital landscape, which now includes multiple overlapping legislations such as the DSA and the Data Act. This **growing complexity is both a challenge and an opportunity,** as it requires supervisors to manage digital entities, data systems, and data flows through a coordinated approach.

Since early 2023, the Dutch DPA has operated under a coordinating structure created by the national government to bring together all supervisors working on AI and algorithms in the digital domain. This structure is built around three main tasks that form the foundation of its work, with AI Act responsibilities to be added on top.

The first task is to conduct early monitoring exercises to identify issues that could impact people or their data before incidents happen. This allows the authority to detect problems early, determine which supervisory powers apply, or identify gaps in regulation that might require legislative or structural solutions.

The second task is to achieve cooperation between supervisors by bringing together all relevant authorities dealing with AI and algorithms. The goal is to develop shared perspectives, maintain close contact, and engage in discussion to ensure coherent guidance.
When it comes to guidance, Stevenson stressed that the GDPR remains central, running through every piece of digital legislation. This allows the authority to ensure consistency across legal frameworks. A concrete example mentioned was the concept of “meaningful human intervention”, with a similar type of wording appearing in other EU instruments such as the Consumer Credit Directive, the European Media Freedom Act, and the DSA. Without coordination, there is a risk that different sectoral supervisors might interpret this notion differently.

9.5. THE ROLE OF THE EDPB IN ENSURING CONSISTENCY ACROSS NATIONAL AI ENFORCEMENT

The discussion turned to the role of the EDPB and its collaboration with national DPAs in maintaining coherence and consistency in AI-related matters.

McDonagh-Forde explained that the relationship between national DPAs and the EDPB is not one of counterbalance, since all national authorities are part of the Board itself. The EDPB derives its legal existence from being a collective of DPAs, and cooperation mechanisms under Chapter VII of the GDPR ensure consensus in cross-border cases. When a consensus cannot be reached, the dispute resolution procedure is applied. McDonagh-Forde mentioned that the Irish DPC requested the EDPB's AI Opinion last year to achieve agreement among supervisory authorities on key issues. He noted that future work would strive for greater consistency, considering developments such as the Helsinki Statement.

In agreement, Artola stated that the EDPB's work complements the national DPAs' efforts. As national members of the EDPB, authorities actively contribute to collective guidance, including the AI Opinion, which was prepared under tight deadlines, and other ongoing work streams. These include guidelines on data scraping in generative AI and joint guidance with the European Commission on the interplay between the AI Act and the GDPR. She stressed that all these efforts are crucial for maintaining consistency across Europe, ensuring that national approaches align as the regulatory environment evolves rapidly.

9.6. THE FUTURE OF DPAS AS AI REGULATORS

The final part of the panel focused on whether DPAs will continue to play a central role as AI regulators once the AI Act begins to take full effect.

Stevenson explained that in the Netherlands all supervisory authorities jointly published a proposal on how AI should be regulated nationally, outlining a model that is now emerging in several other EU Member States. Under this model, the DPA will hold a large and challenging role, particularly in relation to Annex III (defining high-risk AI systems) of the AI Act. In addition, the DPA will be responsible for transparency requirements and prohibited AI systems. He described this stage as an exploration involving "deep dives" into the various AI categories and risk assessment areas. Comparing the process to "walking into a video store," Stevenson noted many AI systems and use cases that must be examined and understood. This represents a significant challenge and workload for DPAs and other authorities involved in AI oversight.

Scorza agreed that there is indeed a future for DPAs in the field of AI, even though in Italy, the national AI Act designated other agencies as primary regulators. In his words, the relationship between personal data and AI is "too strong to imagine that the data protection authorities will not play a very central role in the governance of artificial intelligence". Scorza further noted the need to establish effective cooperation and collaboration mechanisms between DPAs and other national agencies to avoid confusion and uncertainty for the market, industry, and users. He also noted that DPAs are likely to play a particularly prominent role in overseeing AI in the public sector.

TAKEAWAYS

- DPAs are becoming central to AI governance, ensuring the GDPR guides responsible AI development while shaping harmonization under the AI Act.
- The CNIL's guidance confirmed that purpose limitation and data minimization can apply effectively to AI training, reinforcing trust and responsible innovation.
- The Dutch and Italian DPAs foresee a continued, central role for DPAs in AI oversight, emphasizing cross-authority cooperation and consistency across the EU's digital framework.

10. Closing Reflections: In Dialogue Wojciech Wiewiorowski and Gianclaudio Malgieri

Prof. Gianclaudio Malgieri
Leiden University
Wojciech Wiewiórowski
European Data Protection Supervisor
FUTURE OF PRIVACY FORUM

This year's closing reflections between Prof. Gianclaudio Malgieri, of Leiden University, and Wojciech Wiewiórowski, the European Data Protection Supervisor (EDPS), explored the current challenges posed to the GDPR by political changes and the simplification agenda.

The discussion opened with a reflection on how data protection challenges had evolved since December 2019. In the years that followed, global crises, political shifts, and the rise of generative AI deeply affected the field, alongside several new EU pieces of legislation directly impacting the GDPR. By 2025, debates in Europe centered on possible GDPR reforms under the banners of "simplification" or "deregulation." Within this context, Malgieri asked how the EDPS had navigated these turbulent years and what had been his main satisfactions and disappointments.

Supervisor Wiewiórowski recalled that when he began his mandate in December 2019, his office prepared a five-year strategy, ready to be presented in March 2020, when the pandemic began, revealing that many of the current challenges were not reflected. He expressed gratitude to the EDPS team, whose expertise and dedication ensured the institution's resilience. His main disappointment was that, while it is not the EDPS's role to assess them, decisions by other DPAs, political choices, and court judgments sometimes amounted to setbacks for the office.

The conversation turned to how data protection professionals can resist and adapt to historical changes, particularly as recent events seem to have expanded the notion of public interest in data processing. Supervisor Wiewiórowski noted that **data protection was born out of past crises and is founded on a continuous search for balance between State needs and individual rights.** Each crisis, he said, tests the principles of necessity and proportionality.

Regarding the simplification of the GDPR, Supervisor Wiewiórowski emphasized that political changes elsewhere should not dictate EU policy and that any simplification must not compromise fundamental rights. When asked which parts of the GDPR might change after nearly a decade, he insisted that the core principles must remain untouched. Persistent weaknesses include uneven enforcement across Member States and the slow development of codes of conduct and certification mechanisms, while procedural differences continue to hinder uniform application across Europe.

On the intersection of GDPR principles and generative AI, he argued that there is no fundamental conflict, only a continued need for balance and coherent judicial interpretation. He also highlighted the importance of stronger coordination among national courts, noting that some Member States have never referred GDPR questions to the Court of Justice.

Finally, in reference to the Digital Fairness Act (DFA), Supervisor Wiewiórowski observed that, while a consumer-oriented approach appears promising, the concept of “fairness” remains unclear even within the GDPR and varies across languages. The discussion concluded with the reflection that, **ten years after its entry into force, the GDPR’s principles remain valid but still require explanation, interpretation, and deeper understanding.**

TAKEAWAYS

- Each crisis tests the principles of necessity and proportionality, requiring a balance between State and individual rights.
- Any simplification of the GDPR should not compromise fundamental rights, and core principles should remain untouched.
- There are still weaknesses, including uneven enforcement, slow development of codes of conduct, and procedural differences across Member States.
- GDPR and generative AI do not conflict, but there is just a continued need for balance and coherent judicial interpretation.
- The DFA has a promising consumer-oriented approach, but the fairness concept is unclear and varies across languages.

11. Thank You and Acknowledgments

A note from Bianca-Ioana Marcu, Managing Director, FPF Europe

The Future of Privacy Forum and the Brussels Privacy Hub, as co-organizers of this year's Symposium, would like to thank all speakers and attendees for their participation and meaningful engagement in the day's proceedings. We share a special note of thanks and appreciation for those traveling far and wide to spend the day with us in Brussels from the U.S., Japan, and beyond.

The organizers extend a warm thanks to this year's Workshop facilitators: Gianclaudio Malgieri, for leading the Workshop on **"The Right to an Explanation: From the GDPR to the AI Act"**; Bárbara Lazarotto and Pablo Trigo Kramcsák, for co-leading the Workshop titled **"From Theory to Practice: How would *you* change the GDPR?**; and Vincenzo Tiani and Monika Tomczak-Gorlikowska for co-leading the Workshop on **"Agentic AI under the GDPR and AI Act"**.

The organizers similarly extend a warm thanks to this year's sponsors, **Microsoft** and **Prosus Group**, for providing us with the lunch and coffee breaks that are important moments for participants to connect throughout the day.

Last but certainly not least, **we thank all of the staff of the Future and Privacy Forum and the Brussels Privacy Hub** for their brilliant ideas, efforts, patience, and positivity that went into building this year's program. Thank you to the excellent A/V crew that kept the day running smoothly.

We look forward to welcoming you again for the **10th anniversary edition** of the Brussels Privacy Symposium in 2026!